

Confidential

It will be noted that in early 2003 BC

Dematerialised ID
The Alternative to Entitlement Cards

A Proposal

by

David Moss

of

Business Consultancy Services Ltd (BCSL)

Dematerialised ID

The Alternative to Entitlement Cards

May 2003

Outline

1	Executive summary.....	4
2	Introduction.....	5
3	Entitlement cards	6
4	Dematerialised ID	16
5	Dematerialised ID v. entitlement cards.....	34
6	Feasibility.....	38
	References.....	50

First printed: 29 May 2003

© May 2003 Business Consultancy Services Ltd

Dematerialised ID

The Alternative to Entitlement Cards

May 2003

Table of contents

1	Executive summary.....	4
2	Introduction.....	5
3	Entitlement cards	6
3.1	Introduction.....	6
3.2	Public services	7
3.3	Identity fraud and money-laundering.....	7
3.4	Illegal immigration and illegal working	7
3.5	Passport.....	8
3.6	Proof of age.....	9
3.7	Voting	10
3.8	Medical information and organ donation.....	11
3.9	E-commerce	11
3.10	Plastic cards	11
3.11	Biometrics	12
3.12	Budgets	12
4	Dematerialised ID	16
4.1	Introduction.....	16
4.2	PKI.....	16
4.3	Digital certificates.....	18
4.4	Revocation authorities	23
4.5	Mobile phones.....	25
4.6	Tracking	26
4.7	Mobile phones and detection	29
4.8	Civil liberties.....	30
4.9	Location identity	31
5	Dematerialised ID v. entitlement cards.....	34
5.1	Features	34
5.2	Cost-benefit.....	35
5.3	Entitlement cards – SWOT	36
5.4	Dematerialised ID – SWOT.....	37
6	Feasibility.....	38
6.1	Introduction.....	38
6.2	How a scheme might work in practice.....	38
6.3	Digital certificate management.....	42
6.4	Software facilities	44
6.5	Telecommunications facilities	47
	References.....	50

1 EXECUTIVE SUMMARY

- 1.1.1 The objective of this proposal is to reach a point where the UK reaps the benefits of dematerialised ID.
- 1.1.2 The arguments are meticulously rehearsed in the main body of the proposal.
- 1.1.3 The approach taken here in the *Executive Summary* is to consider what we shall say in the year 2009 when we look back.
- 1.1.4 "The entitlement card scheme would have been a plodder – give everyone a card and keep a list. The Home Office would have been reviled for re-introducing ID cards and for wasting the taxpayers' money. It would have been one of the nails in the Labour Party's non-delivery coffin at the recent election.
- 1.1.5 As it is, we have dematerialised ID. Inspired. Imaginative. Society was evolving, a natural adaptation was taking place. Everyone had a mobile phone. They paid for it themselves. We had the *nous* to spot it and to capitalise on the opportunities.
- 1.1.6 Instead of the credulous adoption of biometrics, untested in mass operation, we went for PKI, with 25 years of solid academic backing. Never heard of it at the time. Turned out we'd been using it ourselves for 25 years. Whole Government machine relied on it. And we invented it!
- 1.1.7 Instead of the reckless waste of over £3bn, we put the whole scheme in for £400m. The people are willing. Crime rates are down. Police clear-up rates are up. The banks love it. Business loves it. We have the lowest costs of doing business in the world and the most competitive economy.
- 1.1.8 Home Office initiative, of course. Nothing to do with the Treasury.
- 1.1.9 Thank God we did it. Otherwise the Finns would have got the credit for a scheme which has now swept the world. There has been nothing like it since privatisation."
-

2 INTRODUCTION

- 2.1.1 In February 2003, a proposal ([BCSL 2003a](#)) was submitted by BCSL to the Entitlement Cards Unit of the Home Office advocating dematerialised ID. An acknowledgement was kindly sent but no other response has been received.
- 2.1.2 A related proposal ([BCSL 2003b](#)) was sent to the National Criminal Intelligence Service, also in February 2003. No response has been received.
- 2.1.3 Since then, we have fought and won a war. The threat of terrorism remains high. It is assumed that crime levels remain high and police clear-up rates remain low.
- 2.1.4 The entitlement card scheme remains a poor response, and yet the Home Secretary continues to make impassioned pleas on the BBC Radio 4 *Today* programme for its introduction.
- 2.1.5 The present proposal is submitted in order to try, once again, to promote dematerialised ID, which remains the strong response, with greater benefits attached and lower costs.
-

3 ENTITLEMENT CARDS

3.1 Introduction

- 3.1.1 In July 2002, the UK Home Office published a consultation paper on entitlement cards and identity fraud ([Home Office 2002](#)).
- 3.1.2 "Entitlement card" is another phrase for "identity card" or "ID card". The idea of re-introducing¹ ID cards in the UK surfaces intermittently and has been rejected each time for the past 50 years.
- 3.1.3 On that basis, it is likely to be rejected again. The benefits of ID cards advocated this time (*ibid.*, Chapter 3) are to:
- 1 Make it easier to register for public services and easier to deliver them.
 - 2 Reduce crime, particularly identity fraud and money-laundering.
 - 3 Reduce illegal immigration and illegal working.
 - 4 Provide a convenient alternative to the passport, at least in European Economic Area (EEA) countries².
 - 5 Provide a convincing proof of age.
 - 6 Provide a new basis for the electoral register and a basis for new ways to vote.
 - 7 Store emergency medical information and the bearer's wishes in respect of organ donation.
- 3.1.4 A detailed review of the consultation paper leads to the conclusion that only one of the claims made for entitlement cards is supported by argument – the claim that it will help to reduce identity fraud, see 2 in the list above.
- 3.1.5 11 of the countries listed in Annex 3 of the consultation paper have ID card systems, three of them compulsory. It is disappointing, even to a sympathetic reader, that no statistical evidence is advanced to show whether these countries have achieved any of the benefits held out for entitlement cards.
- 3.1.6 The entitlement card scheme is expensive. A lot of the costs are attributable to setting up and operating a network of biometric recording stations. Biometrics is not without its detractors and the reliability of the science and the equipment involved should be established before substantial funds are committed.
- 3.1.7 If the national biometrics network is taken out of the implementation plan, it may be possible to bring forward the start of an effective scheme, see [section 4](#) below.

¹ The UK had ID cards during the Second World War. The ID numbers used then live on now as National Health Service numbers (*ibid.* p.84). The civilian ID card scheme was discontinued in 1952 (*ibid.*, pp.8 and 85).

² EEA = EU + Iceland + Liechtenstein + Norway.

3.2 Public services

- 3.2.1 One of the benefits held out for the Home Office's proposed entitlement card scheme is to make it easier to register for public services by reducing duplication (Home Office 2002, pp.7-8, 25 & 27). Duplication can be reduced without introducing an entitlement card. It requires only that Government departments change their procedures so that they can share information efficiently.
- 3.2.2 The political desirability of information-sharing between Government departments is a matter for serious thought. Its legality also needs to be established.
- 3.2.3 If an investigating commission decided that information-sharing is politically desirable and is legal or should be legalised, then there would still be no need for entitlement cards, simply a need to improve inter-departmental procedures. If the decision went the other way, then entitlement cards would not make it easier to register for public services since it would be neither politically desirable nor legal for one department to share information with another.
- 3.2.4 One way and another, the efficient delivery of public services is independent of the introduction of entitlement cards.

3.3 Identity fraud and money-laundering

- 3.3.1 Entitlement cards could help to reduce the level of identity fraud in particular and perhaps money-laundering (*ibid.*, pp.29-30, 36-7 & Chapter 4).
- 3.3.2 There are already strict reporting requirements which help to detect money-laundering. Further efforts to reduce money-laundering would need to target the companies and the other organisations through which money is laundered. The entitlement card scheme is only concerned with individuals, not companies.
- 3.3.3 Crime and the state of the health service are the two top political worries regularly expressed in UK surveys. The crimes that people worry about in the main, though, are muggings, burglary, car theft and the illegal drug problems that often lie behind them all. They are not identity fraud and money-laundering.
- 3.3.4 Something like an entitlement card would clearly help to reduce the level of identity fraud and might help with money-laundering. A scheme which achieved these objectives and at the same time helped to clear up or reduce the crimes which worry people more generally would have strong political backing.

3.4 Illegal immigration and illegal working

- 3.4.1 The consultation paper claims that entitlement cards would help to reduce illegal immigration and illegal working (*ibid.*, pp.8, 31-3 and 68). Legal immigrants are already issued with work permits and asylum seekers are already issued with application registration cards (*ibid.*, p.49), which include fingerprints. It is not made clear how yet another card would help.

- 3.4.2 Note that the fingerprints recorded on application registration cards provide a legal standard of proof of identity (*ibid.*, pp.105-6). The fingerprints proposed for the entitlement card are of lower quality. What is the point?
- 3.4.3 The proposed entitlement card is not "compulsory", by which the Home Office mean that there would not be a duty on residents to carry it at all times. Belgium (*ibid.*, p.87), Germany (*ibid.*, p.89) and Spain (*ibid.*, p.91) are the only countries listed in Annex 3 to the consultation paper where it is compulsory to carry an ID card at all times and to show it on demand to the police. The Home Office state that they do not wish to follow that example.
- 3.4.4 If the scheme were compulsory, then the non-possession of an entitlement card might help to identify illegal immigrants and all sorts of other people. As long as it is not compulsory, it is hard to see how entitlement cards will help in these matters.

