TO RT HON JOHN REID MP

DEMATERIALISED ID
THE VOLUNTARY ALTERNATIVE TO MATERIAL ID CARDS

A PROPOSAL BY DAVID MOSS
OF BUSINESS CONSULTANCY SERVICES LTD (BCSL)

ABSTRACT

Dematerialised ID is BCSL's counter-proposal to the UK government's proposed ID card scheme, which may or may not be deployed in eight years time in 2013. Critics of the tawdry scheme devised by the Home Office and their advisors are two-a-penny. Fewer people will have lobbied the government, the Home Office, the Home Affairs Committee and others with a well worked out alternative, based on more than two years of research, as BCSL have done.

Opposition to the government scheme is spread along a spectrum ranging from it-won't-work at one end to it-will-work-only-too-well at the other. BCSL is firmly on the left of this spectrum – the scheme will not work, a lot of money will be wasted and people's hopes are being falsely raised.

Dematerialised ID is designed to assist with the fights against crime and terrorism. It is designed to expand the economy and to manage civil liberties. It is an identity voucher scheme which uses reliable and established technologies to deliver these benefits effectively, acceptably, quickly and cheaply.

If the government ignore dematerialised ID, then they will miss a valuable opportunity and they will waste billions of pounds of taxpayers' money. In summary:

- The expectations of biometrics have been raised to unsustainable heights. The technology is not ready yet, it cannot support the weight of these ingenuous expectations. For the moment, deploying biometrics, which the government ID card scheme relies on, is an expensive charade. The same applies to biometric passports.
- If the technology becomes reliable, then biometrics should be stored on mobile phones, not on separate smart cards, which are expensive, old-fashioned and underpowered compared with mobile phones. A mobile phone is the perfect ID voucher: you voluntarily take your mobile phone with you everywhere you go; not only does the phone identify you, it also locates you and identifies your associates. And mobile phones are here now. We do not have to wait for eight years.
- People knowingly and voluntarily buy mobile phones. The civil liberties problems of dematerialised ID are therefore arguably neutralised.
- That is not a reason to ignore these problems and dematerialised ID indicates where action needs to be taken to safeguard our privacy.
- Not quite everyone has a mobile phone and so an ID voucher scheme like dematerialised ID, based on mobile phones, will not be universal. Neither is the government's proposed scheme universal. It is a naïve mistake to aim for a single universal scheme. The BCSL proposal is that dematerialised ID should be one scheme among many intersecting independent schemes which, between them, tend towards universality.
- With expectations lowered to a realistic level, the budget can be lowered commensurately.

OUTLINE

MOBILE PHONES & CIVIL LIBERTIES

1. The current intermittent debate about ID cards – should we or shouldn't we have them in the UK – is fatuous because it is too late. Between 80 and 90% of us already have an ID card in the form of our mobile phone.

2. This has not gone unnoticed by the police and HM Revenue & Customs. They make requests for location and timing information from the mobile phone network operators at the rate of one per minute, every minute of the year.

3. The Identity Cards Bill requires the deployment of a new national network of ID card readers and biometric verification equipment at airports and seaports, in police stations and benefits offices, banks, hospitals and GP surgeries, perhaps schools and universities and who knows where else? Churches? Pubs?

4. We cannot keep referring to this network as the "national network of ID card readers and biometric verification equipment". No shorter name has been provided by the Identity Cards Bill. BCSL suggest that it should be referred to as "IDNet".

5. No-one knows how many billions IDNet will cost, it is not included in the Home Office's July 2002 budget for the ID card scheme. What we do know is that it is unnecessary. We already have five mobile phone networks up and running in the UK.

6. This objection – that IDNet would be expensive and is unnecessary – applies to any ID voucher scheme based on new smart cards, not just the government's proposed scheme. The London School of Economics (LSE), for example, have published a proposed alternative scheme, which also relies on new smart cards. Just like the government scheme, it would therefore require an expensive and unnecessary IDNet.

7. Recall the problems of government contracts let to Accenture/Arthur Andersen, EDS, Siemens, Capita and other IT services companies. It is not obvious that the Home Office is capable of creating and operating the proposed National Identity Register database. Dematerialised ID

would reduce the project risks by taking advantage of the databases already created and maintained by the mobile phone network operators and other organisations.

8. Should we trust the private sector to create and maintain the National Identity Register? It is too late to ask this question. They have already created it. It is not obvious that we should trust them any less than the public sector. It is the public sector, after all, which suspended UK passport controls at Waterloo station on the Eurostar service and allowed Hussain Osman, one of the 21/7 would-be bombers, to escape thereby from the UK to Italy. (And it is the private sector mobile phone network which helped to catch him subsequently.)

9. The Home Office's proposed scheme will not be deployed until 2013, whereas mobile phones and the associated infrastructure of databases and telecommunications equipment and retail outlets are already with us. There is no need to wait eight years before addressing what the government say is the unprecedented security threat of Al-Qaeda terrorist attacks.

10. It may not be unprecedented, indeed that seems historically inaccurate, but if the government believe that it is, then, by their own logic, it is odd to wait eight years. Either an ID voucher scheme will make an important contribution, in which case the sooner the better, or it will not, in which case, why bother?

11. 80 or 90% is not 100%. The government scheme is called "universal" but it only applies to those aged 16 and over, it will have trouble including many people whose biometrics cannot be registered, it will exclude overseas visitors staying for less than three months and there have been suggestions that the elderly will not be forced to have ID cards. Dematerialised ID would similarly tend to exclude the elderly, who often do not like using mobile phones. On the other hand, it could include all the under-16s and all the overseas visitors who have mobile phones and it does not rely on biometrics. Neither scheme covers the whole universe.

12. And why should they? Why should an ID voucher scheme cover everybody? A genuinely universal scheme would tend to become the single repository of authenticated identity. It would provide a single point of attack. Evolution and free market economics both teach us that safety lies in plurality. We already have several ways to establish identity, it is not a new problem. Multiple intersecting independent schemes are safer and can cover the whole population between them without any single scheme having to be universal.

13. The government have advanced several reasons for introducing ID cards. The emphasis keeps changing. ID cards were meant to provide an alternative to passports when visiting European Economic Area countries. That objective has now been dropped. At one stage, counter-terrorism was specifically downgraded as an objective of the government scheme, which was meant rather to provide an emblem of citizenship. Now counter-terrorism and the fight against crime are advanced as major reasons for introducing the scheme. These are two admirable and popular objectives.

14. Compulsory ID cards did not stop the Madrid railway bombings. A mugger pointing a knife at you remains a threat even if he is holding his ID card in the other hand. No statistics have been presented to show that crime is lower in countries which have ID card schemes. Even if crime is lower in these countries, is it because of the ID cards or something else? We do not know. Do the Home Office know?

15. The government admit that ID cards will not eradicate crime or stop terrorism but state that they will at least impede criminals and terrorists. It is not clear how their proposed scheme will achieve even that.

16. It is clear how dematerialised ID, with its use of mobile phones, would impede criminals and terrorists:

- From this point of view, mobile phones are the ideal ID card. They identify people. Call 123 1234 1234 and you get David Moss. People naturally carry their mobile phone with them wherever they go. Whenever their phone is switched on, people can be located accurately, often to within 50 metres, wherever they are in the world – the mobile phone network is global. The network operators' records show where a person is and where they have been. And they show who the person calls and who calls them.
- Terrorists and criminals who do use mobile phones can be tracked and their associates identified. That is a serious impediment. Those who do not use them will also be impeded in their pursuits, they will be deprived of a very convenient method of communication, which is surely all-important in co-ordinating crimes and terrorist attacks.

17. Dematerialised ID succeeds in achieving these objectives without making everyone feel as though they are under suspicion. Innocent people volunteer to pay for mobile phones because they are useful. They will not so readily volunteer to pay £93 (the Home Office's latest estimate) for an ID card.

18. Mobile phones track you and identify your associates. People know this. It is openly reported in the press how people are located and how alibis are checked by reference to mobile phone records. Anyone looking at their monthly bill can see that there must be a set of databases somewhere which records all the numbers dialled.

19. People know this and yet they still voluntarily use their mobile phones. Perhaps even civil liberties campaigners use mobile phones; certainly there is no civil liberties campaign in the UK against the use of mobile phones for surveillance.

20. Arguably, this neutralises the civil liberties issues raised by dematerialised ID. People have knowingly elected to forgo their privacy in exchange for the utility of the mobile phone.

21. Perhaps, even so, people should be protected from themselves. BCSL has identified the *locus* of the civil liberties problem, four databases maintained on each mobile phone network, the HLR (home location register), the VLR (visitor location register), the EIR (equipment identity register) and the AuC (authentication centre).

22. The HLR and VLR databases record where your phone is, *prima facie* evidence for where you are. The EIR records details of all mobile phone handsets, supports billing and allows stolen handsets to be barred. The AuC uses encryption techniques to authenticate handsets and other network equipment so that, for example, criminals cannot set up spoof networks.

23. Regulate who has warranted access to these databases and you can manage civil liberties, people can be protected from themselves.

