consult hyperion

Conference paper

e-ID as a public utility

Neil A. McEvoy

eema the european association for e-identity and security

Consult Hyperion
Tweed House
12 The Mount
Guildford
GU2 4HN
t: 01483 301 793 f: 01483 561 657
www.chyp.com

V0.1, 11th May 2007

Background

Identification is something that everyone does naturally (and often sub-consciously) many times a day, and yet in a dozen or so years of effort, no effective, general-purpose e-ID infrastructure has been rolled out.

In the public sector, government-issued identity cards have met reasonable public security objectives, but have been less successful in providing for frequent access to a range of e-government services. Further, in many countries, there is widespread antipathy to the concept of identity cards (especially "smart" ones), where people fear that the government will build up a record of their every movement and transaction.

The private sector has been no more successful, with concepts such as PKI and federated identity being too complex for the wider public and confined to unconnected islands of specialized usage.

This short paper addresses the properties that an e-ID scheme might have in order to become a part of the fabric of society, to enable identification to occur with (almost) equal facility in the electronic realm as in the face-to-face realm, but without the threatening overtones of the surveillance society.

The public utility model

We turn on the tap or plug an electrical device into the wall, not because a government official makes us, but because we want to. Piped water, electricity and gas are a *utility*[1] to us, not an imposition. In what way might an e-ID scheme provide such a utility, while still enabling the usual government requirements such as the ability for a policemen to identify a witness to a crime, or to verify that a person is eligible to claim state benefits?

It should not be difficult to answer this question; most people will identify others, and be identified by others, several times a day, without a second thought. As an example, consider a business conference: most people will exchange business cards with many others, obtaining contact details in a moderately convenient form and with a modicum of assurance that they are correct.

If there were a way to do this transaction electronically, providing better security and convenience, and which could also do the same thing at a distance, then this would surely be a boon to society. The requirements are that:

- The scheme is universal
- The transaction is two-way

[1] Whether these services are provided by a state monopoly or by competing private companies supplying a standard product within a regulated framework is not germane to the argument developed in this paper.

- Transactions take place in a second or so
- No out-of-the-ordinary gadgets are required
- The scheme is extensible, without compromising simplicity for basic transactions.

Let us examine these requirements in turn.

Universality

The process for conducting an identity transaction should be exactly the same, regardless of the status of any individual. It must be no less applicable to two people from different continents as to next-door neighbours.

Within a country, it is reasonable to suppose that the national government is best placed to put together a scheme that meets this requirement. To meet the international requirement, it is vital that due attention is paid to standardisation: which has been slow in the realm of identity cards—though better for e-passports. To field such a system worldwide, 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—is desirable.

The two-way street

It is vital that within the same hardware/software e-ID package, provided to everyone, is the means not only for the holder to assert his identity, but to verify anyone else's. The scheme should not seek to limit in any way the ability of consenting adults to swap their identities, in a way that is mutually verifiable.

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. The technology can be used to smooth our dealings with anyone we meet and not just on the rare occasions when we brush with officialdom, which by their nature are not necessarily welcome. Thus, the e-ID technology will be viewed as an enabler and not as an imposition by Big Brother; the uses are limited only by people's imagination and wants, not by the decrees of the state.

Clearly, there will be occasions where the overall relationship between two people performing some transaction will not be symmetrical; but this is no reason why an identity transaction should not be. 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; 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. We must be able to facilitate instant transactions of this two-way nature.

Far from compromising the core and traditional government requirements for e-ID, the two-way street concept supports them. In the first place, people will be

used to carrying and using the identity token; it will not be tucked away at the back of a draw behind last year's Christmas cards and the menus of the local take-away restaurants. Secondly, people will come to regard it as "their" token: not something foisted upon them to be used in unpleasant situations like answering to a petty official or filing a tax return. Thirdly, the verification, by the citizenry, of people *claiming* to be a public official is conducive to public security in itself.

Quick transactions

For such a scheme to be become a part of the fabric of life, it must be usable in the widest possible range of circumstances and, in particular, in ordinary circumstances, such as a face-to-face meeting. 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 order to displace familiar mechanisms (as a first step to achieving still wider utility), it must be better than them. The most important property that it has to better, to achieve any traction with the public, is convenience, of which speed is an important measure. The benchmark should be the swapping of business cards; the transaction should take no more than a second. Of course, by digital means, other aspects of the transaction can be improved: in particular, by the use of cryptography, the privacy and integrity of the transaction.