3.5 Passport

- 3.5.1 The suggestion is made that entitlement cards might be used instead of passports (*ibid.*, p.34 & 95) for travel within the EEA. We would still need passports for travel outside the EEA. There would be no saving. In fact, there would be an extra cost to the taxpayer – producing, issuing and monitoring entitlement cards in addition to all the costs associated with passports. From that point of view, the use of entitlement cards as travel documents does not provide a cogent reason for their introduction.
- 3.5.2 It is suggested that getting through airports and other ports could be speeded up by swiping an entitlement card through a card reader at the Immigration desk (*ibid.*, p.117). "This would probably require biometric information to be stored on the chip to ensure that only the person issued with the card was using it for travel." In other words, a person or a machine would still be required to check that the bearer of the card is the person to whom the card was issued. That takes time. Where is the added convenience?
- 3.5.3 It is claimed that a card would be more "convenient to carry" (*ibid.*, p.34) than passports. The size and frayed condition of our pockets, wallets and purses is surely not a matter for primary legislation.
- 3.5.4 The point is made that many other EEA citizens travel within Europe using their identity cards (*ibid.*, p.34). This is true but it is not a reason to introduce entitlement cards in the UK.
- 3.5.5 The argument based on they-do-it-in-other-countries is circular. The proponent only chooses for example the countries whose practices he agrees with in the first place. They allow the death penalty in other countries but the UK has nevertheless banned it. They allow hunting in other countries but the UK seems set to ban it. They allow the ritual slaughter of animals for food in other countries but the UK is now going to investigate this practice with a view to legislation.
- 3.5.6 The argument based on they-do-it-in-other-countries leads in the following case to a farcical suggestion. The Home Office regard the UK Passport Ser-

vice (UKPS), the Driver and Vehicle Licensing Agency (DVLA) and Driver and Vehicle Licensing Northern Ireland (DVLNI) as having equally good identity checking procedures³. This leads them to suggest in the consultation paper that eligible residents who have neither a passport nor a driving licence could be issued instead with an entitlement card to be known as a "non-driving licence" (*ibid.*, p.9). This peculiar locution is justified on the basis that it is used in the USA.

- 3.5.7 The checking procedures used by UKPS, DVLA and DVLNI to establish that the bearer of one of their vouchers is who he says he is are already recognised internationally as high quality. The Home Office propose further improvements to these procedures both by collecting biometric information and by cross-checking records with credit referencing companies, which tend to have more up to date information about people than Government agencies (*ibid.*, p.102).
- 3.5.8 Note that Experian (2003), the credit referencing company, already provide an e-identitycheck service (2003), which includes controls against money-laundering. Experian are also involved, as guarantors, in CitizenCard, a non-profit company which issues ID cards (2003). The CitizenCard, like the NUS card (2003), supports electronic cash via Splash Plastic's e-wallet (2003).
- 3.5.9 According to the CitizenCard website, "almost every airline, most banks and retailers recognise CitizenCard as valid photo-ID or proof-of-age. The Government, the police, local authorities and many NGOs such as Citizens Advice Bureaux also recognise the card". The card is, therefore, potentially useful. It costs only £7 for life. And yet only 15,000 CitizenCards have been issued in London, 14,000 of them to people in the age range 12-20. 15,000 is less than 0.2% of the 8m people in London. It is not clear from the website how long CitizenCard have been operating but a 0.2% uptake does not suggest a high demand for the product.
- 3.5.10 The advantage the credit referencing companies have over Government departments is their links with banks and utility companies. The utility companies themselves may be expected to enter the ID market, particularly BT (2003).
- 3.5.11 These are interesting digressions but the fact remains that we already have passports that take us anywhere in the world. We do not need a second passport which only covers 26 countries.

3.6 Proof of age

- 3.6.1 The entitlement card would help young-looking people to prove that they had the right to buy cigarettes, go to the cinema or drink in pubs (*ibid.*, pp.34-6, 48, 56 & 119). This is true but it does not seem like a matter for primary legislation.

³ DVLA and DVLNI have more experience than UKPS of issuing photocards. DVLA have issued photocards since 1998 and DVLNI apparently since 1928 (*ibid.* p.95).

- 3.6.2 At this point, some limited market research may help:
- At Finch's pub in *name of town* the doors are manned in the evening by bouncers, who no longer accept the photocard driving licence as proof of age as there are so many good forgeries available.
 - The author is unreliably informed that some schoolboys carry several different forms of ID, sometimes designed to suggest that they are younger than their real age, not older, so that they can take advantage of cheap fares.
 - The author is equally unreliably informed that adolescent girls' magazines include offers of fake ID cards in the classified ads section.
 - A Google search of the web on "fake identity identification id card site:uk" produces 233 results, including for example iDentacard (2003), P.O. Box 5356, Northampton, NN4 9XX, "Home of the world's most effective fake ID's!".
- 3.6.3 How long will it be before iDentacard make a fake entitlement card, so that even the real McCoy fails to get you into Finch's?
- 3.6.4 The Home Office state that they are interested in implementing a "universal" scheme, by which they mean that everyone in the country over the age of 15 should have an entitlement card. In this case, the entitlement card will not help those in the age range 0-15 to prove their age.
- 3.6.5 They also state that they would prefer the scheme not to be "voluntary". In a voluntary system, the residents of the UK would be able to choose whether to apply for an entitlement card. The Home Office would prefer everyone in the UK over the age of 15 to have an entitlement card on the grounds that this will allow all service providers to use a single system to establish identity and entitlement.
- 3.6.6 This sounds efficient in theory but it may not be prudent in practice. Evolution teaches us that there is strength in diversity and plurality. So does free market economics. A single point of weakness in a system reduces resilience, which is why the US Department of Defense designed packet-switching and the Internet. An entitlement card scheme that was the only proof of identity would provide fraudsters with a weak point to attack.
- 3.6.7 The suggestion here, therefore, is that the Home Office should plan to have several identification systems in simultaneous operation in future just as at present.
- 3.7 Voting**
- 3.7.1 Management of the electoral register could be improved if there were an entitlement card scheme (*ibid.*, p.37). It could be but it may not be and there may be other ways to improve it.
- 3.7.2 Entitlement cards could provide the basis for new ways to vote (*ibid.*, p.38). This seems to be a response to the contrast between the low turnouts at elections and the high number of votes cast on reality TV shows. Two ideas are being confused here: on the one hand, the *value* of voting; and, on the other

hand, the *ease* of voting. Attention should surely be paid more to promoting the former than the latter – it is already perfectly easy to vote.

3.8 Medical information and organ donation

3.8.1 We already have organ donor cards and bracelets, for example, for girls to wear with allergy information in them. Entitlement cards might be used to store this information (*ibid.*, pp.38, 116 & 129) if they were introduced for some other reason but storing this information is not a good enough reason on its own to introduce them.

3.8.2 Since the entitlement card scheme is not compulsory, many people will not have their card on them when they are run over and so the hospital will not be able to use it to find what antibiotics they are allergic to.

3.9 E-commerce

3.9.1 There is some reference in the consultation paper to e-commerce and digital signatures (*ibid.*, p.125). However, promoting e-commerce is not included in the seven main objectives of the entitlement card scheme described in Chapter 3 of the consultation paper.

3.9.2 This is a surprising omission and it is suggested here that promoting e-commerce should be a key objective of an entitlement card scheme. Presumably the Office of the e-Envoy had no input to the paper ([e-Envoy 2003](#)).

3.10 Plastic cards

3.10.1 There is a limit to the amount of information which can be displayed on an entitlement card. The entitlement card would be modelled on the photocard driving licence and that does not have space to display any endorsements, for example. As a result, if a prospective customer has failed to bring his paper Counterpart Driving Licence with him, car hire companies have to ring DVLA to check (*ibid.*, p.120).

3.10.2 The same constraints would apply to entitlement cards. They begin to look less convenient if an employer, say, needs to contact a call centre to check a job candidate's work entitlements. The experience of dealing with most call centres is awful. The suggestion that the call may on occasion be at premium rates (*ibid.*, p.120, pp.144-5) will make the prospect even less attractive.

3.10.3 Where will the call centre be? They often seem to be based abroad in order to economise on wages. The UK could lose control over who has access to the confidential information of private citizens.

3.10.4 Plastic cards wear out with use.

3.10.5 There is always a danger that counterfeit entitlement cards would become available. This is acknowledged throughout the consultation paper but see particularly pp.39-40. See also BBC ([2003j](#) and [2003k](#)).

3.10.6 It becomes harder to counterfeit entitlement cards if they are fitted with holograms (*ibid.*, p.34) and embedded chips (pp.55-6). These allow more in-

formation to be stored such as fingerprints and work entitlement. But then special reading equipment is required, which reduces convenience again.

3.10.7 Note that it is implicit in the consultation paper that a lot of new equipment will have to be deployed in airports and benefits offices and hospitals, for example, to record and read data stored on the proposed entitlement cards.

3.10.8 Plastic cards are not the ideal vehicle of entitlement.

3.11 Biometrics

3.11.1 Considerable importance is accorded by the Home Office to the use of biometrics. The consultation paper abjures the use of DNA (p.104) but expresses an interest in biometrics based on the geometry of our faces, iris patterns and fingerprints (pp.104-11)⁴.

3.11.2 The claims made for the accuracy of biometrics are impressive. Identix, for example, claim to be able to record the unique features of a person's face in only 84 bytes of memory. They claim to be able to match a scanned face against a biometric database at the rate of 15m per minute ([Identix2002](#)) – you could be picked out from the entire population of the UK in a maximum of about four minutes. This applies to faces scanned in person, faces scanned from photographs and faces picked out by CCTV cameras mounted in, for example, Newham town centre, see Penenberg ([2001](#)).

3.11.3 The results of trials done to date are less impressive ([BBC 2002c](#) and [Ward 2003b](#)). It is not obvious that biometrics are reliable. The technology should be treated as guilty until proven innocent, it must demonstrate reliability and adequate performance before a lot of money is spent on it.

3.11.4 A lot of the inconvenience of the proposed entitlement card scheme arises from the use of biometrics as do a lot of the costs. Again, it needs to be shown in advance of specifying the scheme that biometrics will deliver the benefits claimed.

3.12 Budgets

3.12.1 The cost of the entitlement card scheme is estimated at Annex 5 of the consultation paper. It is not known how the initial cost estimates were compiled. They have had large percentage uplifts added to them in the name of risk management.

3.12.2 The consultation paper assumes that it would take three years to set up the entitlement card scheme between 2004/5 and 2006/7. The set-up costs are estimated to be £136m (*ibid.*, pp.133-5), made up as follows:

- £45m – central entitlement card database

⁴ Why no mention of using teeth as a means of identification? Crime reports often finish by saying that the victim was identified by his dental records. They never say that he was identified by his iris pattern. Suppose that Peter Bazalgette started a company called Celebrity Eyeballs selling copies of the iris patterns of the rich and famous.