24. The government's Bill allows visiting terrorists a three-month period of grace to case the joint before they have to apply for an ID card. Thanks to its use of mobile phones, dematerialised ID would impede their activities, wherever they are in the world, as long as they are making

a call from a mobile phone or to a mobile phone whose location is recorded on any of the UK HLRs or VLRs.

25. £2bn of the government's incomplete budget for the ID card scheme (as at July 2002) is for the smart cards alone. People will not voluntarily carry smart ID cards with them wherever they go, smart cards will not generally help to locate people and they will not identify who people associate with. Use the mobile phones people have paid for anyway and not only do you save £2bn but you also get a more effective ID voucher and you know where to concentrate your efforts to manage civil liberties.

26. The high rate of mobile phone theft in the UK is a problem for dematerialised ID. The network operators have it within their power to make a stolen phone useless. If any operator does not use that power, then it is suggested that a case be brought against them accusing them of being accessories after the fact. More stolen phones will soon be made useless and the rate of theft will fall.

27. Mobile phone loss and theft are problems which need to be managed. In that, they are not unique. The loss and theft and counterfeiting of the government's proposed ID cards would also need to be managed.

28. Stating baldly that the mobile phone is a voluntarily adopted electronic tag makes dematerialised ID sound nasty. The government's proposed ID card scheme seems cuddly by comparison. That is an index of how ineffective it is.

29. The global mobile phone network is here with us now. It is not going to go away. The great strength of the network is that it creates in the mobile phone a more effective ID voucher than could ever previously have been feasible. Your mobile phone identifies you, locates you at all times and identifies your associates. This great strength is also a great danger to civil liberties. That will remain the case whether or not the Identity Cards Bill is enacted. The Bill is in that sense an expensive diversion from the real ID voucher scheme.

30. If the government will amend its scheme to rely on mobile phones rather than new smart cards, then attention will at last be drawn where it is needed, to the already pressing question how to regulate the mobile phone network operators in such a way as to protect our civil liberties.

EMPOWERMENT

31. Deploying IDNet – installing and maintaining the terminals required – will be an expensive and complicated project. No sensible project manager genuinely interested in the success of the project would take on the risk of creating this new, national network, not when there are already five mobile phone networks available.

32. The IDNet terminals would be in fixed locations. This would be inconvenient compared with a mobile phone, which you can use more or less wherever you are. The terminals would be subject to breakdown and to vandalism. The cost of installing and maintaining them is unbudgeted and would fall on public and private sector organisations like another stealth tax.

33. Dematerialised ID is different. In dematerialised ID, the handset is the terminal.

34. Mobile phone handsets are portable computers (power source, processor, memory, operating system, software applications, keyboard, screen, microphone, speaker, video, ...) with built-in te-

lephony, messaging and networking facilities. The networking facilities include dialled connections, which you have to pay for, and infra-red and Bluetooth connections, which are free. It is hard to imagine a device better adapted to the mass deployment of IT systems. Mere smart cards are miserably under-powered by comparison.

35. Consider the case of disabled people. EU recommendations specify a network of specially adapted terminals for the disabled with "sound to augment poor sight capability", "enhanced graphics [for those with] poor aural capability", "user profiles held on the smart card [to] allow the terminal to adapt differently to different user requirements", two pairs of screens and keyboards at each terminal, the lower pair being for wheelchair users or perhaps a single pair "on a motorised stand".

36. In a country where vandals smash bus shelters, people put chewing gum in parking meters for fun and we can't even make the trains run on time this is manifestly unrealistic.

37. It is also unnecessary. The text facilities of mobile phones make them ideal communication devices for deaf and dumb people. Voice synthesisers can be fitted to handsets so that text on the screen can be read out to blind people. Wheelchair users can hold their handset to their ear at whatever height it happens to be at the time. Anyone who cannot use a mobile phone as required by dematerialised ID is probably not going to be able to use the ID card and terminals required by the government scheme.

38. Disabled people, like everyone else, are more likely to be shackled by schemes which rely on fixed location terminals and more likely to be empowered by dematerialised ID.

BIOMETRICS

39. The government want to include biometrics on their ID cards at a budgeted cost of £0.7bn (as at July 2002). Once again, the budget figure gives an incomplete picture. The proprietary technologies used will attract royalties, payable every time anyone anywhere uses their ID card. We do not know the value of these royalties any more than we know the cost of IDNet.

40. The hope is that a biometric can be found which, throughout their life, identifies each person uniquely in a practical way such that, for example, a Jumbo jetful of people can be whisked quickly through the arrivals procedures at an airport while confirming each passenger's identity.

41. The biometric that people trust is DNA. DNA evidence is admissible in court and it is trusted by our ex-Home Secretary. Unfortunately, DNA tests take too long to meet the requirements above.

42. Three apparently more practical biometrics are under consideration – facial geometry, irisprints and fingerprints.

43. In trials conducted on behalf of the United Kingdom Passport Service (UKPS), facial geometry successfully verified identity a few minutes after registration only 69% of the time for able-bodied people and only 48% of the time for disabled people. Fingerprints verified identity successfully only 80% of the time. Irisprints were successful 96% of the time for able-bodied people and 91% of the time for disabled people, which is better than fingerprints, but only 90% of able-bodied people could be registered in the first place – as far as irisprints are concerned, 10% of able-bodied people do not exist and that figure rises to 39% for disabled people.

44. Suppose that 330 able-bodied people buy tickets for a long haul flight. Using the statistics above, 33 of them will not get as far as the Departures lounge, having been unable to register their irisprints. And what is going to happen at the Arrivals desk? Facial geometry will wrongly require 93 of them to be sent home, fingerprints will wrongly require 60 of them to be sent home and irisprints 12. Up to 198 of the original 330 ticket-holders – 60% of them – will be victims of the registration problems and the false negatives of biometrics. How many false negatives should there be? None. Biometrics are not ready to be relied on.

45. The Home Office describe this unacceptable performance as "teething problems". That is an inordinately lenient judgement and the panglossian response of Mr Tony McNulty MP is not businesslike: "… there are difficulties with the technology … not least with people with brown eyes ... none of these problems are new, but increasingly as biometrics are more and more used ... we think the technology can only get better and better and better …". Given that today's biometrics cannot verify identity with anything like adequate confidence, the only prudent and businesslike option is to delay any deployment of biometrics until they can be relied on.

46. The National Physical Laboratory (NPL) were commissioned by the Home Office to study the feasibility of these three biometrics. Their terms of reference were to calculate the probability that any of these biometrics could identify a person uniquely in a population of 50m, the likely number of UK ID cards in circulation. Given that UK residents travel abroad and overseas residents visit the UK, it might be argued that the real test is to see whether biometrics can be used to identify a person uniquely in the world population of 6.4bn.

47. The NPL's findings are in line with the UKPS trial results above:

- Biometrics based on facial geometry do not work. This conclusion of theirs is unqualified. "Even under relatively good conditions, face recognition fails to approach the required performance", they say, and "facial recognition is not a feasible option". The Commissioner of the Metropolitan Police confirms that biometrics based on facial geometry are unlikely to be useful.
- Unlike facial geometry, irisprints almost never say that Person B is Person A (false positive), but too often they say that Person A is not Person A (false negative) and too often people cannot even register their irisprints in the first place.
- With many reservations, fingerprints might work if at least four and preferably all 10 prints are registered on enrolment into the scheme.

48. Some of these are major reservations. For example, the registration work must be done properly, by an organisation which is trusted – the one-legged Romanian roofer *débâcle* which led to the resignation of Beverley Hughes from her Home Office post does not inspire confidence. And the fingerprinting method chosen will produce prints which are not admissible as evidence in court: these are not the fingerprints the public know and trust after 100 years of experience, rolled prints taken by police experts using ink; the chosen fingerprinting method is arguably no more than a glorified photocopy of people's fingers ("fingercopies").

49. The evidence given by David Blunkett to the Home Affairs Committee suggested that computers could use biometrics to deliver conclusive decisions about identity with mathematical certainty. That raises the level of expectations.

50. The Commissioner of the Metropolitan Police has confirmed that biometric identification needs to be "almost perfect" if ID cards are to achieve their objectives. The NPL report reveals that, far from perfection, all that can be delivered is a probability that a given person is who he

says he is. The evidence of biometrics trials suggests that this probability is too low to support conclusive decisions. That is the state of the art. Biometrics do not provide the basis for a reliable ID voucher scheme.

51. When biometric equipment at an airport, say, indicates that a passenger's identity is suspect, that passenger will have to be investigated. There is a limit to how many investigations can be carried out by the given number of staff on duty. The tolerance levels on the biometric equipment will have to be set to suit the number of staff. That is a far cry from the offer of conclusive identification. The level of expectations with respect to biometrics in particular and to ID voucher schemes in general needs to be lowered.

52. The LSE's alternative to the government ID card scheme relies on biometrics. It must therefore be subject to the same problems as the government scheme – biometrics are not yet reliable enough to identify people – and it is therefore not a viable alternative.

