It will be noted that in early 2003 BCSL believed the marketing literature put out by the biometrics suppliers. That belief was undermined by the evidence of the UKPS biometrics trial and US-VISIT. BCSL is now a biometrics apostate, a state recommended here to everyone else, the UK Home Office included.

Mobile Phones are the ID Cards of the Future

A Proposal

by

David Moss

of

Business Consultancy Services Ltd (BCSL)

bcsl@blueyonder.co.uk

... mobile phones with digital certificates stored on them should be considered as an alternative to plastic ID cards ...

... an ID card unlike any ID card ever proposed in that it not only identifies the holder but also tracks him ...

... mobile phones have been paid for by the users. The cost does not appear in the national accounts. This could be a case of a successful PFI ...

... commended to the Home Office as a lower risk way to achieve its objectives ...

... at the heart of PKI is a "web of trust" concept, which the Home Office may find helpful in explaining and promoting an entitlement card scheme based on digital certificates ...

1 PROPOSAL

1.1 The Home Office has invited comments on proposals for a national entitlement card system based on:

- Compiling a new database covering 67m people ...
- ... improving checking procedures in various agencies ...
- ... incorporating biometrics and
- ... issuing everyone with either a dumb or a smart plastic card.

1.2 That is one feasible architecture.

1.3 No arguments are raised in this proposal concerning procedures being improved nor concerning biometrics. The benefits are self-evident.

1.4 There must, however, be considerable doubts about the advisability of creating a large new database. The Home Office would run the risk of another Accenture/EDS/Capita debacle.

1.5 Is there any need to run that risk? Surely not. Much of the data required must already be stored in the existing databases maintained by the various departments of state and their agents. New data, such as biometric data, could be added to the appropriate databases where needed.

1.6 It is suggested that an alternative architecture for the entitlements system could be based on developing an interface to all the existing databases, a portal to which they are all connected and from which they can all be queried using powerful search engines like Google.

1.7 Initially, at least, this would be a smaller, more prudent project and could be managed inhouse. No further points are made here on this subject.

1.8 It is further suggested that mobile phones with digital certificates stored on them should be considered as an alternative to plastic ID cards.

1.9 Digital certificates are part of the PKI, the public key infrastructure. They are issued by Certificate Authorities following checks carried out by Registration Authorities. The Passport Agency and DVLA (among others) are effectively both Certificate Authorities and Registration Authorities. They could issue digital certificates instead of material passports and driving licences.

1.10 The use of digital certificates here may be compared to dematerialisation in the securities industry.

1.11 If the mathematicians behind PKI are correct, then it is impossible to forge digital certificates. It may be all too possible to forge plastic entitlement cards.

1.12 Digital certificates must be stored on a device such as a server, a desktop PC, a laptop, a PDA or a mobile phone. Other consumer electronics products like digital cameras or MP3 players could be considered but 70% of people in the UK apparently have a mobile phone and that makes it the best candidate for the device on which to store digital certificates.

1.13 Mobile phones can be tracked. The US Federal Communications Commission's E911 directive specifies that, by 2005, most mobile phones in use in the US should be locatable accurately to within 50m 67% of the time and 150m 95% of the time. The US mobile phone network operators are using either GPS or E-OTD to determine location. The same technology may be used in Europe.

1.14 These levels of accuracy are not ideal but they would obviously help the police to some extent in tracking down terrorists, criminals, illegal immigrants and missing persons.

1.15 Several services offered by the mobile phone network operators rely on accurate location-detection and consumer demand may drive the search for greater accuracy.

1.16 This architecture may be presented as making effective and imaginative use of modern technology.

1.17 It offers an ID card unlike any ID card ever proposed in that it not only identifies the holder but also tracks him.

1.18 It is revolutionary in another way. Mobile phones have been paid for by the users. The cost does not appear in the national accounts. This could be a case of a successful PFI.

1.19 Paying a fortune to Accenture, by contrast, and giving everyone yet another plastic card may not be seen as a good use of taxpayers' money. (In this connection, note that digital certificates could allow us to empty our wallets of credit cards, cashpoint/cheque cards, loyalty cards, library cards, AA membership cards, business cards and, maybe one day, cash.)

1.20 There are problems. Of the mobile phones in use, many are "prepays" and no personal user details are registered with the mobile phone network operators. Many others are bought by public and private sector organisations in bulk for use by their employees in the same way as company cars and with the same problem – the registration and insurance details name the organisation, not the user. That makes it harder for the police to associate these mobile phones with individuals.

1.21 The solution to the registration problem suggested here is that legislation should be passed to change the mobile phone network handshake protocols. While the phone is in an unregistered state, handshaking should allow it to:

- ... associate with the network ...
- ... be tracked ...
- ... receive a digital certificate which would have the effect of registering it but
- ... not otherwise be used for voice, text or other messaging.

1.22 If the change to handshaking cannot be achieved, then some more pedestrian changes could be considered requiring identification to be registered when people buy and upgrade mobile phones.

1.23 For overseas visitors, the digital certificates which allow them to connect to their own mobile phone networks should generally be recognised as suitable by the networks in this country.