- £29m – biometric fingerprint and iris pattern equipment
 - £62m – links to related databases at UKPS, DVLA, DVLNI, other Government departments and credit referencing companies.
- 3.12.3 Entitlement cards would be issued for 10 years in the main to the 67.5m people aged 16 or more estimated to be in the UK during the first 10-year period between 2007/8 and 2016/7. Operating costs for a national network of biometric recording offices during that period are estimated to be £608m⁵ (*ibid.*, pp.137-9).
- 3.12.4 Other operating costs, for the whole 13-year period, are estimated to be £394m, comprising:
- £263m – IT infrastructure (*ibid.*, p.136)
 - £69m – biometric equipment (*ibid.*, p.136)
 - £62m – additional staff at UKPS (*ibid.*, p.137).
- 3.12.5 Three types of card are considered. Production costs depend on the type of card chosen and are estimated variously as follows⁶ (*ibid.*, p.66):
- £180m – for plain cards
 - £502m – for simple smart cards
 - £2,007m – for sophisticated smart cards
- 3.12.6 On these assumptions, total costs range from £1.318bn to £3.145bn for the ID card scheme depending on how smart a card is chosen.
- 3.12.7 These are big numbers. Reducing the cost of the entitlement card system is good for the UK taxpayer⁷.
- 3.12.8 It could be good for the taxpayers of other countries, as well. People travel. The UK needs to be able to handle visitors from other countries. Other countries need to be able to handle UK visitors. The point is not made in the consultation paper but, in order to deliver the greatest benefits, the same entitlement card scheme should be used internationally. There should be an international standard. That requires international co-operation. The cheaper the scheme, the more likely it is to be adopted internationally.
- 3.12.9 Conversely, introducing the scheme may promote international co-operation.
- 3.12.10 For the reasons above, for UK and other taxpayers, it is worth looking for areas where the cost of the entitlement card scheme could be cut.

⁵ At this point, the entitlement card scheme looks like a subsidy to the Post Office.

⁶ It is assumed that plain cards will last for the full 10 years of being swiped through card readers, whereas smart cards will only last for five years, a replacement card will be issued free during the 10-year period without the bearer having to submit another application.

⁷ As Senator Everett McKinley Dirksen is reputed to have said, but didn't, in a debate on the US budget: "A billion here, a billion there, and pretty soon you're talking real money".

- 3.12.11 Large cuts of up to £706m⁸ could be made by excluding fingerprints and iris patterns from the requirements. Taking fingerprints and iris prints requires each applicant to attend a nearby office fitted with specialist biometric recording equipment. That requires the acquisition of extra equipment and the establishment, staffing, training and management of a network of offices around the country.
- 3.12.12 The benefit suggested in the consultation paper is that biometrics can be used to reduce the possibility of multiple applications being made by a single individual. This claim is unreliable, as noted (BBC 2002c and Ward 2003b).
- 3.12.13 Even if the claim proves in future to be reliable, though, the same benefit can be obtained from facial characteristics and these can be scanned from photographs. Photographs can be sent by post to a centralised processing facility. There would be no need to set up and operate a national network of biometrics offices.
- 3.12.14 Excluding biometrics from the proposals would save money. It could also allow the scheme to be implemented earlier.
- 3.12.15 The entitlement card database is referred to in the consultation paper as a "population register" (*ibid.*, pp.25-6, 63 and Annex 2) or "central register" (*ibid.*, pp.9, 16, 29, 33, 37-8, 57, 60-3, 64, 67, 69-74, 76, 119-21, 124, 126-130, 135-7, 141-2, 144 and 146). The consultation paper recognises that a lot of the data for the population register already exists in various Government departments and credit referencing company databases.
- 3.12.16 What is needed is to build interfaces to these databases so that they can be interrogated from a portal using powerful search engines such as Google. The population register is, in that case, the set of Google search results, with an added unique search ID which could, in turn, be the entitlement card ID number.
- 3.12.17 Creating the central register would provide the opportunity to resolve incoherences between the data stored on different databases, a laborious process. Nevertheless, this is a web services⁹ project and, for a web services project, the estimated costs seem high. To put it another way, there may be savings to be made here if the benefits of web services materialise:
- £62m buys you a lot of XML¹⁰ for the interfaces to the existing databases.

⁸ £29m (biometric equipment acquisition) + £608m (network of biometric offices) + £69m (biometric equipment operation).

⁹ From the computer trade press *passim*, you would think that the choice of web services architecture is between Microsoft's .Net and Sun Microsystems's J2EE. However, see Middleware (2003) for performance problems with J2EE. The choice is more likely between Microsoft's .Net and IBM's WebSphere.

¹⁰ Extensible markup language, the stock in trade of the web services industry.

- £45m buys you licences for a lot of Oracle databases on which to store the Google search results.

3.12.18 The most spectacular savings, between £180m and £2,007m, could be made if material cards were excluded from the requirements. The total cost of the scheme would then drop to £432m¹¹ even if nothing is allowed for savings made by using an efficient web services approach to systems development.

¹¹ £45m (central database) + £62m (links to other departments and private sector) + £263m (IT infrastructure) + £62m (additional UKPS staff)

4 DEMATERIALISED ID

4.1 Introduction

- 4.1.1 Digital certificates are tools used by PKI, the public key infrastructure. PKI has a strong basis in mathematics and is designed to certify identity and to authenticate communications between the parties identified.
- 4.1.2 Mobile phones are hand-held computers with powerful telecommunications facilities. They are the ideal device on which to store digital certificates.
- 4.1.3 The conjunction of digital certificates and mobile phones is referred to as "dematerialised ID".
- 4.1.4 Only two references to a comparable idea have been found on the web, see Finland (2003a) and Udell (2003). On the web, that amounts to a closely guarded secret – dematerialised ID is an original idea.
- 4.1.5 Dematerialised ID covers not only individuals but also organisations such as companies and charities. It provides a stronger tool than entitlement cards, as a result, to reduce money-laundering.
- 4.1.6 Mobile phones can be tracked. Dematerialised ID provides a strong tool to increase the clear-up rates on all location-based crime, not just identity fraud.
- 4.1.7 Any supplier who issues any voucher which grants any entitlement to the bearer will benefit from dematerialised ID. The Home Office has the opportunity here to provide a catalyst for e-commerce, barely addressed by entitlement cards, to reduce the costs of doing business in the UK and thus to make the economy more competitive.
- 4.1.8 Early estimates suggest that dematerialised ID could cost about one-seventh of the price of the entitlement card scheme. The benefits are greater and the costs are lower.

4.2 PKI

- 4.2.1 Suppose that you are an officer of the French immigration service on duty in the Arrivals lounge at Charles de Gaulle airport and I present you with my entitlement card. How would you know that it had been issued by UKPS? How would you know that it hadn't been tampered with since it was issued? And how would you know that it had been issued to me, the bearer?
- 4.2.2 These are the same questions that arise with the exchange of encrypted messages. And we know the answers. They come under the general heading of PKI. There is a large literature of PKI, see for example:
- Singh (1999, Chapters 6 and 7 and Appendix J)
 - PGP (1999, Appendix C)
 - Netscape (1999)
 - What is PKI (ITC 2003)
 - NIST PKI Program (NIST 2001)
 - Mobile Commerce FAQ (Nokia 2003a)

- Digital Certificate ID Links ([Security-Online 1997](#))
- 4.2.3 PKI includes: 300-digit prime numbers; cipher algorithms; private keys; message digests; message authentication codes; digital certificates; digital signatures; trusted third parties/certificate authorities; root certificates; registration authorities; public keys; revocation authorities; non-repudiation; ...
- 4.2.4 For present purposes, note that:
- A person's or organisation's private key must be kept secret.
 - Their public key can be published.
 - Public keys may be published by a certificate authority, also known as a "trusted third party".
 - Public and private keys are issued as digital certificates.
 - They are only issued when the identity and entitlement of the bearer have been established by a registration authority.
 - Registration authorities have variable strength checking procedures.
 - In many cases, digital certificates may expire or they may be revoked by a revocation authority.
 - Revoked digital certificates are added to certificate revocation lists, which need to be checked by any supplier relying on a bearer's digital certificate before supplying goods or services to the bearer.
 - A message encrypted with the public key can only be decrypted with the private key.
 - A unique message digest can be calculated for any message.
- 4.2.5 The effect is that, in the case of an encrypted message, the recipient knows that it came from the sender, the sender knows that it can only be read by the recipient and, thanks to the message digest, both know that it cannot be secretly tampered with *en route*. This is exactly what is needed for the entitlement card scheme. PKI provides strong guarantees of identity and authentication.
- 4.2.6 It is not claimed that the encryption methods used are impossible to break, merely that, if procedures are properly followed, it would take several times the age of the universe to break them. When procedures are not properly followed, PKI can fail ([BBC 2003h](#)).
- 4.2.7 We can apply the same technology, PKI, and all its well-worked out methodology to the problem of entitlement cards if we replace material cards with digital certificates:
- The checking procedures followed by UKPS already give it a high international reputation as a registration authority.
 - UKPS is already a globally trusted third party and could operate as its own certificate authority. It could issue private keys to legitimate UK

residents in addition to material passports. And it could publish the public keys¹², thus facilitating a huge [variety of services](#).

- 4.2.8 PKI can be traced to work done on encryption at GCHQ between 1969 and 1975 ([Singh 1999](#), pp.279-92). Several English and US mathematicians made contributions to the theory. RSA (2003), one of the leading PKI companies, was started by three of the US mathematicians, Messrs Rivest, Shamir and Adleman.
- 4.2.9 PKI is heavily used by the intelligence services and the military but is by no means restricted to them. It is used throughout the business-to-business world by big businesses and small. BT, for example, use PKI to allow their suppliers to trade with them on their extranet ([BT 2001](#)). It is also used in the business-to-consumer market whenever consumers shop on secure websites ([Netscape 1999](#)). It is made available free¹³ to the consumer-to-consumer market by PGP Corporation's Pretty Good Privacy product ([PGP 2003](#)).
- 4.2.10 It is not as though the Home Office has not heard of PKI. All public sector communications are secured by PKI. Their digital certificates exist in a hierarchy in which the ultimate certificate authority is GCHQ, who operate the root certificate system. The contract to supply root certificate software has just been awarded to Entrust, Inc. ([2003](#)).
- 4.2.11 Does PKI work? The fact that the UK Government and a huge number of other organisations use it is good circumstantial evidence that they believe that it works.
- 4.2.12 The mathematics involved is difficult to understand. It would be difficult to win the confidence of the whole population by advancing mathematical arguments. A well-presented case, though, can be made to the public so that we finish in the same situation as we find ourselves with DNA. Few people understand what DNA is or how it is used to prove identity but everyone accepts nevertheless that it does prove identity.
- 4.2.13 The Home Office may believe that it is not feasible to operate a wide-scale digital certificate system but it is surprising that PKI is not even mentioned in the consultation paper on entitlement cards when its applicability is so clear.