53. The members of the International Civil Aviation Organization (ICAO), including the UK, have agreed unanimously, in the Berlin Resolution, that all passports should in future include biometrics based on facial geometry.

54. The Berlin Resolution says "ICAO TAG-MRTD/NTWG endorses the use of face recognition as the globally interoperable biometric for machine assisted identity confirmation with machine readable travel documents". But facial geometry is the least reliable biometric of all, it is a waste of money. Far from forcing the Home Office, as they suggest, to introduce biometric passports and ID cards, the Berlin Resolution surely needs to be reconsidered.

55. The Berlin Resolution also says: "ICAO TAG-MRTD/NTWG further recognizes that Member States may elect to use fingerprint and/or iris recognition as additional biometric technologies in support of machine assisted identity confirmation". That is "may elect to", not "are forced to".

56. The ICAO list 13 considerations behind their reasoning in favour of the Berlin Resolution, including the following: "facial photographs do not disclose information that the person does not routinely disclose to the general public"; "it does not require new and costly enrolment procedures to be introduced"; and "[facial geometry] can be captured from an endorsed photograph, not requiring the person to be physically present".

57. The Home Office are certainly not being forced by the ICAO to introduce an expensive system of compulsory attendance at a national network of 2,000 biometric registration centres where people will have their fingerprints taken like criminals in order to obtain a UK passport. That is their own initiative.

58. The Home Office's May 2005 *Identity Cards Briefing* document includes several more of these unconvincing arguments for introducing biometric passports:

- They cite the US-VISIT scheme in the US as a reason for registering everyone's fingercopies on biometric passports. US-VISIT has its own problems, discussed below. Suffice to say here that there is no point, for the US or for the UK, introducing a scheme which will fail to verify the identity of 20% of visitors to the US.
- They cite the EU's decision to record facial geometry and fingercopies on passports issued by members of the Shengen area. This does not alter the fact that facial geometry is useless and fingercopies are unreliable. Further, the UK is not in the Shengen area.

- They cite the EU decision to move towards introducing the same unreliable biometrics based on facial geometry and fingercopies on residence permits and visas issued to Third Country Nationals. The relevance of this point is unclear. UK citizens are not Third Country Nationals.
- They mention the existing practice in the UK of recording fingerprints on the Application Registration Cards (ARCs) issued to asylum seekers. But these are proper rolled prints, taken by fingerprint experts, admissible as evidence in court, unlike the fingercopies envisaged for UK citizens.

59. The attempt is being made to use these poor precedents as cover for the introduction of ID cards. We have to do so much work anyway to abide by the Berlin Resolution and the other initiatives above that we might as well, it is argued, spend just the little bit extra which is needed for ID cards.

60. This cockeyed reasoning based on marginal costs was used by David Blunkett, when he gave evidence to the Home Affairs Committee, to suggest that the cost of an ID card would be only £4. He went further and argued that the cost of ID cards is tiny if you look at it on an annual basis. The Home Office's July 2002 budget covered a 13-year period. Of course if you divide any positive number by 13, then you get a smaller number. 13 times smaller.

61. You still have to pay the whole bill and that is rising fast. In July 2002, the Home Office estimated the budget for ID cards, covering three years of development work and the first 10 years of operation, to be between £1.318bn and £3.145bn. Their latest estimate is £5.8bn. The LSE estimate it to be between £10.6bn and £19.2bn, more like £157-£286 per card than £4 per card.

62. The budget for passports is being confused with the budget for ID cards. One minute the focus is on the whole budget, next it is on the marginal cost. One minute the focus is on the whole budget, next it is on just one year's worth.

63. These tricks with budgets cannot disguise the fact that the NPL's findings and many other reports confirm that biometrics based on fingercopies and irisprints are unreliable and biometrics based on facial geometry are useless. That means that biometric passports are unreliable and useless. The Berlin Resolution should be renegotiated. It is a separate case of money being wasted. It does not provide cover for the introduction of ID cards and neither do the other precedents.

64. In email correspondence with BCSL, the NPL have confirmed that they were surprised at their findings when they investigated biometrics for the government's feasibility report. They were surprised how poorly the biometrics performed. So much so that they felt it necessary to include in their report the results of investigations by other organisations, who had recorded even worse performance, so that it would be clear that the NPL's own findings were not freakish exceptions.

65. If biometrics are unreliable and useless, then there is no point building and maintaining and staffing a national network of biometric registration centres. There is no need to pay royalties to the suppliers of proprietary biometric technology. And there is one less excuse to waste everybody's time with interviews which require attendance in person to get a passport.

66. If biometrics are unreliable and useless for passports, then they are unreliable and useless for ID cards. If biometrics are unreliable and useless in the UK, then they are unreliable and useless in the rest of the EU and in the US and everywhere else where they are being considered or being

adopted. The argument that other countries are relying on biometrics and therefore the UK has to rely on them does not hold water. This emperor has no clothes.

BIOMETRICS & DIGITAL CERTIFICATES

67. The ICAO say that there is no point recording biometrics on passports if they can be changed by forgers. They recommend that the established technology of the public key infrastructure (PKI) should be used to authenticate these biometrics.

68. PKI is all about authentication. It was developed by GCHQ in the early 1970s and independently and slightly later in the US. It is a technology used every day by governments, the military, the security services, academic institutions, businesses and secure websites, among others, to authenticate whatever needs to be authenticated.

69. The revolutionary element of PKI is that the key required to encrypt a message can be published, it is a public key. You can use my public key to encrypt a message and send it to me secure in the knowledge that only I can read it, because only I have the private key needed to decrypt it.

70. PKI involves multiplying very large prime numbers together to produce even bigger numbers. The security of PKI depends on the difficulty of factorising these even bigger numbers. This means that PKI is vulnerable to advances made by mathematicians in the study of factorisation. There is no sign of any such advances being made. It is also vulnerable to the advent of quantum computing. There is no sign of sufficiently powerful quantum computers becoming available but, for when they do, quantum authentication techniques at least as effective as PKI have already been worked out by mathematicians and physicists.

71. As long as this remains the case, according to the US National Security Agency (NSA), commenting in 1997 on PGP, one of many PKI software packages: "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 a single message".

72. The mathematics of PKI is hard for most of us to grasp. The attempt may be made to explain it to those who are interested but all that is needed in general is to promote the same attitude to PKI as we already have to DNA. Very few people understand how it works but most people believe that it does its job.

73. When a message is sent from one person to another using PKI, as long as established procedures are followed, the sender, the recipient and the message itself are all authenticated. The sender can be sure that only the intended recipient will be able to read it, the recipient can be sure that the message comes from the purported sender and he can tell if it has been tampered with *en route*.

74. Functionally, your stored biometric on an ID voucher would be a message from the authority operating the National Identity Register, to whom it may concern, affirming that you are you. Use PKI, and it would be evident if a forger had tampered with the biometric since it was issued.

75. We cannot keep referring to this organisation as "the authority operating the National Identity Register". No shorter name has been provided by the Identity Cards Bill. BCSL suggest that the authority should be called the "UK Registration Authority" or "UKRA" (apologies to the United Kingdom Rocketry Association, the United Kingdom Reading Association, the UK Reiki

Alliance and any other UKRAs, many of them Ukrainian). Registration authorities, like certification authorities and revocation authorities, are components of the PKI, so the name is conventionally correct.

76. The set-top boxes people attach to their TVs to receive satellite and cable TV programmes have a card in them to authenticate the user as a *bona fide* customer of Sky, for example, or Telewest/blueyonder. There is a grubby market in illegitimate cards, which allow people to receive these programmes without paying. Without PKI, there will be the same market in ID cards.

77. This could explain why we have yet to see a single bank, for example, say that they will accept a government ID card as proof of identity. Will the UK government underwrite their ID cards as the Finnish government do theirs? If not, why should the banks rely on them? And if the banks will not rely on them, then why should people pay for them? Bank acceptance is a crucial litmus test for ID cards.

78. The government argue that, because biometrics are unique, ID cards cannot be forged. There is considerable doubt as noted whether a practical, unique biometric can be found. Even if it can, the argument is confused:

- If all verification of identity were conducted by checking people's biometrics against the National Identity Register, then there would be no need to have ID cards.
- If we do have ID cards, then biometric uniqueness will not make them secure against forgery. A forger could overwrite Person A's unique biometric with Person B's unique biometric. The biometric is still unique but the ID card is now a forgery. PKI is needed to protect against this sort of forgery and that is why the ICAO recommend it.

79. So does every other informed system designer. The European Commission (EC), for example, funded the development of OSCIE, the Open Smart Card Infrastructure for Europe, a generalised specification of ID voucher schemes which relies centrally on PKI. This specification is being implemented in many EU countries. There is no controversy about it. PKI is there, it works, it is natural to use it and it is essential for authentication.

80. The UK is unique in not recognising the central importance of PKI. BCSL was told in a telephone call with the Home Office that "the British public is not ready for PKI". The Identity Cards Bill makes no mention of PKI. Without PKI, our ID cards will be expensive and worthless and IDNet will itself pose a security threat.