The gadget

The requirements for the device that a person must carry to engage in identity transactions are:

- It must house a physically secure chip, with a cryptographic capability
- It must be able to communicate with similar devices at any range with minimal effort on the part of the user
- It must have a keyboard, so that the holder can enter a PIN to verify himself to the secure chip (using a device that he trusts not to misuse the PIN)
- It should have a biometric capability
- The users must already have one, which they are used to taking everywhere.

Of course, the mobile phone is the only device to fit the bill, which it does excellently. They already contain secure SIM cards. Phones which contain an additional secure (NFC–Near Field Communication) chip are being promoted by the manufacturers (and are being demanded by organisations such as payment schemes and transport operators), which will enable organisations other than the network operator to manage applications on a secure chip.

The NFC chip will enable near-instantaneous, close proximity transactions between phones. Thus, the swapping of business cards will be accomplished by "kissing" phones. In an instant, verified contact details will be swapped, will appear on screen, and can be filed automatically in the phone's address book—

perhaps to be synchronised to a laptop contact manager via Bluetooth at a convenient moment.

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 Bluetooth and an internet-connected PC across the world.

Phones can capture and transmit the most natural and convenient biometric: the 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.

Of course, the single most important property of the mobile phone is that everybody already has one and they don't leave home without it; and that they either freely pay for it or others (the network operators) are prepared to subsidise them.

Extensions

The amount of information that people want to associate with themselves to some other person (and the latter are happy to obtain) may vary with the circumstances. For the business card case we have pursued, it will be name, affiliation and business contact details. In other cases, name may not be important: for example in proving one's age in a bar. In other cases, name and home address may be appropriate. Therefore, the more sophisticated users may want to set up 'profiles': sets of information to give out in different circumstances—at their discretion. It may be that not all of this information is stored on the phone. The individual could set up and manage his profiles on the internet. In a transaction, a url, containing an authorisation code, might be passed to the other party: his phone could go online to get the extra details. However, if such niceties are to be included in the scheme, it is vital that their potential use does not obstruct 'vanilla' transitions between those who are less than 'geeky'.

Scheme considerations

This paper has concentrated on the facilities that should be provided to the citizen, to allow him to assert his identity and to verify that of others. This section provides some indication of how the central facilities, which will tie the system together, should be organised.

Firstly, there must be some kind of central register.[2] The sole purpose of the register should be to ensure that each person is registered only once. It will contain, for each person, a unique (but otherwise meaningless) number to identify that individual, and whatever set of biometrics is needed to ensure that the probability of two people possessing the same set is vanishingly small. And that is all. The system will be on a vast scale. To give this pivotal element any extra functionality is to invite failure, given the industry's track record in delivering systems that are both large and complex. To add any personal information, would to present criminals with a one-stop shop for identity fraud on an industrial scale.

[2] In a truly global system, this may need to be distributed across jurisdictions.

Organisations (be they public or private sector) that have a need to associate personal data with identities, and which are duly regulated, can look after their own specific and proportionate set of personal data. To prevent a thorough criminal from associating data pertaining to the same individual, these organisations, or sectors, should use an identifier for the individual which is specific to the organisation or sector. Thus the unique number associated with the unique set of biometrics would not be used for any transactions. A central 'blinding' service would generated sectoral identifiers for an individual, by applying a cryptographic one-way function using the individual's core identifier and an organisation or sector specific key. Thus, there would be no way for any organisation (or anyone employed by it) to work backwards to the core identifier and hence to an individual's other sectoral identifiers and private personal data held by others. In special circumstances, for example on production of a judicial warrant, a law enforcement agent of appropriate rank could apply to the blinding service to re-generate the sectoral keys so that a suspect's activities could be tracked. Thus a reasonable balance between privacy and the needs of law enforcement can be struck.

Summary

Having confidence in others' identity and attestable attributes is central to day-to-day human interactions. And yet, in the digital age, no private sector e-ID scheme has achieved ubiquity and no public sector scheme has seen everyday usage. To achieve this, electronic schemes have got to better traditional methods in a face-to-face environment as well be usable for remote transactions. Such a system must be based on reciprocity—no one individual should be placed in a subordinate relationship to some special class of individual, or corporate entity, by virtue of the system used to establish identity. The natural vehicle for such a system is the mobile phone, especially as they become enabled with an NFC capability. They meet all the essential requirements, at no marginal cost. No other device is likely to do this in the foreseeable future.

** END OF DOCUMENT **