4.3 Digital certificates

4.3.1 Consider the benefits of digital certificates over plastic cards:

- Multi-colour plastic cards, with their embossed characters, holograms, magnetic strips, ultra-violet light features and embedded chips have high production costs compared with a string of numbers generated by a computer.

¹² The equivalent of a material passport number?

¹³ The reasoning of Mr Phil Zimmermann, the founder of PGP Corporation, was that if the state had access to PKI, so should the people.

- They have high distribution costs by post or courier compared with the phone call needed to transmit a digital certificate from the certificate authority to the bearer.
- Distribution of plastic cards takes hours or days compared with the seconds taken for transmission of a digital certificate.
- If entitlements change, plastic cards have to be withdrawn and re-issued – a long and expensive process compared with revoking and re-issuing digital certificates.
- Digital certificates have local and remote management facilities thanks to the hand-held computers (mobile phones) on which they are stored which simply do not exist for plastic cards.
- Digital certificates form part of PKI and have stronger authentication than plastic cards, which can be counterfeited.
- Plastic cards wear out with use, whereas digital certificates do not.

4.3.2 Several of the ways to take advantage of these benefits are explored in the paragraphs below.

4.3.3 Individuals can and do hold multiple digital certificates. What is envisaged is that an individual might hold one pair of digital certificates¹⁴ issued by UKPS which affirms his identity and any number of other digital certificates issued by other certificate authorities. These others might include a certificate issued to the bearer by:

- ... the Department of Work and Pensions (DWP) which includes a National Insurance number and affirms his right to work.
- ... the Department of Health which includes his National Health Service number and maybe his emergency medical information and organ donation wishes.
- ... the Transport and General Workers Union which includes his membership number and union branch code.
- ... Visa which includes his Visa card number and expiry date.
- ... LloydsTSB which includes his account number and cheque guarantee limit.
- ... Merton Library Service which entitles him to borrow books.
- ... Thresher Wine Shop which entitles him to discounts.
- ... the Automobile Association which entitles him to roadside assistance.
- ... a tennis club which allows him to open the secure doors, switch on the lights on the squash court and pay for drinks at the bar with electronic cash.
- ... the Football Association which guarantees that it is an authentic ticket to the FA Cup Final ([BBC 2003](#)).

¹⁴ One certificate containing the private key and one containing the public key. There is an argument here for having the bearer generate his own pair of keys. If UKPS know his private key, then the bearer may repudiate a document apparently signed by him, digitally, claiming that it was actually signed by a defalcator at UKPS. This argument may be pursued at a later stage.

- 4.3.4 Some individuals might need a digital certificate issued by the Inland Revenue granting them the right to stay in the country for a limited number of days each year, after which they would be liable to UK tax on their overseas income. This entitlement is hard to administer without digital certificates and the computerised management facilities which come with them.
- 4.3.5 Digital certificates, it is suggested, will be stored on mobile phones. Mobile phones can be tracked. The presence of a mobile phone in the UK with one of these Inland Revenue certificates stored on it can be detected automatically. That would give the Revenue the facility to use a computer to count the days and warn the bearer when his time is nearly up.
- 4.3.6 The list may be extended indefinitely. Any organisation which issues any voucher conferring any entitlement on the bearer could become a certificate authority and issue digital certificates instead of material vouchers.
- 4.3.7 It is surprising that the Home Office do not seem to have involved the retail banks and credit card companies in the preparation of the consultation paper. They have millions of customers, international experience and a profusion of cards which entitle you to borrow money or to access your own money. They should be just as interested in this proposal as the Home Office.
- 4.3.8 The retail banks might find digital certificates issued by UKPS and Companies House particularly useful for their know-your-customer initiative which is, in turn, linked with the fight to reduce money-laundering, see Fildes (2002).
- 4.3.9 UKPS could issue a variety of digital certificates. Some would be equivalent to passports and would certify citizenship as well as identity. Others would certify identity and add either an asylum status or the right to stay in the country indefinitely or a visa with a limited right to stay in the country.
- 4.3.10 This conjunction of digital certificates and mobile phones, referred to as "dematerialised ID", has great flexibility. Changes can be made at any time, subject to a dematerialised ID protocol, which needs to be agreed, without having to re-issue millions of cards.
- 4.3.11 A person's UKPS certificate of identity would be pre-eminent and would provide the foundation on which other certificates stand. Having established that you are you, by reference to UKPS, DVLA's or DVLNI's certificate only has to indicate what vehicles you are allowed to drive, when you will have to re-take your driving test and how many points you have on your licence. It does not have to certify further that you are you although, [as noted](#), it might be prudent to have further checks on identity.
- 4.3.12 Digital certificates may be invested with more or less respect depending on the integrity and diligence of the registration authority behind them. There are security assurance standards for measuring the level of trust that you should place in a certificate authority, e.g. ISO 15408 and FIPS 140, see Larroche (2000) and NIST (2002). UKPS cannot afford a debacle like Microsoft's experience, see Hopkins (2003). Nor could any certificate authority.

- 4.3.13 The checking procedures behind digital certificates issued right now by UKPS, in particular, would command the highest respect nationally and internationally. The consultation paper talks of further improvements being made to UKPS registration procedures and so that respect should grow even higher in the future.
- 4.3.14 The consultation paper suggests that retailers could be charged to use facilities on a Government-issued smart card but that they would miss the branding they enjoy on their material cards. Two points:
- The dematerialised ID proposal dispenses with entitlement cards and so there would be no question of the retailers storing their certificates on the Government's entitlement cards.
 - The brand would still be there and surely the retailers might enjoy the lower costs and greater efficiency of issuing digital certificates.
- 4.3.15 Digital certificates can be issued for companies as well as for individuals. Companies House could issue digital certificates in addition to or instead of certificates of incorporation. The combination of those with the digital certificates issued to individuals by UKPS would begin to assemble the armoury required to make a serious attack on money-laundering. Further advances could be made with international co-ordination of PKI.
- 4.3.16 Digital certificates can certify any organisations, whether companies or charities or co-operatives or Government departments or parliaments. They can certify websites. The Charity Commission could become a certificate authority and issue a digital certificate identifying Oxfam. Companies House could issue a digital certificate identifying BCSL.
- 4.3.17 If BCSL then wishes to recruit an employee and needs to enquire as to the right of this potential recruit to work, the enquiry can be sent over the Internet to DWP digitally signed with BCSL's certificate from Companies House. In that way, DWP know that the enquiry comes from BCSL and can send back the potential recruit's work entitlement details, encrypted in such a way that only BCSL can read them.
- 4.3.18 What we have here is a triangle between Companies House, BCSL and DWP. PKI works on a series of these triangulations. BCSL's enquiry to DWP may, for example, include a copy of the potential recruit's digital certificate issued by UKPS. DWP could make an enquiry of UKPS using this certificate. UKPS knows that it is DWP because DWP signs the enquiry with its digital certificate issued by, say, the House of Commons. There is another triangle, this time between DWP, the House of Commons and UKPS.
- 4.3.19 Digital certificates can contain any details, including graphics like photographs, iris patterns and fingerprints, see PGP (1999, pp.47-9). In a national or international system, the contents of certificates must be governed by standards, see for example Sun (1998), but that does not detract from the flexibility.

- 4.3.20 Like a material passport, most digital certificates have an expiry date. But dematerialised passports could be managed in ways impossible for material passports:
- Your mobile phone operating system could warn you months in advance that your UKPS certificate, i.e. your passport, will soon expire.
 - Equally, UKPS could warn you by sending a message to your mobile phone.
 - If you are in the UK on a visa, represented by a digital certificate, your mobile phone could warn you that you have only a week left to leave the country or get the visa renewed.
- 4.3.21 The management possibilities are increased thanks to the use of digital certificates. The fact that these certificates are stored on mobile phones, with all their communications facilities, adds remote management facilities.
- 4.3.22 Digital certificate standards must encapsulate the protocol for their use. This protocol might include the expiry messages displayed in the examples above. We want a polite message, something better than "You have 6.447 days to leave the country". Thanks to dematerialised ID the message may be in the language of the user's choice and delivered either as a voice message or as text or both.
- 4.3.23 The protocol must also include access control facilities. Is BCSL allowed to see the photograph of the potential recruit stored at UKPS? The answer depends on the decisions made in respect of the access control facilities of the certificate standards. Perhaps some Companies House certificates would grant the right to see the photograph and others would not. This is the sort of point that would have to be agreed in the establishment of a dematerialised ID protocol.
- 4.3.24 Dematerialisation would increase the flexibility of feasible protocols. As things stand today, either someone sees your passport, together with your photograph, or they don't. With dematerialised ID, the set of people allowed to see your passport details could be divided into those who are allowed to see your photograph and those who are not.
- 4.3.25 What happens if you lose your mobile phone or it is stolen? Have you, in effect, lost a blank cheque? This danger does exist but can be avoided by the service suppliers and the users taking proper precautions.
- 4.3.26 You might use a password to protect access. It might be possible to incorporate voice recognition software in mobile phones to identify you or to incorporate a fingerprint reader in the mobile phone handset. This issue needs to be investigated and resolved. For the moment, we may take our lead from the UK retail banks and credit card companies, who are moving away from signatures to verify identity during a transaction and towards personal identifi-

cation numbers (PINs), i.e. numeric passwords, see BBC (2003i)¹⁵. The most feasible protection for digital certificates on mobile phones is likely to be a PIN.

- 4.3.27 Digital certificates do not have to exist in a hierarchy with a root certificate at the top. It is also possible to operate on the basis of a web of trust, whereby we all sign each other's certificates and the value of the certificate lies more in community recognition than the authority of a powerful Government organisation.
- 4.3.28 The contention here is that, once more people and organisations come to realise the convenience and power of digital certificates, their use will become widespread¹⁶. That process could be seeded if the Home Office issues digital certificates instead of entitlement cards.
- 4.3.29 The entitlement card scheme as proposed by the Home Office has a negative, punitive feel to it. Dematerialised ID could achieve punishment of the guilty but it could also offer positive benefits to the innocent.