1.24 Many of these suggestions rely on international co-operation and may promote it.

1.25 Travellers who today require visas to enter the UK could in future receive their visa in the form of a digital certificate, which would allow them to connect to the UK mobile phone networks until they leave. If they stay beyond the term of their visa, the digital certificate could automatically identify that fact and the mobile phone could help to track them down.

1.26 The same technology could:
- Both identify people who are only allowed to spend a certain number of days in the country before they have to pay UK tax on their overseas earnings ...
- and it could count the days.

1.27 People would face problems if they lost their mobile phone or it was stolen. They face problems now if they lose their passport or their credit cards. In future these problems could be minimised.

1.28 Nokia, for example, already have a service called "Mobile Personality". People could store their digital certificates with some trusted supplier like this. When the person's phone is lost or stolen, the trustee could be contacted to get the original certificates revoked and to get new ones issued. The trustee could then download the replacement certificates to the person's replacement mobile phone.

1.29 There may anyway be less incentive to steal mobile phones if the digital certificates stored on them are revoked when the theft is reported so that the phones can no longer be used to make or receive calls.

1.30 Mobile phone operating systems will need to be enhanced. Facilities will be needed to:
- ... receive and store digital certificates ...
- ... transfer certificates from one phone to another ...
- ... manage several certificates for one person on one phone and
- ... manage certificates for several people on one phone. That would allow parents to store certificates for their children on their phone in the same way as they can currently have their children listed on their passport. This may be compared to the multiple identity facilities on email clients.
- ... sign messages with a digital certificate ...
- ... encrypt messages ...
- ... warn the user in good time when digital certificates are near expiry and
- ... revoke digital certificates.

1.31 Most people will not understand the number theory behind PKI.

1.32 An education programme will be needed to teach people how to use digital certificates.

1.33 There are several legal issues involved. Location records, required for tracking, will be stored on the mobile phone network operators' databases. Is it legal to link Passport Agency, DVLA, Department of Work and Pensions, Inland Revenue and network operator databases together in one entitlement portal? What about the privacy issues and civil liberties? Do the network operators keep location records? If not, can they be obliged to?

1.34 The scope of the entitlement card system needs to be narrow to start with and to expand only gradually. Otherwise, it will drown in deployment issues. It may be best to start by deploying new equipment in libraries, cinemas and pubs, for example, before trying to upgrade every border crossing in the world.

1.35 And then there are the people, perhaps 30% of the UK population, who do not have a mobile phone. Their number may be slightly reduced by offering them cheap, recycled mobile phones but, in the main, they will have to be issued with material entitlement cards.

1.36 These cards, it is suggested, should have the facility to store digital certificates so that the same identification procedures can work for card users as for mobile phone users.

1.37 It is suggested that more and more organisations will become Registration Authorities. They will be swayed when they see the security and convenience of issuing digital certificates as opposed to plastic cards.

1.38 As a result, more and more transactions will require digital certificates. That will cause card users to carry their material ID cards around with them. And that will make it worth fitting their cards with a GPS receiver and a (re-chargeable?) power source. They, too, can then be tracked.

1.39 The emphasis on tracking in this proposal results from the assumption that it would help to improve crime clear-up rates. That assumption may be false. It may be that the police can already track mobile phones and that clear-up rates are low all the same. In that case, less weight would be put on the importance of tracking facilities.

1.40 The widespread use of digital certificates, however, will remain important and would still be advocated. If no-one can forge an individual's digital certificate, then no-one can steal his identity for long without his knowing.

1.41 And locating digital certificates on mobile phones, thus turning them into ID cards, would still be a big and original idea, which is commended to the Home Office as a lower risk way to achieve its objectives.

2 MISCELLANEOUS BACKGROUND

2.1 It is an observable fact that mobile phones are evolving into ID cards. Not for everyone, certainly, but some people feel bereft if they leave home without their mobile phone. Children, in particular, identify with their phone. It seems to make some sort of a statement about them. Most people find the mobile phone convenient most of the time and have come to rely on it to some extent. If you know where their mobile phone is, you know where they are.

2.2 People are willingly buying videophones with decent quality graphics screens and built-in cameras – just the sort of equipment needed for passport-type applications. Perhaps they would agree to have their photograph taken when they buy a videophone. The photograph could be transmitted to the mobile phone network operator together with other registration data needed to activate the phone. It could also, perhaps, be stored in the SIM of the mobile phone with a view to reducing the level of mobile phone theft, currently running at 700,000 units p.a.

2.3 Does PKI work? PGP is a PKI system. The following quotation is taken from the user's guide to *PGP Desktop Security*, p.246:

> “If all the personal computers in the world – 260 million – were put to work on a single PGP-encrypted message, it would still take an estimated 12 million times the age of the universe, on average, to break [that] message.”
>
> William Crowell, Deputy Director, National Security Agency, March 20, 1997.

2.4 PKI is already widely in use wherever authenticity and confidentiality are essential. The military and the security services are heavy users as are big businesses. BT, for example, issues its suppliers with digital certificates so that they can trade on the BT extranet. The rest of us are using PKI whenever we buy something on a secure website, prefixed "https" as opposed to "http".