81. The stock in trade of PKI is the digital certificate. Private keys and biometrics can be digitised, encrypted and recorded in a digital certificate. Digital certificates can be stored on any digital medium. That may be a smart ID card – as the government propose – or an MP3 player, a digital camera, a PDA (personal digital assistant), a mainframe computer, a PC or a laptop, for example, or a mobile phone – as proposed for dematerialised ID. Mobile phone operating systems and PC-based email clients such as Outlook Express already have facilities to manage digital certificates. There is nothing new about PKI, the technology is ready.

82. If a suitable biometric can be found, then BCSL's suggestion is that UKRA should transmit digital certificates containing their biometrics to people's mobile phones:

- There are several advantages to this approach. It is quick and cheap and, in that sense, flexible compared with recording the biometric on smart cards, which you then have to post or courier to people. A voucher in the form of a digital certificate stored on a mobile phone can

be revoked simply by making a phone call, whereas a material voucher still looks to the naked eye as though the bearer has the associated entitlement, even if it has actually been revoked. And digital certificates do not wear out and need replacing the way smart cards do, even contactless RFID (radio frequency identity) cards.

- Smart cards can be intercepted in the post, as we are re-discovering with chip and PIN cards, and then used fraudulently. Digital certificates transmitted to mobile phones cannot be intercepted in the post, of course, they do not suffer from that problem but they can be intercepted in the air. The solution is simple. People must, *ex hypothesi*, attend an enrolment centre in person if they are going to have their irisprints and fingercopies recorded. They should attend with their mobile phone. The digital certificate can then be issued – activated or not – across a free, short range infra-red or Bluetooth link, preferably in a Faraday cage, thus avoiding the possibility of interception.

83. If, on the other hand, a suitable biometric cannot be found, then the biometrics component of the ID card scheme should be suspended. There is no point wasting £0.7bn.

84. There is a weak argument that biometrics have a deterrent effect even if they do not work. That is a very expensive bluff with diminishing returns.

85. We certainly do not want to get into the same position as the US. Despite spending a lot of money on biometric systems to check 100% of visitors to the US, the Department of Justice (DoJ), the State Department, the Department of Homeland Security (DHS) and the National Institute of Standards and Technology (NIST) cannot agree whether two fingercopies should be used for registration or 10. The DHS, with the support of the State Department, are currently using only two, there isn't time to take more at border crossings and ports, they say, whereas the NPL, the NIST and the DoJ all recommend registering a minimum of four fingercopies and preferably all 10.

86. At least the US are doing something, it may be argued. Are they? They may be spending the money and installing the equipment but what are they achieving, what results have there been, what risks have been reduced? Having set out to achieve 100% checks, the reality is that incompatibilities between different fingercopying systems mean that only 1% of visitors can be checked against FBI files.

DEMATERIALISE – CRIME & THE ECONOMY

87. Digital certificates are not material. That is what gives dematerialised ID its name. The principle is that public and private sector organisations alike should stop issuing material certificates and start issuing digital ones instead.

88. There is a successful precedent. Compare dematerialisation in the UK securities industry. We no longer have material share certificates. We still manage to invest in shares.

89. Dematerialised ID would have the effect of providing each subscribing member of the public with a collection of digital certificates from several sources, each one vouching for some entitlement. You might have one digital certificate issued by the Department of Work and Pensions (DWP) affirming your right to work, for example, another one issued by your union showing that you are a member, a third issued by the Department of Health certifying your right to treatment under the National Health Service, a fourth issued by your bank confirming your current account number and allowing you to write digital cheques, and so on.

90. In general, under dematerialised ID, any supplier who currently issues any material voucher which entitles the bearer to any benefit could, instead, issue a digital certificate to be stored on the bearer's mobile phone or his PC.

91. The Home Office's July 2002 budget includes £2.007bn for 67.5m sophisticated smart cards. ("Sophisticated" is undefined by the Home Office.) It follows that the cards cost £29.73 each.

92. This is the production cost alone. It does not include the cost of making checks on people's personal details. That is covered by other elements of the budget. It does not include the cost of registering or checking biometrics or the cost of card distribution.

93. With these volumes, the comparable cost for producing a digital certificate alone, no smart card required, is estimated by BCSL to be less than 1p, i.e. that component of dematerialised ID would be around 3,000 times cheaper than the government scheme. Digital certificates are cheaper in this case than material ones.

94. Compared with material certificates, it is quick and cheap to produce digital certificates, quick and cheap to distribute them and easy to revoke them. That makes it feasible to introduce the wide variety of certificates needed to reflect the sophisticated variety of requirements of our complicated lives. And thanks to the mobile phone network, these certificates can be remotely and continuously monitored and managed.

95. The principle of dematerialisation can be applied widely.

96. For example, suppose that visas were issued in future in the form of digital certificates and stored on each visitor's mobile phone. The mobile phone could monitor the visa locally and warn the visitor when it was running out, just as mobile phones already warn you when the battery is running out. Equally, UKvisas, the organisation which administers visas, could send text and/or voice messages to the mobile phone, in the language selected by the visitor, warning him or her that the visa was running out.

97. Some individuals are exempt from paying tax on their overseas income as long as they spend no more than a certain number of days per year in the UK. Dematerialised ID would allow HM Revenue & Customs to count the days spent in the country by reference to the presence of that individual's phone on any of the UK's mobile phone networks. It may be objected that the individual might simply leave his phone abroad in order to evade the count. But if the phone also stored his entry permit then he couldn't get into the country in the first place.

98. There is an active market in forged academic qualifications, for example, in forged FA Cup Final tickets and forged tickets to pop concerts. Replace the material exam certificates and the material football match and concert tickets with digital certificates and PKI can be used to promote authenticity.

99. Another example, cheques need to be signed. There is a digital signature facility in PKI. Again, this is nothing new. There is already a body of law in most countries covering the question whether digital signatures are irrevocable. Replace cheques with digital certificates which have been digitally signed and another source of fraud is reduced. (The clearing system could be speeded up at the same time.)

100. A further example, Finland are considering the feasibility of prescriptions being digitally signed by GPs.

101. Final example, credit card fraud will be reduced by the introduction of chip and pin cards, but it will only be reduced for transactions where the customer is present. The credit card companies already use PKI to authenticate their merchants' credit card terminals. The weak link is the one between the customer and the terminal. If material credit cards were replaced with digital certificates, then even customer-not-present credit card fraud could be reduced. How? Answer:

- When the customer is present during a credit card transaction, his mobile phone can connect to the merchant's credit card terminal using a free Bluetooth or infra-red link. PKI will authenticate the transaction from end to end, from the digital certificate credit card on the customer's mobile to the merchant's terminal to the credit card company's mainframe.
- When the customer is not present, the only difference is the link – the customer will be connected by the mobile phone network instead of a short-range link. Nothing else is different. The same high level of authentication can be provided whether the customer is present or not.
- The customer's private key must be issued under secure conditions, preferably involving a Faraday cage, as noted above. Thereafter, the strength of PKI allows the customer safely to use public networks such as the mobile phone network. PKI is the general solution to the customer-not-present problem.

102. Again, Finland are already conducting a feasibility study, in this case with Visa.

103. Where does the Home Office's sometimes voiced notion come from that their scheme places the UK in the vanguard?

104. With authenticity promoted by PKI, there will be less provision in company accounts for fraud and there will be less money spent on insurance against fraud. What with that and the reduced cost of producing vouchers, dematerialised ID could help to reduce the costs of doing business and so expand the economy.

105. This again distinguishes it from the government's ID card scheme, which contributes nothing to eCommerce. Dematerialised ID provides incentives for people to enrol. There are benefits on offer to everyone, unlike the government scheme, which is simply penal.

106. Digital certificates could be issued to companies by Companies House instead of the present material certificates of incorporation. The FSA could issue digital certificates to banks. The Trades Union Congress could issue them to unions and the Charities Commission could issue them to charities. Any club could issue digital certificates to its members instead of material membership cards. Individuals and organisations both could be brought into one single infrastructure, the PKI.

107. That would improve the chances of combating money-laundering and identity theft. Money-laundering, after all, involves not just individuals but also companies and banks and others. Issuing smart cards to individuals alone, as the government propose, can be at best only a partial solution to the money-laundering problem. Similarly, it is not just individuals who suffer from identity theft, so do companies and other organisations.

108. The incidence of identity theft in the UK is estimated to be £1.3bn p.a. (There is something suspicious about this figure. It never changes. Year after year, whoever is doing the survey, the annual cost of identity theft in the UK is always £1.3bn.) The Home Office promise that ID cards will reduce identity theft but they do not say how much it will be reduced by. There is no

value associated with this promise. And there is no argument advanced to support it. It is quite conceivable that the introduction of ID cards should actually increase the incidence of identity theft, not reduce it.

109. The National Criminal Intelligence Service (NCIS) estimate the annual value of money-laundering in the UK to be of the order of £10bn. Their figures suggest that the annual value of detected money-laundering is of the order of £0.1bn, a mere 1% of the total incidence. These figures are embarrassing. Some major change in detection methods is surely called for. Forgeable ID cards issued to individuals alone will do little to improve the figures. Dematerialised ID could be the change required.