4.4 Revocation authorities

- 4.4.1 If dematerialised ID is implemented as envisaged here, then a person's mobile phone will have several digital certificates stored on it. These certificates may have been issued by any number of certificate authorities.
- 4.4.2 When a mobile phone is lost or stolen or becomes for some other reason unusable, the user will have several certificate authorities to contact to get all the stored certificates revoked and re-issued. He will be hampered in this partly by the difficulty of remembering which certificate authorities to contact and partly by the fact that *ex hypothesi* he no longer has a digital certificate to prove who he is¹⁷.
- 4.4.3 The revocation authority must ensure somehow that he is the legitimate bearer of the digital certificates and not someone maliciously trying to get his certificates revoked. The usual solution is to store between three and five questions at the certificate authority that only the bearer is likely to be able to answer. This is the practice adopted by two of the Internet banks, smile and Intelligent Finance. A reduced form of the procedure is suggested in the Home Office consultation paper. See also Price (2003).

¹⁵ This reference estimates the annual cost of UK credit card fraud at £400m. Digital certificates could reduce that figure.

¹⁶ Their use could become widespread not only in the UK but overseas as well. There could be an international standard for UKPS-equivalent digital certificates. The implications are interesting – a world registration authority? Let us see if we can get a scheme operating in the UK first.

¹⁷ He may have a backup copy on his PC but, given that he is asking for revocation and re-issue, the question of identity must still arise.

- 4.4.4 UKPS could become its own revocation authority. The dematerialised ID idea has already made UKPS into a registration authority and its own certificate authority. Revocation could become a third responsibility for UKPS.
- 4.4.5 Combining certificate authority and revocation responsibilities could be sensible:
- UKPS knows whether it has already revoked an identity certificate. Introducing a separate organisation to which UKPS has to distribute certificate revocation lists seems like an unnecessary step.
 - It is also sensible as, if the UKPS identity certificate does become the pre-eminent proof of identity, then UKPS will receive most of the requests for confirmation of identity. If it logs those requests, then UKPS will know which other certificate authorities are likely to have issued certificates to the user with the unusable mobile. UKPS can contact these other certificate authorities to get their certificates revoked and replacements issued.
 - UKPS, *qua* registration authority, is best placed to establish whether the user with the unusable mobile phone is who he says he is.
- 4.4.6 Although apparently sensible, there may be good reasons to split these rôles. This matter needs to be investigated further.
- 4.4.7 With the present rate of mobile phone theft, revocation authorities are going to be very busy. Mobile phone theft could be reduced if procedures were employed quickly to render the phone useless to a thief.
- 4.4.8 Mobile phone thieves often throw away the SIM (Subscriber Identity Module) of the stolen phone and replace it with one of their own, see James (2002). What they want is the handset.
- 4.4.9 The handset has an IMEI (International Mobile Equipment Identity). That can be easily reset to a legitimate IMEI (*op. cit.*). If the mobile phone network operators barred the IMEI on the stolen phone, they would also be barring a legitimate user. They prefer not to do that even though the effect is to make mobile phone theft worthwhile.
- 4.4.10 IMEI numbers must become hard or impossible to change. Mobile phone network operators must bar¹⁸ stolen SIM and IMEI numbers. Mobile phone theft must be reduced.
- 4.4.11 Note that dematerialised ID would allow certificate authorities, subject to protocol, to revoke certificates at any time and re-issue new ones, cheaply and quickly. In the entitlement card system, by contrast, UKPS may have revoked one of the bearer's entitlements but he still has the card and to the naked eye that means that he still has the entitlement.

¹⁸ It should be impossible for the stolen phone to be used to make or receive calls. It should not be impossible for the phone to associate with the network. Allowing it to do so will mean that it can be tracked and the thief arrested.

4.5 Mobile phones

- 4.5.1 Digital certificates must be stored on some digital medium. Not long ago, it would have been expensive to equip all eligible residents with an appropriate device on which to store digital certificates. Now, however, most eligible residents have already equipped themselves with just the device needed – a mobile phone. This is a public private partnership (PPP) which the Home Office can capitalise on.
- 4.5.2 Estimates vary but it seems that up to 83% of the UK population now has a mobile phone ([Sabbagh 2003a](#)). Compare that with the 0.2% uptake of CitizenCards. Mobile phone adoption is a far-advanced and irresistible evolutionary process. The Home Office could take advantage of it; or it could back the 0.2% horse.
- 4.5.3 The opportunity exists here to dematerialise entitlement cards. There would be no material cards involved. The opportunity is provided by the prevalence of mobile phones. Almost everyone has one and takes it almost everywhere with them. Many people identify with them ([Freaan 2003](#)).
- 4.5.4 Mobile phone operating systems already have many digital certificate management facilities, see Symbian ([2002](#)). Digital certificates offer almost guaranteed authentication, thanks to PKI. If digital certificates are small and the memory available in mobile phones is relatively large, then people could carry several digital certificates around with them all the time.
- 4.5.5 Digitised photographs, iris patterns and fingerprints could all be stored on mobile phones. Indeed, the photograph could be taken by the mobile phone, now that camera-phones are becoming available, and mobile phones could have built-in fingerprint readers, as noted. These images could be displayed on the graphics screen of the mobile phone or on the screen of a PC to which the data has been transmitted. Mobile phones are good at transmitting things.
- 4.5.6 The text facilities of mobile phones open up communications for deaf people and dumb people. Voice synthesisers could be added to mobile phones so that blind people can "see" what is on the screen.
- 4.5.7 Mobile phones are the ideal vehicles of dematerialised ID¹⁹.
- 4.5.8 Instead of adding yet another card to our wallets, the Home Office could start a process which would empty them. They could all be replaced by digital certificates and so could cash²⁰. If the Home Office would dematerialise its entitlement card scheme, that could be a catalyst for e-commerce.
- 4.5.9 83% is not 100%. The Home Office propose a universal scheme. However, they do not propose in general to issue entitlement cards to those under the

¹⁹ Biometric software could be installed in mobile phones.

²⁰ Note the debate whether electronic cash can ever be as anonymous as material cash, see for example Privacy International ([2003b](#)).

age of 16. They exclude a large section of the population from their universe. Mobile phones appeal least to the elderly. A dematerialised ID scheme would in that case exclude from the universe a large section of the population at the other end of the age range²¹. From the point of view of coverage, entitlement cards and dematerialised ID may well be equivalent.

4.5.10 It is suggested here that this lack of universality does not matter. For one thing, it is not generally the elderly who commit crimes or work illegally. For another, 83% coverage is already high and would yield many benefits.

4.5.11 Uptake could be increased slightly by giving people who do not otherwise have a mobile phone one of the millions thrown away every year and sold by the ton to the third world. There is a danger here of people who have paid for their own phone feeling resentful, see Hellen and Winnett (2003).

4.5.12 The scales could be tipped further towards 100% if the benefits of having dematerialised ID became evident. Suppose, for example, that:

- It proves to be quicker to get through Immigration at the airport using a dematerialised digital passport than a material one.
- Credit card companies start to charge merchants a lower commission for digital certificate transactions than for plastic card transactions.
- It is easier to open a bank account or quicker to start work in a new job or easier to guarantee that an FA Cup Final ticket is authentic (BBC 2003d) using digital certificates than material vouchers.

4.6 Tracking

4.6.1 Mobile phone networks, like any other network, cannot be operated unless the location of each associated device is known. That cannot be avoided. Current mobile phone networks in the UK record location in terms of cell ID. Cells are defined by base stations, also known as "radio masts" or "antennae". Each base station has an ID and defines a cell. Assuming that an omnidirectional antenna²² is used:

- In low message traffic areas the cell is a sphere with a radius of several kilometres.
- In high message traffic areas, where there are more base stations, the radius falls to 150 metres or so.

4.6.2 When a mobile phone associates with a base station, i.e. when there is at least one blob of signal on the screen, its location can be narrowed down to the given cell. At any time, the mobile phone network operators can, therefore, detect the location of a mobile phone accurately to within 150 metres or

²¹ For a survey of mobile phone uptake in Tokyo, see NTT (2000b). The UK is not necessarily like Japan. A UK survey must be found. Henley Management Centre (Frean 2003)?

²² The topology of cells varies. Cells can be divided into sectors. Cells can comprise multiple micro-cells. Omnidirectional antennae do not necessarily define spherical cells.

so at best. See BBC (2003e) for an unfortunate example of a case of the mobile phone network being used to find people.

4.6.3 Several questions arise:

- 1 Is location information recorded by the mobile phone network operators?
- 2 If so, for how long are the location records kept?
- 3 What do the mobile phone network operators do with this location information?
- 4 Who else can access the location information?

4.6.4 There is a partial answer to questions 1 and 4 above. During 2002, the UK police and HM Customs & Excise (HMCE) made 500,000 requests for location and/or timing information from the mobile phone network operators, see BBC (2002g). Further investigation is required to establish full answers to all four questions.

4.6.5 The reference makes clear that responding to the police and HMCE requests is a chargeable service. It would be relevant to know how much the Government is spending on these requests²³.

4.6.6 Turning our attention overseas, the Finns are considering the use of mobile phone tracking for road traffic management, see (Finland 2003b). Note that the reference includes the following point: "The organisation [Finnra] is avoiding infringing the privacy of drivers by discarding data once it is used and by using codes that camouflage exactly which mobile phone is being used to time trips".

4.6.7 A friend-finder service is operated in many countries, notably Japan, whereby individual mobile phone users can under certain circumstances see where the other consenting members of their group are on a map displayed on the screen of the phone, see Benefon (2003) and Nokia (2002d).

4.6.8 There are many other cases like this where phone users themselves embrace tracking facilities, see for example:

- Baby-sitting via satellite (BBC 2002a)
- Children's tracking device invented (BBC 2003b)
- Watching your kids' every move (CBS 2003)
- Something to watch over me (NYT 2000)
- With GPS, KDDI finds a new cell-phone audience (Tanikawa 2002)
- 36.5% of adolescent Japanese want navigation/mapping functions on their mobile phone (NTT DoCoMo 2000a)

²³ The operators could do with the money. They are already three years into the 20-year term of their 3G licences and, in the UK at least, they have nothing to show for the £22.5bn (2.75% of UK GDP) they spent on them (Gibson 2002). They are currently seeking to impute a VAT element to that £22.5bn which they could reclaim (Sabbagh2003b). And they are writing down the value of the 3G licences in their books. mmO₂, for example, have reduced the value of their UK 3G licence by £2.1bn or 52.5% and of their German 3G licence by £3.8bn or 74.5% (mmO₂ 2003).