2.5 Different levels of trust are placed in different Registration Authorities. The level of trust in a well-known and long-established Registration Authority such as the Passport Agency with strong checking procedures would be high. US Immigration would be more inclined to take account of a digital certificate issued by them than one issued by, say, the Wimbledon Swimming Club. The Swimming Captain, on the other hand, may be more interested in the latter.

2.6 All digital certificates have a value to someone. There are tangled cross-connections between the interests of all Registration Authorities. At the heart of PKI is a "web of trust" concept, which the Home Office may find helpful in explaining and promoting an entitlement card scheme based on digital certificates.

2.7 Will digital certificates work on mobile phones? There are references on the Nokia, Ericsson and Motorola websites to WAP applications using digital certificates.

2.8 The author has researched the question extensively whether the idea of using mobile phones as ID cards is original. Not out of vanity alone. If the suggestion is unique, some reviewers may unfortunately see it as eccentric science fiction.

2.9 The only reference found so far connecting mobile phones and ID cards is an almost opaque press release on the Finnish eGovernment website, (see http://e.finland.fi/netcomm/news/showarticle.asp?intNWSAID=9333):

> **Finland: Electronic identification to mobile phone**
>
> **eGovernment news**
> Helsinki, 16 October, 2002 (Esmerk) — The Finnish Population Register Centre is preparing a future electronic identification, possibly available in spring 2003. The mobile phone identification will be combined with the SIM card of a mobile phone, and it can be used for electronic signature. The project aims at enhancing electronic services and trade.
>
> Operators will also start to offer mobile phone identification. The state of Finland and private companies aim at extensive usage of different identification systems in federal and private on-line services.
>
> The Population Register Centre will publish its project towards the end of 2003. Chief manager Ritva Viljanen says that mobile phone identification will become more common the more benefits it presents. There has to be enough usage for the system.

2.10 The BBC News website carried a report on 20 December 2002 that the UK police and Customs officers made nearly 500,000 requests to mobile phone network operators in 2002 for call information, see http://news.bbc.co.uk/1/hi/uk/2592707.stm. The value of mobile phones in detection is clearly recognised.

2.11 Unfortunately, not only by the police. The following quotation is taken from the National Criminal Intelligence Service (NCIS) *Threat Assessment 2002* report, see §2.38:

> In choosing telecommunications products and services, criminals are guided by the need for security, anonymity and convenience. They remain keenly aware of new products and services and take advantage of any that enhance these three features. Mobile phones, in particular prepays, are particularly popular, since there are no legal requirements for registering them and so no need to reveal any personal details. They are also inexpensive enough to be bought in bulk and regularly changed. Organised criminals also make use of telephone kiosks, foreign roaming mobiles (also available as prepay) and satellite phones.

2.12 Does biometrics work? Identix sell equipment which can scan a human face or a photograph of a human face and store metrics to identify it uniquely in only 84 bytes of memory, see http://www.identix.com/newsroom/face_ts.html. Their database can compare a single faceprint, against all the others stored, at the rate of 15m per minute. You could be picked out from the entire population of the UK in a maximum of about four minutes.

3 ABOUT THIS SUBMISSION

3.1 Who does this submission come from? David Moss (48), the author of the proposal and Business Consultancy Services Ltd (BCSL) are one and the same. The BCSL website at http://www.bcsl.pwp.blueyonder.co.uk includes a CV.

3.2 The author was researching the location-aware services of 3G mobile phones as part of an MSc course at Kingston University when he developed the idea of mobile phones evolving into ID cards. This, in turn, led to the idea of using mobile phones for crime detection and the feasibility of a service called "AppealNet".

3.3 The idea behind AppealNet is to collect evidence when the police are having trouble getting witnesses to come forward after an incident. The New Year's Eve shootings in Birmingham are a particularly nasty example.

3.4 A search of the mobile phone network operators' records could reveal who was in the vicinity of the incident and these people could be contacted by phone and asked to submit evidence. They could do so by phone or by email or in person at a police station or using the web and a prototype website has been developed, see http://www.bcsl.pwp.blueyonder.co.uk/AppealNet[1].

3.5 AppealNet may be compared to the TV programme, Crimewatch, and to the UK police appeals website, http://www.police.uk/appeals.html. They are examples of "pull" technology. You have to watch the programme or log on to the website to see the appeal. AppealNet is an example of "push" technology. The subjects are contacted out of the blue.

3.6 The AppealNet website is still unfinished and in a primitive state, not least because the author discovered the related Home Office request for submissions on the entitlement cards system on the same day as the deadline, 31 January 2003. This led to hasty email submissions being sent that moment. The present submission is meant to amplify those emails.

3.7 The author is keen to pursue these researches and, if they meet with any interest, to do so in collaboration with the Home Office and on a paid basis. A separate proposal will be sent to NCIS. The objective is to help to establish the entitlement cards and AppealNet projects and to deliver working systems.

[1] Use mobile phone no. 12345 123 123 and incident no. 12345 123456.