110. PKI is an established technology. There is nothing new about issuing and using digital certificates. BT, for example, already issue digital certificates to registered suppliers who wish to trade on the BT extranet. And HM Revenue & Customs, for example, already insist that companies which make certain tax payments and submit certain returns on the Government Gateway on the web identify themselves using a digital certificate rather than the less secure user ID and password combination.

111. One benefit the government use to advocate their scheme is the reduction of crimes like money-laundering and identity theft. These are not, however, the crimes which worry people generally. Rather, it is mugging, burglary, drug-trading, car theft and vandalism which depress the national mood. These are all location-based crimes, and mobile phones help to locate the victims, criminals and witnesses involved. The political benefits of reducing these crimes are obvious and it is obvious how dematerialised ID could help. Smart ID cards would make no contribution whatever. They are based on the wrong technology.

PRODUCER CAPTURE

112. Dematerialised ID makes imaginative and effective use of existing technology. Its merits seem evident. Apart from the replacement of cardboard cards with plastic ones, the government scheme is redolent of the typewriters and rubber stamps of another age. The question arises how they have come to adopt such a pedestrian, old-fashioned, inflexible, give-everyone-a-card-and-keep-a-list scheme. The answer seems to be that they are advised by Intellect, a UK trade association of 1,000 or so IT suppliers.

113. Three members of the Board of Intellect, including the President and the ex-President of the Board, are from Phillips, who supply smart cards themselves and who also own 32% of Atos Origin. Atos Origin, in turn, own the old SchlumbergerSema smart card business. Phillips win whether they get the £2bn contract for ID cards or Atos Origin get it.

114. It is common to use smart cards to implement mass consumer systems but you do not have to follow convention blindly, there is an alternative, as we have seen – mobile phones. How many of our five mobile phone network operators in the UK are members of Intellect? None.

115. This is producer capture. The smart card suppliers in this case represent a £2bn threat to the UK taxpayer.

CAPABILITY

116. Atos Origin head the consortium which was chosen to conduct the UKPS biometrics trial. They had trouble getting their facial geometry, irisprint and fingercopy equipment to work and the start of the trial had to be postponed twice.

117. When the US government became anxious about cost and time over-runs on IT projects, they established the Software Engineering Institute (SEI) to try to find a way to overcome the problem. The SEI devised the capability maturity model (CMM), which they use to score IT departments on a scale of 0 (worst) to 5 (best).

118. The Atos Origin corporate brochure says that it is a CMM-level 3 organisation, "we are one of the few organizations rated Level 3 in Europe". To be precise, according to the SEI, there is no such thing as a "CMM-level 3 organisation". Big organisations like Atos Origin have many IT departments, not just one. It is individual IT departments which are rated by the SEI, not the organisation as a whole. Boeing, Lockheed Martin and Motorola, for example, each had five CMM-level 5 IT departments within the organisation when BCSL last checked and Tata had 16 of them.

119. Perhaps it would be more appropriate for UKPS to choose an excellent CMM-level 5 supplier like Tata, as we taxpayers deserve, rather than a third division team like Atos Origin.

120. The Atos Origin consortium includes Identix Inc. Identix bought Visionics Corp., who specialise in biometrics based on facial geometry. Visionics used to claim that they wiped crime off the streets of the London Borough of Newham with their FaceIt system, which matches CCTV images of people in the street to a database of known offenders.

121. The police say that the Visionics system failed to match a single CCTV image to a database record and led to precisely zero arrests. The NPL describe this technology as failing even to approach the performance required of an ID voucher scheme. This is the technology that failed to recognise 31% of the able-bodied and 52% of the disabled participants in the UKPS biometrics trial just a few minutes after registration.

122. How many times does the taxpayer have to pay for biometrics based on facial geometry to fail?

ANONYMITY

123. The government claim that they are listening to the advice of the police and the security services. They are selective, though, in what they listen to.

124. NCIS say, in their annual UK threat assessment report, that criminals are much assisted in their pursuits by the wide availability of pay-as-you-go mobile phones, which allow them to communicate anonymously as far as the mobile phone networks are concerned, i.e. they do not need to register their personal details when they buy a pay-as-you-go phone.

125. The Identity Cards Bill ignores NCIS. Dematerialised ID addresses their concerns.

126. The government could reduce the anonymous use of the UK mobile phone networks with a Bill which could be enacted quickly. Call it the "Dematerialised ID Bill". This Bill would not kill the pay-as-you-go business. People could still use pay-as-you-go phones, there would still be no monthly itemised bill arriving by post, it's just that their personal details would be registered.

127. It is not just pay-as-you-go phones. Anonymous use arises also when an organisation buys 1,000 mobile phones for use by its staff and each phone is registered in the name of the organisation, not the user.

128. An anonymous user is one whose identity is not known. The Home Office offer three criteria for identity:

- Biometric identity – "things which you 'are' ... fingerprints, iris patterns ... and DNA profile".
- Attributed identity – "things which are given to you ... full name, date and place of birth and parents' name and addresses".
- Biographical identity – "things which happen to you during your life ... education/qualifications ... electoral register entries ... benefits claimed/taxes paid ..."

129. To these criteria, dematerialised ID adds a fourth:

- Location identity – where you have been. One person cannot be at two locations at once. Two people are unlikely to have been at exactly the same locations throughout the months and years past. You can be identified by the set of locations you have occupied. And these locations are automatically recorded by the mobile phone network operators as you roam, with your mobile phone switched on, from base station to base station and from country to country.

130. We are not dependent on biometrics and, as we have seen, that is just as well. If biometrics can prove themselves reliable, then biometric identity can be incorporated into dematerialised ID. It is an option. Until then, the approach must be sceptical, guilty until proven innocent. There is no point wasting money on biometrics.

131. We already have several ways to establish identity, mostly relying on attributed and biographical properties. The banks, for example, operate their know-your-customer scheme on this basis. Internet banks add biographical details such as the accountholder's favourite film or first school. The Dematerialised ID Bill could provide for similar registration procedures to be carried out by mobile phone shops even when the customer is only buying a pay-as-you-go phone. Once again, use the existing distribution network, avoid the risk of establishing a new network of 2,000 enrolment centres.

132. In the case of purchases of mobile phones by organisations on behalf of their staff, the Dematerialised ID Bill could provide for the organisations to register the personal details of each user. They must have these details for personnel and payroll purposes.

133. The Dematerialised ID Bill could also provide for all public sector forms to include a box for mobile phone numbers. Every opportunity should be taken to collect people's mobile phone numbers.

134. These provisions would help to associate each mobile phone number with a person. They would help to reduce the anonymous use of the mobile phone networks.

135. The Home Office suggest that identity could be further confirmed by cross-checking with the records maintained by the major credit referencing companies such as Experian. Experian offer on-line credit referencing services to subscribers and this procedure is already followed by at least some mobile phone shops for mobile phone accountholders. The procedure could be followed for pay-as-you-go users as well.

136. BCSL suggest adding location identity to the list of checks that could be made. It would not be appropriate for mobile phone shops and employers to conduct this check. The Dematerialised ID Bill could provide for it to be carried out by UKRA.

137. In view of the UK's poor record in preventing money-laundering, it must be admitted that know-your-customer is not working well. Cross-checking with credit referencing companies and using location identity may prove to be more successful.

138. UKRA would not be required in the first instance to create any new databases. They would merely need to operate a portal, which links to the existing databases maintained by the mobile phone network operators and the credit referencing companies. It should also link to the databases maintained by the departments of state and their agencies. These databases should include in particular the Police National Computer, so that UKRA can make checks on criminal records.

139. The portal should be provided for in the Dematerialised ID Bill and could be called "UK Rapport", it is suggested, or simply "Rapport".

140. The results of searches on the linked databases could themselves be stored in a Rapport database. The Rapport database would be an investigations database, built up gradually on an exception basis. It would not be the National Identity Register. That database already exists and is distributed among the five mobile phone network operators in the UK. There is, as noted, no need to incur the costs and risks of trying to build a new one from scratch.

141. Dematerialised ID is a public private partnership (PPP). The National Identity Register is maintained by the private sector. The ID vouchers – the mobile phones – have already been paid for by the consumers. The mobile phone networks, the network of credit card terminals and the Internet all exist already. So dematerialised ID just leaves UKRA to develop Rapport to do one of the jobs that we currently consider must be done by government – policing.

142. Registered users of the mobile phone networks can already be investigated by the police. The effect of the provisions above will be more and more to isolate the unregistered users. They will become more and more suspicious, more and more worth investigating. Their phones may not be registered but they can be tracked and they will make and receive calls to and from other phones. If any of these associated phones are registered, then investigations can be started to see if there is a criminal or terrorist connection.

143. According to a 16 August 2005 article in *The Times*, 'Ban on "security risk" pay-as-you-go phones', Malaysia is banning the use of unregistered pay-as-you-go phones from the end of this year and "security ministers around Europe" are considering "enforcing the same clampdown".