- 4.6.9 If it is not the safety of the children or the pets, it is telemedicine that promotes tracking, see BBC (2002f and 2003g). And if it is not your health, it is businesses sending you advertisements and discount vouchers as you walk past their shops and offices, see Crouch (2001) and Kanaracus (2002) – that is a partial answer to question 3 above. The network operators are paid by companies to send advertisements to you when you are in an appropriate location.
- 4.6.10 And then there are the government initiatives. The US Government, for example, has demanded mobile phone-based location-detection with 50m accuracy for 67% of calls and 150m accuracy for 95% of calls, see FCC (2001). This is in connection with 911 calls made to the emergency services but the effect is that all mobile phones will be locatable all the time.
- 4.6.11 The FCC's E911 directive is being phased in with different deadlines for different operators and different technologies with the final deadline being 31 December 2005.
- 4.6.12 E112 is a European Union initiative similar to the US's E911, see (CGALIES 2003). This initiative requires further investigation.
- 4.6.13 The location-detection technologies being used in the US are EOTD and AGPS. Both technologies are also available in Europe:
- Extended observed time difference is a GSM-specific technology and the leading practitioners are Cambridge Positioning Systems, see CPS (2003). Nokia provide a location-detection service based on EOTD, see Nokia (2001). EOTD may not meet the FCC's accuracy requirements, see Charny (2002) and Harrison (2002).
 - Assisted Global Positioning System is based on GPS, see Dana (2000). GPS cannot always be used, see Banahan (2000) for an amusing and informed description of the problems. AGPS overcomes some of these problems, works with GSM and CDMA networks and already offers, so it is claimed, 5m accuracy, see Qualcomm (2002).
- 4.6.14 It needs to be established what is being located by EOTD and AGPS. Is it a phone number, a SIM number, an IMEI number or the identification number of a separate GPS receiver?
- 4.6.15 While EOTD and AGPS approach greater accuracy in location-detection, other related technologies are overtaking them. 802.11 wireless networks can provide 5ft accuracy, see for example Anhalt *et al* (2003), Carnegie-Mellon (2003), Smailagic *et al* (2001) and Small *et al* (2000). RFID can achieve 50cm accuracy²⁴, see Ekahau (2003a). Ekahau provide a useful starting point for comparing the various location-detection technologies, as do Sarvanko (2002) and Dornan (2001). Start with those and then try Soliman and Wheatley (2002).

²⁴ Other sources say 10", RFID Wizards (2003).

- 4.6.16 EOTD looks as though it has problems achieving accurate location-detection, AGPS seems to be well on the way and the possibility of using multi-protocol mobile phones, incorporating 802.11, looks most promising given the growing prevalence of WiFi hotspots²⁵.
- 4.6.17 Location-detection accuracy is set to grow. At the same time, UK residents remain apparently uninterested in the privacy issues. For example, the London Congestion Charge scheme incorporates Automatic Number Plate Recognition software attached to CCTV cameras, which also photograph the whole car. Identix FaceIT software could be attached as well, allowing you personally rather than your car to be tracked each time you cross the ring of cameras. While Ken Livingstone won *Worst Public Servant* at the 2003 UK Big Brother Awards and Capita won *Most Invasive Company* ([Privacy International 2003a](#)), the scheme has been declared a success and is set to be emulated all over the UK and overseas.
- 4.6.18 Taking all these points together, it seems sensible and fair that the police should have access, when warranted, to the same location information as so many other organisations if it will help them to clear up crimes and other incidents which require detective work.

4.7 Mobile phones and detection

- 4.7.1 The following paragraphs rely on the assumption that the mobile phone network operators store some location data.
- 4.7.2 If a criminal is foolish enough to keep his mobile phone switched on and with him as he commits a crime, then the mobile phone network operator location records could help the police to discover who perpetrated the crime and subsequently to track him down. The location data may also be admissible in court as evidence.
- 4.7.3 The mobile phone network operators will know the telephone number of the phone. They may not know who the user is at that time. In this case, the location data could still be useful if it can later be shown who is the regular user of this phone.
- 4.7.4 A search through the mobile phone network operator records would discover which other telephones had rung this one and which other telephones it had rung. These phones together form a group. If the regular users of a few of the phones in the group can be identified then that would give the police somewhere to start in the search for the criminal.
- 4.7.5 If a criminal is strongly suspected of having committed the crime and his mobile phone was switched off half an hour before the crime was committed and switched on again half an hour later and at both points he was within,

²⁵ WiFi hotspots use 802.11 which operates in the unlicensed, free ISM bands. If hotspots one day achieve the coverage of mobile phone networks, can we look forward then to using VoIP instead of GSM/GPRS/UMTS/CDMA, with their attendant waveband licence fees, and saving money as a result?

say, five miles of the scene of the crime, then that might provide circumstantial evidence of his guilt.

- 4.7.6 If the police are having trouble finding witnesses to a crime or to a serious accident, for example, then a search of the mobile phone network operator records might reveal who was in the vicinity at the time. The police could then approach these people to see if they have any useful evidence to give, see BCSL (2003b).
- 4.7.7 Once caught and convicted, a search of the mobile phone network operator records could reveal who a criminal was previously in regular contact with, which may on occasion help to discover who is the ringleader of a criminal group and who else is involved.
- 4.7.8 What applies to criminals applies equally to terrorists.
- 4.7.9 Location data could also on occasion provide circumstantial evidence of an alibi and help someone to prove his innocence. It could help to find kidnap victims and missing persons.
- 4.7.10 Not all crimes have a location. Tracking by mobile phone will not help with those. But burglaries and muggings, car theft and drug-dealing do have a location and these are the crimes which worry people. Clear-up rates are low. Mobile phone tracking may help to increase them.

4.8 Civil liberties

- 4.8.1 The entitlement card proposal raises civil liberties issues, most of which come under the general umbrella of a fear of the world of Big Brother described in George Orwell's *1984*, see for example Liberty (2003) and Privacy International (2002). Both of these organisations make criticisms of the Home Office consultation paper similar to the points made at section 3 above – the benefits sought do not obviously require entitlement cards.
- 4.8.2 The introduction of a dematerialised ID system based on digital certificates and mobile phones raises similar civil liberties issues to the introduction of entitlement cards and adds a further one – mobile phones can be tracked. At its most Orwellian, dematerialised ID could mean that not only would the Home Office know *who* the citizens and other residents of the UK are but, most of the time, they could know *where* they are.
- 4.8.3 For an exposition of the civil liberties issues raised by tracking, see Clarke (2000) and particularly Penenberg (2001). The attempt to manage privacy while still being tracked is discussed in Levijoki (2000) and Smailagic *et al* (2001).
- 4.8.4 Ethical matters are rarely simple but, on balance, dematerialised ID as outlined above is benign in terms of civil liberties. People do not have to apply for digital certificates and they do not have to use them even if they apply for them.

4.8.5 There are extensions to dematerialised ID, however, which cross the line. These are discussed in the [location identity](#) section below. It is still not simple. There would be benefits to extended dematerialised ID, particularly in connection with crime detection. But, on balance, location identity would probably be on the malign side of civil liberties. In brief:

- ✓ Dematerialised ID = digital certificates + mobile phones
- × Extended dematerialised ID = dematerialised ID + location identity

4.9 Location identity

4.9.1 The Home Office consultation paper offers some criteria for identity (*ibid.*, pp.100-3), which they label as:

- 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 ..."

4.9.2 To these may be added location identity – where you are and where you have been. One person cannot be at two locations at once and two people cannot be at the same location at once. You can be identified by the set of locations you have occupied.

4.9.3 If a person claims on his passport application form to live at post code SW1A 2AB and if the mobile phone network operators' records show that mobile phone number 123 1234 1234 has spent an average of 10 hours a day at 51:30:11N, 0:07:37W over the past year and if their records show that this phone is registered to him, then that is a good indication to UKPS that the person really does live there.

4.9.4 Location identity would be a powerful extra check to be made in the registration procedures operated by registration authorities but is it feasible? Some of the implications are investigated below.

4.9.5 It should be made clear first that location identity would be an extension to dematerialised ID. Dematerialised ID works and delivers benefits even without adding location identity.

4.9.6 In order to extend dematerialised ID, several elements of the current order would have to change. This would bring additional benefits, like strengthened procedures at the registration authorities, but it would also bring additional intrusions into people's privacy which, on balance, probably make the extension unacceptable in terms of civil liberties.

4.9.7 It would, first, be necessary for the mobile phone network operators to know who is the regular user of each mobile phone. They do not currently have this information:

- Pay-as-you-go phones, also known as "prepays", can be bought and used without revealing the identity of the user.
- When companies and other organisations buy mobile phones for their employees, only the name of the purchasing organisation is known, not the names of the users²⁶.

- 4.9.8 Procedures would have to be changed when people buy and upgrade their phones so that their name and address was given and registered with the mobile phone network operator²⁷. With cameraphones, their photograph could also be registered and stored in the SIM of the phone. These changes would probably be unacceptable.
- 4.9.9 The great value of location identity could be in crime detection. The National Criminal Intelligence Service highlight this point in their 2002 threat assessment report (NCIS 2002, §2.38): "In choosing telecommunications products and services, criminals are guided by the need for security, anonymity and convenience. They remain keenly aware of new products and services and take advantage of any that enhance these three features. Mobile phones, in particular prepays, are particularly popular, since there are no legal requirements for registering them and so no need to reveal any personal details. They are also inexpensive enough to be bought in bulk and regularly changed. Organised criminals also make use of telephone kiosks, foreign roaming mobiles (also available as prepay) and satellite phones."
- 4.9.10 Crimes may be committed in the UK or overseas. Crimes in the UK may be committed by UK residents or roaming visitors from overseas. In order to make location identity deliver the greatest crime detection benefits, it would be necessary to implement the UK changes to registration on purchases and upgrades of mobile phones overseas as well. That would require international co-operation, which might or might not be forthcoming.
- 4.9.11 It would then be convenient, from the point of view of the police, if the handshaking protocols were changed so that, when a mobile phone associates with the network, it can only be used to make and receive calls if a UKPS or foreign equivalent digital certificate is stored on the phone and transmitted to the network. That, again, would probably be unacceptable.
- 4.9.12 Identities sometimes have to be created. The Home Office give the example of someone "fleeing an abusive partner" (*ibid.*, pp.44, 63 and 130). There are

²⁶ The same applies to company cars. DVLA and the police do not know who uses a company car. They only know the name of the company to which it is registered. This explains the success of Retainagroup (1998) and similar security businesses, which can make the connection between a car and an individual.