144. With the provisions of the Dematerialised ID Bill in force there would be less anonymous use of the mobile phone networks. That would impede criminals and terrorists now, not in 2013. These measures would go some way to solving the so far unheeded anonymity problem brought to the government's attention by NCIS. It depends on the co-operation of the mobile phone industry. That cannot be taken for granted and some re-negotiation of their licences may be required but, as noted, they do seem to be co-operating already every minute of the year.

VERIFICATION

145. The Dematerialised ID Bill proposed by BCSL would include the provisions described in the paragraphs above and no more. The Identity Cards Bill requires further provisions. These could be added to the Dematerialised ID Bill if that is the decision of its sponsors.

146. The Identity Cards Bill requires in particular that authorised people should be able to verify that you are who you say you are and that you have the entitlements which you claim. These authorised people include policemen. They include benefits offices checking that you are entitled

to benefits, hospitals checking that you are entitled to NHS health care, universities checking that you are entitled to state education, employers checking that you have the right to work in the UK, and others.

147. If these provisions are added to the Dematerialised ID Bill, then there are certain implications. Firstly, only authorised people should be able to make these checks. Policemen, benefits offices, hospitals, universities, employers and others must therefore be able to authenticate themselves to prove their entitlement to make enquiries. Second, the Bill must provide some way for authorised enquirers to authenticate your identity and to establish your entitlements.

148. Where authentication is required, PKI is the tool for the job.

149. In that case, it is suggested that a policeman making a verification enquiry would require a digital certificate issued by the Home Office or by his police force to prove that he has the authority to make that enquiry. A benefits office and an employer would require digital certificates issued by DWP and Companies House, respectively, an NHS hospital would require a digital certificate issued by the Department of Health or the local trust and a state university would require a digital certificate issued by the Department for Education and Skills.

150. It has already been suggested that vouchers like passports, National Insurance numbers, NHS numbers, birth certificates, examination results certificates, professional qualifications certificates and so on could in future be issued in the form of digital certificates instead of material certificates. It is further suggested that when mobile phone shops have conducted their registration checks on a person buying a mobile phone, they should issue a digital certificate to be stored on that mobile phone. This certificate would be a receipt, proving that the bearer has undergone the registration checks, and could be used as part of any subsequent verification of his identity. Similarly, if UKRA have performed location identity checks, then they too should issue a digital certificate receipt to be stored on the bearer's mobile phone.

151. Armed with these digital certificates, both the enquirers and the individuals whose identity and entitlements are being checked can use PKI to authenticate themselves.

152. On the Internet, there are a number of WhoIs facilities which anyone can use to discover who is the registered owner of a given website name. Using the WhoIs facility on http://order.-internic.co.uk/?funct=tools, for example, reveals that the BBC's website was first registered on 13 December 1994 in the name of The British Broadcasting Corporation giving an address in Tadworth and the registration must be renewed by 13 December 2006 if the BBC are to retain the site.

153. A policeman on the beat will need access to a restricted but otherwise similar WhoIs facility to establish who a suspect is. A facility could be developed for employers to check the identity of prospective employees and an IsEntitledToWork facility could be developed to check their right to work in the UK. Other enquirers would need facilities with names like IsEntitledToBenefits, IsEntitledToNHSHealthCare and IsEntitledToStateEducation.

154. With digital certificates, mobile phone handsets, PCs, WAP, Wi-fi, the mobile phone networks, infra-red, Bluetooth and the Internet all available, there is no shortage of tools for dematerialised ID to do the verification job. How? Consider the following example.

155. Section 8 of the Asylum and Immigration Act 1996 requires employers to check before hiring them that new recruits have the right to work in the UK. New procedures were introduced

on 1 May 2004 which specify the material certificates a selection of which must be checked. These include passports, other travel documents with specified endorsements, residence permits, ARCs, P45s, P60s, birth certificates, naturalisation certificates, work permits and specified Home Office letters.

156. Suppose that these certificates are all available in digital rather than material form, that RecruitingCo would like to employ ProspectiveEmployee and that PersonnelOfficer has been given the job of checking ProspectiveEmployee's right to work in the UK. The scenario envisaged is as follows:

Step 1 PersonnelOfficer logs on to RecruitingCo's computerised, PC-based HR system. He identifies himself by specifying his user ID and password. The HR system checks and establishes that PersonnelOfficer is authorised to perform IsEntitledToWork checks.

Step 2 PersonnelOfficer uses the IsEntitledToWork transaction to log on to DWP's website. The data he types in to the transaction dialogue is encrypted using the private key of RecruitingCo's digital certificate of incorporation. DWP decrypts the data using RecruitingCo's public key, available via the Internet from Companies House, and checks that the Companies House certificate has not been revoked. DWP has thus established that this is a person (RecruitingCo) authorised to make IsEntitledToWork checks.

Step 3 The IsEntitledToWork transaction displays a list of acceptable certificates, PersonnelOfficer chooses passports and asks ProspectiveEmployee to answer the Yes/No questions which will appear on his mobile phone display as long as he is within range of the Bluetooth adapter (£10.99 from Misco) on the PC.

Step 4 The effect is to send data to DWP, encrypted with the private key of ProspectiveEmployee's digital passport, a certificate issued to him by UKPS and stored on his mobile phone. DWP decrypts the data using ProspectiveEmployee's public key, available via the Internet from UKPS, and checks that the passport has not been revoked.

Step 5 A picture of ProspectiveEmployee obtained from UKPS is transmitted from DWP to RecruitingCo and displayed on the PC. PersonnelOfficer performs a human visual check, nothing biometric, and confirms that this is, as near as he can tell, what the man in front of him looks like.

Step 6 Having established that ProspectiveEmployee is allowed to work in the UK and that this is ProspectiveEmployee in the room, DWP displays a message to that effect on the PC and sends a confirmation to RecruitingCo by email. It is now legal for RecruitingCo to make ProspectiveEmployee a job offer.

157. The use of the mobile phone at Step 3 above is akin to using the zapper to change channels on your TV or to using the key-fob to lock your car from across the street. It is also like the process of entering your PIN at the supermarket check-out, except that there are no material cards or documents or certificates or vouchers involved, they are all dematerialised.

158. Any number of amendments to this scenario may be needed in practice. For example, perhaps a receipt should be sent to ProspectiveEmployee at Step 6 above as well as to RecruitingCo. This elaboration aside, it should be clear that dematerialised ID could theoretically be used for verification of the right to work in the UK and, similarly, for the other verification transactions mentioned above.

159. Remember that dematerialised ID incorporates PKI. The passport in the example above is authenticated, it cannot be a forgery. The dialogue between RecruitingCo, ProspectiveEmployee and DWP is all encrypted, there is no possibility of eavesdropping.

160. Compare this scenario with the current situation when we hire a car in the UK. The photocard driving licence does not include details of any endorsements. These are recorded on a separate counterpart driving licence. Instead of one certificate, therefore, we end up with two. If you forget to take the counterpart with you to the hire company, they have to telephone the Driver and Vehicle Licensing Agency to check your endorsements, if any, which takes time, annoys the people in the queue behind you, increases the cost of the transaction and may make your endorsements embarrassingly public. The photocard includes a tiny photograph of the bearer, only a quarter the area of a passport photograph, and is of severely limited value for verification, whereas the photograph used at Step 5 above can be as big as the PC screen. The government's ID card scheme could well repeat this clumsiness. Dematerialised ID would avoid it.

EXTENDED DEMATERIALISED ID

161. The provisions of the Dematerialised ID Bill would reduce the anonymous use of the mobile phone networks. They would not make anonymity impossible.

162. There is a way fully to solve the anonymity problem identified by NCIS. It is included in this proposal in the interests of completeness. It would raise new civil liberties issues and it might or might not have an adverse impact on the mobile phone industry's turnover. It would pose political risks and business risks and it would require international co-operation. This option is Orwellian and cannot be chosen lightly but, if political capital is going to be spent, better it be spent on a scheme that will be effective than on the government's proposed ID card scheme.

163. An extended version of dematerialised ID, designed to make anonymous use of the UK mobile phone networks impossible, would work as follows.

164. After successful registration of your personal details, UKRA would issue a digital certificate to be stored on your mobile phone. That certificate would affirm your identity and, crucially, it would become a part of the protocol which mobile phones follow when they handshake with the network such that mobile phones without a UKRA certificate would be unable to make or receive calls, they would be unable to make use of the UK mobile phone networks.

165. "UK mobile phone networks" will need to be defined, as will "use of the UK mobile phone networks". These definitions will be assisted by the fact that each mobile phone has one home MSC (mobile switching centre) and one only. Wherever you are in the world, all the calls you make or receive with your mobile phone have to be switched through your home MSC.

166. The MSC is a piece of hardware which performs the same function for mobile phone voice calls as a telephone exchange performs for landline calls. It connects the caller and the recipient. It is the MSC which has access to the databases already mentioned – the HLR, the VLR, the EIR and the AuC.

167. The location of the MSC in the UK or its operation by a mobile phone network operator under the terms of a UK licence will no doubt enter into the definitions above. The definitions will need to be updated as MSCs are replaced by equivalent machines performing the same function in 2G, 2.5G, 3G and subsequent generations of mobile phones.

168. It should be evident from the above how extended dematerialised ID could apply to all mobile phones with a UK home MSC. Wherever one of these phones is in the world, in the UK or overseas, whether it is making or receiving a call, whether or not it is a pay-as-you-go phone, whether the other party to the call is on a landline or is using a mobile, that call will be switched through the home MSC and may be barred if the mobile phone lacks a UKRA certificate.

169. The definition of "use of the UK mobile phone networks" will need to include using a mobile phone not only for making and receiving voice calls but also for browsing the web and sending and receiving text messages, emails, faxes, photographs and videos. The owners of handsets with a UK home MSC who refuse to register their personal details, and who therefore have no UKRA certificate, would not be able to use the UK mobile phone networks with their own phone. That would be their choice.

170. When a mobile phone with a UKRA digital certificate on it is reported as lost or stolen, the certificate must be revoked. UKRA can revoke the certificate simply by making a phone call to delete the old certificate from the mobile phone or to overwrite it with a revocation certificate. A certificate revocation list (CRL) can also be maintained, as one is already for lost and stolen credit cards, the biggest CRL in the world. The effect of revocation would be to render the phone useless to the bearer.

171. Even if a given mobile phone is unable to use the UK mobile phone networks, it should still be able to associate with them. "Associate", here, is a technical term, the force of which is that extended dematerialised ID could make the phone useless to the bearer without depriving the police of its use as a location-detector.

172. Looking now beyond the UK, consider the case of a mobile phone with a German home MSC, say, being used by a terrorist in Hamburg to call a landline in the UK. The UK mobile phone network is not being used in this case and so extended dematerialised ID would not stop the call from being connected. Some other surveillance scheme might bar the call. This is an example of the point already made that dematerialised ID is just one scheme among many, it is not meant to solve all problems single-handed.

173. Now consider the case of the same mobile phone being used in Hamburg, but this time to call a mobile phone in the UK. Dematerialised ID would apply in this case because the UK mobile phone network is being used. It would also apply in the case where someone was attempting to use this phone in the UK. In each of these two cases, the call would be barred and the terrorist would be impeded.

174. The UKRA digital certificate would thus be a sort of visa required to visit/make use of the UK mobile phone networks. Wherever he is in the world, in the UK or not, the bearer of a mobile phone with a non-UK home MSC would only be able to use the UK mobile phone networks if he had a UKRA certificate. Either that, or his phone would need a certificate issued by his national equivalent of UKRA. That certificate would work on the UK mobile phone networks only if the issuing authority is deemed trustworthy by UKRA.

175. PKI depends on trusted third parties. Some registration authorities will have more difficulty than others inspiring the trust required.

176. PKI is a mature technology. There are already international security assurance standards for measuring the quality/trustworthiness of registration authorities.

177. Finland, again, are already investigating with other countries how to make their ID vouchers reciprocally acceptable.

178. It would take a long time to establish the extended version of dematerialised ID but then there would be no more anonymous use of the UK mobile phone networks. The problem identified by NCIS would be solved.

179. There are several objections to extended dematerialised ID. Among others, if you bar calls from terrorists, which is a good thing, you also bar people living under totalitarian regimes from calling for help, which is a bad thing.

180. There are arguments in favour of extended dematerialised ID. Under the existing government proposals, people will be fined for failing to enrol in the ID card scheme and for failing to keep their registered address up to date. Under extended dematerialised ID, there would be no need for the government to incur the anathema which will be fomented as a result – anyone failing to register would simply not be able to make or receive mobile phone calls with their own phone. And it would no longer be their address which matters but their mobile phone number. There would be no need for these fines.

181. Extended dematerialised ID should be distinguished from plain dematerialised ID. They are two different schemes. A person might be in favour of the plain version but against the extended version.

IDENTITY

182. To argue about function creep – if ID cards are introduced for one purpose, they will soon be used for many others, unless the government take steps to ensure that that does not happen – is, again, fatuous. Of course the uses of ID vouchers will multiply. Identity and existence are fundamental to everything we do and you can no more limit the functions of an ID voucher that works than King Canute could stop the tide coming in.

183. We have considered only three objectives for ID vouchers. Dematerialised ID could expand the economy, it could reduce crime and it might help in the fight against terrorism. Any number of other objectives may be achieved but these are three big ones, which help to make the attractive political and economic case for dematerialised ID.

184. Dematerialised ID may help with some of the other objectives the government have set. It may make it easier to register for public services and easier to deliver them, for example. It may make it easier for people to provide a convincing proof of age. It may make it easier to compile the electoral register. It may make it easier to vote – not that it is particularly difficult to vote at the moment. And it may make it easier to avoid some of the authentication shortcomings of postal voting which have become evident in the past year.

185. It is as well that the government abandoned their earlier plan to call ID cards "entitlement cards". This picture of people as nothing more than a walking collection of rights is unattractive. ID vouchers should restrict themselves to just that, affirming the identity of the bearer. Having issued these vouchers, or having got the mobile phone network operators to issue them, preferably in the form of digital certificates stored on mobile phones, let the government stand back, their job done, and let the departments of state and local government and charities and the private sector show what enterprising things they can do with these vouchers.

186. A person is not just a collection of rights. Equally, a person is not just a mobile phone. You do not cease to exist if you turn off your phone. When the phone registered to you is being used, it may be you using it or it may be someone who has borrowed it or stolen it. The location of the phone, as recorded by the HLR and VLR databases on the mobile phone networks, is only circumstantial evidence that that is your location. But at least it is some sort of evidence to assist the police during an investigation.

187. How do we establish who a person is in the first place, when they are enrolled into an ID voucher scheme? Biometric, attributed, biographical and location identity have all been mentioned, as has the idea of using the credit referencing companies to assist with checking that people are who they say they are. No mention has been made of references from respected members of the community – vicars, doctors, lawyers, head teachers, accountants, local councillors, and so on. These personal references can be more convincing, richer than other identity criteria and should be included in any registration scheme.

188. There are ways of deploying PKI which make use of these local, community-level "webs of trust" as they are known. People can sign each other's certificates and the more signatures there are, the more the certificate can be trusted correctly to identify the bearer.

189. The government's existing PKI is hierarchical, with the root certificate being managed by GCHQ, but that is not the only way to deploy PKI. People can issue their own digital certificates. Now that we have mobile phones, there is little to stop local communities and even individuals from using dematerialised ID to build up their own PKIs, which could co-exist with the government's. That was the admirable reason for developing PGP, for example, the PKI software package already mentioned.

190. Although it is not acknowledged in their report, the LSE's alternative to the government's ID card scheme, with its use of digital credentials and unconditional anonymity, owes a debt to one of these alternative PKIs, specifically the scheme devised by David Chaum in the 1980s. His insight was that you do not need to reveal your entire identity for most transactions, you simply need to demonstrate that you have the credentials required for the given transaction, you can remain otherwise unconditionally anonymous.

191. His scheme was investigated by the EC during the development of OSCIE. They were sympathetic but had to reject it for lack of software to implement Chaum's ideas. There is a more endemic problem – Chaum certificates have to be short-dated and repeatedly renewed. If these problems have been resolved – frequent renewal and the lack of software – then Chaum's ideas could be implemented, and they could be better implemented on mobile phones than on separate smart cards. Dematerialised ID does not exclude Chaum.

192. The idea with dematerialised ID is to associate a person with one or more mobile phones, but what is a mobile phone? The phone number, i.e. the SIM card (subscriber identity module)? The handset, i.e. the IMEI? Both the IMEI and the phone number need to be recorded. In addition, mobile phones are available with RFID tags in them and GPS (Global Positioning System) transceivers. These devices have identifiers associated with them which also need to be recorded in order to identify the mobile phone.

193. Dematerialised ID would have to manage one-to-one relationships between mobile phones and people – one mobile phone and one identity. In the case of people who have several mobile phones, dematerialised ID would have to manage many-to-one relationships. Where one mobile phone is shared between several people, dematerialised ID would have to manage one-to-many

relationships. The Home Office have identified some classes of people who need multiple identities simultaneously – actors with stage names, for example, writers with *noms de plume*, and transsexuals, who often need simultaneous male and female identities, at least for a while. In these cases, dematerialised ID would have to manage many-to-many relationships between mobile phones and personal identities.

194. There are limits to the ability of the mobile phone network to track you. It doesn't work if your phone is switched off or if you are underground or in a poor reception area generally. The same applies to GPS transceivers, which work well in the desert but not underground, not in built-up areas, not under leafy trees and not in the rain. Nevertheless, as long as your mobile phone is switched on, whether or not you are using it, you can be located most of the time.