²⁷ See BCSL (2003a, para. 1.21): "While the phone is in an unregistered state, handshaking should allow it to:

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

also the lurid cases of Stakeknife ([MacKay 2003](#)) and Mary Bell. Once location identity was introduced, it would be necessary to devise a protocol to amend the mobile phone records to support the new identity. Entirely new people could be created. To put it another way, existing people could be entirely erased. This is all beginning to out-Orwell Orwell and is probably unacceptable.

- 4.9.13 People change their mobile phone numbers, they have several of them during the course of their life and they may have several at once. They may use different network operators. Establishing their location identity would be a matter of stitching together parts of their history from the records of several phones from several operators. Creating a new identity should replicate that variety – a continuous record on one number with one operator might look suspicious.
- 4.9.14 In order to implement location identity, it would be necessary for the mobile phone network operators to store location information. We know from our itemised bills that they already store the time and duration of calls and the numbers dialled. They would need to store location information in addition and not just the location of billable customers. That would probably be unacceptable.
- 4.9.15 The existing facilities for tracking mobile phones may help the police to clear up crimes. Certainly, that is the hope.
- 4.9.16 However, suppose that they do not. Crimes like muggings and car theft and burglary fall disproportionately on the poor. To abjure location identity then would be to say that the poor are just going to have to live with being mugged and burgled unless you can think of some other way to improve clear-up rates. It would amount to saying that it is alright for the law to be widely flouted. That is why the statements above are repeatedly qualified with "probably".
-

5 DEMATERIALISED ID V. ENTITLEMENT CARDS

5.1 Features

Features	Entitlement cards	Dematerialised ID
Material	Yes – plastic cards, dumb or smart	No – digital certificates
Voluntary	No – everyone over the age of 15 would have one	Yes – although it is expected that uptake would be high as convenience is recognised
Universal	Yes – except that no-one under the age of 16 would have to have one	No – excludes people with no mobile phone, particularly the elderly, and anyone who doesn't want digital certificates
Compulsory	No – cardholders would not have to carry their card with them at all times	No – but as a matter of fact people do tend to carry their mobile phone with them wherever they go
Population register	Yes – from inception of the scheme	Yes – a population register would evolve gradually
Authenticity	No – possible to counterfeit	Yes – all the authentication features of PKI
Communications facilities	No	Yes – all the communications facilities of mobile phones
Remote management facilities	No	Yes – mobile phones are handheld computers which can be interrogated and instructed to carry out commands remotely thanks to telecommunications
Tracking facilities	No – except when card is used	Yes – all mobile phones are tracked as part of normal network management
Improved checking	Yes – addition of biometrics and cross-checks with credit referencing companies	Yes – cross-checks with credit referencing companies. Maybe biometrics based on photographs. Iris prints and fingerprints only if technology proves itself
Biometrics	Yes – if stored on the chip in a smart entitlement card	Yes – biometrics may be stored in digital certificates on mobile phones or alternatively only stored at the certificate authority and accessed remotely subject to authentication of the enquirer

5.2 Cost-benefit

	Entitlement cards	Dematerialised ID
Cost – total	£1.318bn-£3.145bn	£0.432bn+
Cost – vouchers	Material cards – £0.180bn-£2.007bn	Digital certificates – £0.000bn
Cost – Extra equipment	£69m acquisition + £29m operation + £608m biometrics network = £706m	Uncosted. Infra-red and/or Bluetooth-enabled equipment. The mobile phones have already been paid for by the population – PPP. Certificate authorities would have to pay to acquire and operate PKI software
Benefits	Some measures to counter identity fraud. Limited deterrents against money-laundering. No benefits so cogent as to warrant the introduction of the scheme	Strong on identity fraud. Strong on money-laundering. Could improve clear-up rates on all location-based crimes. Could promote e-commerce

5.3 Entitlement cards – SWOT

Entitlement cards
<p>Strengths</p> <ul style="list-style-type: none"> • People are used to plastic cards • Reduce identity fraud and money-laundering
<p>Weaknesses</p> <ul style="list-style-type: none"> • ID card schemes rejected in UK since 1952 • Public services – introduction of entitlement cards quite independent of/nothing to do with improving efficiency of delivery • Illegal immigration and illegal working – already covered by work permits and application registration cards • Not compulsory – limits effectiveness • Under-16s excluded • No deterrent against the crimes which worry people – muggings, burglaries, ... • Fingerprints not recorded to legal standard for proof of identity • Doubts about reliability of biometric equipment • Passport – already have passports • CitizenCard, similar product, not popular, 0.2% uptake • Vulnerable to counterfeit • Expensive to produce and distribute • Inflexible – issue and recall take a long time • No remote management facilities • None of the strong authentication of identity of PKI • Wear out with use • Lack of space to record information visible to the naked eye • Need to use call centres a disincentive • Use of premium rate telephone numbers a disincentive • Single point of weakness in entitlements system increases vulnerability to fraud • Limited catalyst for e-commerce • Expensive additional equipment required • Cover individuals only, not companies, charities, ... • Voting – introduction of entitlement cards quite independent of/nothing to do with convincing people of value of voting • Medical information and organ donation – already have donor cards, allergy bracelets, ... • No statistical evidence that the introduction of such a scheme works • Expensive – £1.318bn-£3.145bn • Poor record of delivering large IT systems on time and on budget
<p>Opportunities</p> <ul style="list-style-type: none"> • Plastic card manufacturers, embedded chip manufacturers and card-reader manufacturers could make a lot of money • Biometric software and hardware suppliers could make a lot of money
<p>Threats</p> <ul style="list-style-type: none"> • Political unpopularity – ID cards have been rejected in the UK since 1952 • Economic unpopularity – waste of taxpayers' money if the scheme doesn't deliver • Loss of reputation – UK could be seen as plodding along with old technology while Finland takes the lead • Adverse publicity – criticisms from civil liberties organisations

5.4 Dematerialised ID – SWOT

Dematerialised ID
<p>Strengths</p> <ul style="list-style-type: none"> • PKI – strong authentication of identity • PKI – long academic history proving reliability • PKI – proof against counterfeit if procedures followed • PKI – already in use nationally and internationally in Government and commerce • Digital certificates – cheap/free to produce • Digital certificates – quick to distribute • Digital certificates – easy to revoke and re-issue via mobile phone • Digital certificates – flexible • Digital certificates – remote management facilities, e.g. managing complicated entitlements granted by Inland Revenue • Digital certificates – do not wear out with use • Digital certificates – appeal to banks and credit card companies • Capitalises on the voluntary mass adoption of mobile phones • Mobile phones – almost universal uptake • Mobile phones – carried by users everywhere • Mobile phones – paid for by users • Tracking facilities – assist clear-up rates of the crimes that worry people • Tracking facilities – assist in non-criminal serious incidents, e.g. finding missing persons, finding witnesses to an accident • Promote e-commerce – any supplier who issues any voucher which grants the bearer any entitlement will benefit • E-commerce – reduce some costs of doing business, e.g. no plastic cards to manufacture and distribute, reduced credit card fraud • E-commerce – improve competitiveness of economy • Extends beyond individuals to cover companies, charities, trade unions, associations – part of co-ordinated deterrent against money-laundering • Relatively cheap – £0.432bn+
<p>Weaknesses</p> <ul style="list-style-type: none"> • People may find digital certificates exotic to start with • Hard to explain mathematics of PKI • No data visible to the naked eye • Poor record of delivering large IT systems on time and on budget • Single point of weakness in entitlements system increases vulnerability to fraud • New idea, unproven
<p>Opportunities</p> <ul style="list-style-type: none"> • UK could be seen as a world-leader making imaginative use of technology • Scheme could be adopted worldwide, like privatisation • PKI suppliers could make a lot of money
<p>Threats</p> <ul style="list-style-type: none"> • Plastic card manufacturers, embedded chip manufacturers and card-reader manufacturers will oppose the scheme • Economic unpopularity – waste of taxpayers' money if the scheme doesn't deliver • Adverse publicity – criticisms from civil liberties organisations

6 FEASIBILITY

6.1 Introduction

- 6.1.1 Dematerialised ID is a new idea. Its feasibility must be investigated.
- 6.1.2 Scenarios are worked out in detail below for some uses of dematerialised ID.
- 6.1.3 The mobile phone operating system requirements are identified. Many are already satisfied and the rest can probably be developed quickly, well within the three-year timescale for deployment of the dematerialised ID scheme²⁸.
- 6.1.4 It is assumed that the cost of enhancing mobile phone operating systems will be borne by the handset manufacturers.
- 6.1.5 The near-field telecommunications requirements are identified and a selection of the relevant technologies available is described. There is a wide choice and it seems likely that, between them, they will be able to meet the outstanding requirements.
- 6.1.6 It has not been possible to estimate the costs of the extra telecommunications facilities required. The unit prices are low. It is likely that many organisations already have the requisite equipment and that there will, therefore, be no extra costs for them.
- 6.1.7 Many organisations will be converted by dematerialised ID into certificate authorities. They will need to subscribe to a PKI service or acquire PKI software themselves, together with computers, staff and high capacity telecommunications facilities. No estimate has been provided for this cost.
- 6.1.8 This is a first attempt at requirements elicitation for dematerialised ID. More research is needed before, for example, the contents of the population register required by dematerialised ID can be specified. Prototypes need to be developed. The sponsors of dematerialised ID need to see proof of concept.

6.2 How a scheme might work in practice

- 6.2.1 How will a mobile phone be used in practice to pay for the groceries in Sainsbury's? The following scenario is suggested:
- 1 Your groceries have been scanned and packed, the cash register is displaying the total amount to pay and broadcasts a message saying Sainsbury's £101.74 Pay? which displays on three lines on your mobile phone.
 - 2 You press the Yes button, a list of your credit cards is displayed, you scroll down, highlight Visa and press the Yes button.
 - 3 You are prompted and enter your PIN and press the Yes button.
 - 4 The payment is authorised by Visa and confirmed on the screen of the phone and on the cash register display.
 - 5 Extra points are added to your Nectar balance.

²⁸ Assumed to be 2004/4 to 2006/7, as for the entitlement card scheme.

- 6 Your phone receives a voucher for 4p off a litre of petrol at Sainsbury's garages if used within 30 days.
- 7 The assistant hands you a material receipt.

6.2.2 That is one scenario. Alternatively:

- You may pay with cash or a material credit card or a cheque, in which case either the *Pay?* Message on your mobile phone is cancelled by the cash register or it disappears because it is automatically timed out after 30 seconds, say.
- There may be a step 1A, which offers to reduce the amount payable by using your stored Nectar points.
- There may be a step 1B, which offers you a cashback so that you pay more but the assistant hands you some cash at step 7 in addition to the receipt.
- The customer may use a LloydsTSB digital debit card rather than a Visa digital credit card at step 2.