195. If location identity ever sees the light of day, there will be some interesting design considerations:

- If a person has used the same mobile phone handset, the same phone number and the same mobile phone network operator for years, then it is easy to build up the history of the locations he has been in.
- It is more complex if he has changed operator several times, changed phone number, changed handset twice a year, has several mobile phones at once, has taken over someone else's mobile phone at some stage, has had three mobile phones stolen and one returned, has regularly lent a handset to his daughter, etc … In this more complex case UKRA would have to stitch together a person's location identity from several sources.
- This more fragmented past is probably common and this is the model which should be chosen when people need a new identity to be created for them – people in witness protection programmes, for example, undercover agents and battered wives escaping abusive partners. These people must be able to prove that they are who their new identity says they are, which means that, as well as their new identity being inserted into the record in a realistically fragmented way, their old one must be deleted or otherwise excluded from verification. In this sense, dematerialised ID must allow people to be created and deleted.

CONCLUSION

196. The implication of the points above is that the government are ignoring or misunderstanding the extensive, detailed and authoritative intelligence available to them, in this case intelligence from the EC, GCHQ, the ICAO, NCIS, the NPL, the SEI, the NSA, the LSE and BCSL.

197. No argument has been advanced by them to show how the government scheme will achieve its objectives. The Berlin Resolution does not provide cover and neither do the other precedents adduced. The government have a poor record of developing new IT systems which bodes ill for the ID card scheme. The budget for the scheme has climbed, between July 2002 and now, from £1.318bn to £3.145bn to £5.8bn to £10.6bn to £19.2bn.

198. The government's proposals will be ineffective. Smart ID cards do not help to locate people continuously and they do not help to identify people's associates. BCSL's suggestion is that mobile phones are an effective alternative, an opportunity which the government should not miss. The distinction between what the government are proposing and what BCSL proposes is summarised below.

199. The government scheme will become compulsory, it will waste money on smart cards, it will be 2013 before it can be fully deployed, it uses the wrong technology to be effective, it does

nothing for eCommerce, it raises unanswered civil liberties questions, it requires the payment of unknown royalties to biometrics technology suppliers and it requires the deployment of IDNet, the uncosted national network of inconveniently fixed location terminals, liable to breakdown, vandalism and undetected eavesdropping. It may be represented by the following equation:

Identity Cards Bill scheme = new national identity register + smart cards + biometrics

200. Using the government's own July 2002 figures, if you remove the cost of the smart cards and the biometrics, then the budget for dematerialised ID may be just £0.4bn. That is 48 times cheaper than the LSE estimate of £19.2bn for the government scheme.

201. The BCSL scheme is cheaper, it is voluntary, it can be deployed quickly, it will empower people, it uses the right technology to reduce crime and to expand the economy, the civil liberties issues are already arguably neutralised, it identifies the need to regulate HLRs, VLRs, EIRs and AuCs, it answers the call by NCIS to reduce the anonymous use of the UK mobile phone networks, the project risks are minimised by using existing resources and the scheme makes no pretence to be the single solution to all problems. It may be represented as follows:

Dematerialised ID = portal to existing databases + mobile phones + PKI
(optionally, + biometrics)

202. Subtract one equation from the other and the difference will remind you that the Home Office are placing credulous reliance on biometrics and that they have omitted an essential component, PKI.

203. There is no point yet spending money on biometric registration facilities, on biometric verification equipment and on royalties for the use of proprietary biometric technology. There is no point spending billions on IDNet and on new smart cards, not when we already have mobile phones.

204. Expectations with respect to ID voucher schemes need to be lowered to a realistic level. The budget can be lowered in line. No scheme today can offer conclusive decisions about identity. The best that can be offered is probabilities and circumstantial evidence and the good judgement of staff on the ground and the intersection of multiple independent authentication systems. Dematerialised ID has a good claim to be one of those systems.

205. Dematerialised ID is a PPP which will deliver good value for taxpayers' money. There can be no serious technological feasibility objections – Finland are already doing it, it works. Any country with a mobile phone network could do it. Like privatisation, dematerialised ID could take off globally. It takes advantage of the almost universal voluntary adoption of mobile phones, a natural evolutionary change in society which it is wanton to ignore.

REVIEW – ORIGINALITY & INFLUENCE

206. One of BCSL's objectives is to advocate dematerialised ID to the government with a view to providing the UK with an effective scheme, which delivers good value for money to the UK taxpayer. But what is dematerialised ID, in the end, after 205 paragraphs? It doesn't seem to be anything new. It just seems to be mobile phones and all the infrastructure that surrounds them.

207. The police already use mobile phone records to help with crime detection and perhaps with prevention as well. And yet we still have high levels of crime and low clear-up rates, so perhaps dematerialised ID doesn't work anyway.

208. Do we have high levels of crime and low clear-up rates? The UK crime statistics are famously untrustworthy, to the point of being useless, but suppose that we do. Mobile phone records would perhaps help better to reduce crime if, as suggested by BCSL, a more concerted effort was made to use them and a more concerted effort was made to reduce the anonymous use of the UK mobile phone networks.

209. Perhaps that is all there is to the scheme. Dematerialised ID identifies what may not have been noticed otherwise, *viz.* that in the mobile phone, we have an ID voucher more effective than could ever previously have been possible. That, some well-chosen names – "dematerialised ID", "UKRA", "Rapport", "fingercopy" and "be me" (see below) – and 205 paragraphs of well-organised, thoroughly researched and, it is hoped, convincing polemic.

210. The idea of dematerialised ID is original to BCSL in that this particular configuration of all the components occurred to the author without seeing it described anywhere else.

211. It was recognised at the outset, in December 2002, that the original recommendations of a lone consultant would not carry much weight with the government, the police, the security services, the mobile phone network operators, the banks and all the other organisations involved. The attempt was made therefore to find other advocates of dematerialised ID and quickly revealed Finland and no-one else.

212. Some of BCSL's ideas had not been stated by anyone else when last checked. The need for government agencies to collect mobile phone numbers wherever they can in order to reduce anonymity on the networks, for example, the recognition that PKI is the general way to achieve secure remote communications and thus to solve the problem of customer-not-present credit card fraud, the inclusion of organisations as well as individuals in the same ID voucher scheme to combat money-laundering and identity theft, the detection of terrorist and criminal groups by reference to who calls whom on the mobile phone networks, the use by UKRA of a portal to access existing databases instead of creating new ones, the concept of location identity and the importance for civil liberties of regulating HLRs, VLRs, EIRs and AuCs, not to mention the Orwellian idea of amending the mobile phone network handshaking protocol to implement extended dematerialised ID. They may still be original.

213. When we make a dematerialised credit card purchase or we take part in an IsEntitledTo-NHSHealthCare enquiry, for example, we may need a "be me" button on our mobile phone handset to invoke the associated dematerialised ID functions. Or a "be me" chip in the handset. Or a "be me" menu option. The temptation then to say "beam me up, Scotty" will be irresistible. No apology is made for the *Star Trek* overtones of dematerialised ID. There is nothing fantastic about the idea, it is utterly practical and more or less with us already. And what is the recent history of science, anyway, if not an attempt to catch up with the inventions of *Star Trek*?

214. In the main, though, Finland seem to have worked out dematerialised ID for themselves in much the same way as BCSL and BCSL seem to be acting, unbeknownst to Finland, as their ambassador.

215. The fact that Finland are pursuing dematerialised ID and succeeding with it, albeit in tandem with a scheme based on material ID cards, should carry considerable weight but lobbying efforts in the UK have nevertheless proved fruitless so far. There are vested interests involved and there is blinkered thinking to overcome.

216. Funds are now being sought as a result to establish a multi-disciplinary Institute of Dematerialised ID (IDID) to research all aspects of the scheme and to provide paid consultancy advice on its deployment to governments everywhere. Is it legal for the UK government to cross-refer between databases maintained by the mobile phone network operators, the credit referencing companies and the departments of state? BCSL doesn't know. This is one of many research projects for IDID.

217. The table overleaf shows the expertise required in IDID. There are 6.4bn people on the planet and millions of organisations. They are all potential users of dematerialised ID. IDID should be a profitable consultancy.

Institute of Dematerialised ID (IDID)	
The staff needed/consultants to retain should have expertise in:	
Anti-virus techniques	Money-laundering
Banking	Operating systems
Biometrics	People-smuggling
Broadcasting	Pervasive computing
Certification	Policing
Civil liberties	Politics
Credit cards	Portals
Data protection	PR
Dealing with central government	Project management
Diplomacy	Public key cryptography
Disability access	Public service provision
Drug-dealing	Registration
Economics	Regulation
Ethics	Retail
Foreign languages	Revocation
Forgery	Sales
Fund-raising	Security services
Identity theft	Smart cards
International passenger transport systems	Specific countries
IPR	Specific UK government departments
Journalism	Supranational organisations
Law	Systems engineering
Lobbying	Telecommunications networks
Marketing	Telematics
Mathematics	Web services
Mobile phone handset architecture	Wireless networking protocols

NOTES

218. References can be supplied to support most statements made in this proposal

219. Printed from: Dematerialised ID Reid 001.doc on Sunday, 11 June 2006 at 23:03

220. 15,481 words

END