6.2.3 Once real retailers review the script above, the words and the order of events will no doubt be changed considerably. Also, it may be possible to store scripts and to speed up the whole process by just getting the phone to execute *MySainsbury'sScript* in one go. However, some features should be retained:

- The script is initiated by the cash register. There is no need for the customer to fumble with his mobile phone looking for the WAP (wireless application protocol) services menu option and then logging on to the right service, all of which is too complicated and takes too long.
- The customer's phone is not permanently broadcasting his identity.
- The customer has to press buttons to affirm his willingness to be a buyer.
- Throughout the transaction, the identity of the customer is guaranteed by PKI. The only way the entitlement to use Visa can be on that phone is because there is a UKPS digital certificate on it first. Visa will have checked with UKPS that this is the certificate for their client before issuing the Visa certificate. The PIN number adds further proof that this customer is who he says he is. The risk of identity fraud/credit card fraud is reduced. The credit card company can afford to reduce the commission they charge Sainsbury's. Sainsbury's can afford to reduce their prices. This is e-commerce.

6.2.4 Opening the secure doors at your tennis club could work in a similar way. The lock could broadcast a message, all the time except when the door is actually open, asking if you want to open the door. Your phone displays *AELTC Door Open?* And you press the *Yes* button. Switching on the lights on the squash court would involve a similar script. Buying a drink at the bar could involve the use of electronic cash rather than Visa but is otherwise similar.

- 6.2.5 In each case you just need your phone, you don't need a club membership card, you don't need a credit card or a debit card or a cheque book or a cheque guarantee card and you don't need any cash.
- 6.2.6 Note how e-commerce turns so many suppliers into certificate authorities. In the examples above, it is not just UKPS but also Visa, Nectar and the tennis club who have issued digital certificates granting entitlements to the bearer.
- 6.2.7 The Football Association can issue digital certificates instead of tickets, as noted. They will need to buy some PKI software and implement new procedures. These costs will ultimately be recouped by the savings on material voucher production and distribution and the reduction in fraud.
- 6.2.8 When it comes to the case of a UK resident using a digital certificate instead of a material entitlement card or passport to get through Immigration at an airport or other port, the desired scenario is that:
- ... thanks to his mobile phone being switched on,
 - ... as he walks up to the immigration officer,
 - ... his UKPS photograph is displayed on a big, high quality graphics screen,
 - ... making it easy for the immigration officer to compare it with the UK resident's face
 - ... and let him into the country.
- 6.2.9 Alternatively, Identix FaceIT software may be used to compare the photograph with the UK resident's image caught on a nearby CCTV camera. This avoids the need to use a human immigration officer. That is not necessarily a good idea and is not recommended here²⁹.
- 6.2.10 In order for this to work, the following infrastructure must exist:
- The immigration service at the airport must have been issued with a digital certificate, perhaps by the department of internal affairs of whichever country.
 - Having identified themselves as the immigration service using this certificate, they must then have been granted a certificate from UKPS³⁰.
- 6.2.11 The immigration service must know the UKPS public keys of all the UK resident passengers on the incoming flight. It is suggested that passengers will use their mobile phones to copy their UKPS public keys to a PC in the departures lounge when they are issued with their boarding passes. The UKPS public keys can then be transmitted to the immigration services at the

²⁹ If biometrics are being used, of course, whether iris patterns, fingerprints or facial geometry, then the comparison has to be made by a machine.

³⁰ Note the variety of digital certificates which UKPS must be able to issue. There are a lot of elements of the dematerialised ID protocol.

various destination airports to arrive well ahead of the aeroplane and the passengers.

- 6.2.12 Some time before the flight arrives, the immigration service must log on to the UKPS servers, identify themselves using their UKPS certificate, enter the passengers' UKPS public keys and download their photographs³¹ from UKPS. This should be done hours before the flight arrives. Otherwise, poor performance of the telecommunications facilities involved or surges in demand on the UKPS servers could cause long queues to build up at Immigration.
- 6.2.13 At this stage, the immigration service have a collection of photographs, which need to be matched with the passengers as they make their way from baggage reclaim in an unpredictable order to the immigration service desk. Some communication between a passenger's mobile phone and the immigration service PC must choose his photograph from the collection, based on the public key, and display it on screen.
- 6.2.14 If the passenger has, say, three children travelling with him on his UKPS certificate, their photographs must be displayed as well.
- 6.2.15 We haven't closed the triangle here. The immigration officer believes that the person in front of him looks like the person in the photograph. He knows that the photograph came from UKPS and he trusts UKPS's registration procedures to be good enough to know that this is a photograph of the person to whom the public key was issued. The private key, however, has not been tested³². The following procedure is suggested. A real cryptographer will probably think of a better one:
- 1 The immigration officer's PC should generate a random n -digit number, encrypt it with the public key and transmit the ciphertext to the mobile phone in the communication session referred to above.
 - 2 The mobile phone should decrypt the ciphertext and transmit the plaintext³³ number back to the PC.

³¹ Sometimes it is worth documenting ideas which have been rejected:

- The first idea here was to download photographs (JPEG files, say) encrypted with the passengers' public keys. The immigration service would not be able to see the photographs on their PCs until they had been decrypted using the passengers' private keys. The idea was to avoid having copies of people's photographs stored all over the world. It was rejected because it would be difficult to decrypt the photographs without running the risk of revealing the private keys, which could be stored on the immigration service PCs.
- The photographs displayed could come from the passengers' mobile phones. It was decided that authentication will be stronger if the photographs come directly from UKPS.

³² It is conceivable that the person who submitted the public key in return for a boarding pass is actually an impostor who has had plastic surgery.

³³ It is important here that only plaintext is returned from the mobile phone to the immigration service PC. There is a passive application running on the mobile phone. If the immigration service PC sent hundreds of requests to the mobile phone and had access to the ciphertext produced, then it would stand a chance of working out the passenger's private key.

- 3 If it matches the original, then the PC can confirm to the immigration officer that the person in front of him has the correct private key, perhaps by displaying his name diagonally across the picture on the screen followed by the word `Confirmed`³⁴.
- 6.2.16 The procedure at the Immigration end of the flight described above is largely passive or hands-free as far as the passenger is concerned. He only has to have his mobile phone switched on. He does not have to press any keys. Further research may determine that this is insecure and that some affirmation from the passenger is preferable.
- 6.2.17 In each scenario above, the bearer of the digital certificate is present at the point of service. What happens if he is not? How do you prove your entitlement to AA roadside assistance from the junction of Roehampton Lane with the A3 where you have broken down? The following scenario is suggested:
- 1 You dial the AA call centre and press the option for roadside assistance.
 - 2 The call centre initiates a session which asks you to confirm your AA membership.
 - 3 You press the `Yes` button and your AA public key is transmitted to the call centre, perhaps together with your location, as identified by the mobile phone network.
 - 4 The call centre checks that this is an AA public key and that it has not expired or been revoked.
 - 5 The call centre sends a random n -digit number to your mobile phone encrypted with your public key.
 - 6 Your mobile phone decrypts the ciphertext and sends back the plaintext number.
 - 7 If the returned number matches, then a human operator takes the details of the breakdown and despatches an AA van.
- 6.2.18 The AA script above is not unlike the T-Mobile script people execute when they register a new pay-as-you-go card to top up their balance. T-Mobile also have a script to pay by debit card.
- 6.3 Digital certificate management**
- 6.3.1 In order to support the scripts above, there must be certain digital certificate management facilities in mobile phones.
- 6.3.2 Under dematerialised ID, when someone applies for a first passport or a passport renewal or a driving licence or when they are issued with a National Insurance number, they will be offered a digital certificate in addition to or, perhaps one day, instead of a material one.
- 6.3.3 People may apply at any other time as well for a digital certificate.
- 6.3.4 The certificate authorities may offer digital certificates at any time.

³⁴ If there is a family group in front of the immigration officer, then all the private keys on the mobile phone must be checked, adult and children, and all confirmed on the immigration service PC.

- 6.3.5 In order to issue them, the certificate authorities must know the applicant's mobile phone number. The certificate will be transmitted from the certificate authority to the applicant's mobile phone.
- 6.3.6 In order for UKPS and other certificate authorities to issue digital certificates, there must be some facility in the mobile phone operating system to receive, store and manage them.
- 6.3.7 Present practice allows adults with a young family to add their children to the parents' passports. There will have to be a similar facility with digital certificates if dematerialised ID is implemented. The mobile phone will need some facility for managing multiple identities.
- 6.3.8 People are already used to performing on-line transactions on PCs, shopping with a credit card on <http://www.amazon.co.uk>, for example. They will not want to have to shop using their mobile phone, with its tiny keypad and poor quality graphics screen when they could be using a PC. PKI provides strong authentication and so reduces the likelihood of credit card fraud. The credit card companies will want the same strong authentication of identity from PC transactions as from mobile phone transactions.
- 6.3.9 There will, therefore, have to be some facility in the mobile phone operating system to copy the UKPS digital certificate and any other certificates from the mobile phone to the PC and Amazon will have to change their payments script to take these certificates into account.
- 6.3.10 Not only will this facility assist e-commerce, it will also provide an essential backup facility. And it will facilitate the scenario described [above](#), where someone is applying for a new job and the prospective employer wishes to send the applicant's UKPS digital certificate to DWP to check his entitlement to work.
- 6.3.11 Restoring from the backup will involve copying from the PC to the mobile phone. So, two-way copying facilities between PCs and phones will be needed.
- 6.3.12 If you can copy your private key back from a PC to your mobile phone, then so can someone else unless you have taken care to protect it on the PC with a password.
- 6.3.13 People change phones. They will want the digital certificates stored on the old phone to be transferred to the new one. If this amounts to more than simply taking the SIM out of one phone and putting it in the other, then there will have to be a facility to copy certificates between mobile phones.
- 6.3.14 When people use their digital certificates, the service supplier will often check the identity of the bearer with the certificate authority. It is conceivable that this check could pass on the mobile phone number of the bearer. If it does not match the phone number recorded at the certificate authority, perhaps because he has changed phones, then the certificate authority could

store the new number to keep track of the set of mobile phones used by the bearer of their certificate.

- 6.3.15 If this practice is deemed to be unacceptable from the point of view of civil liberties, then it must be banned in the dematerialised ID protocol agreed.
- 6.3.16 Digital certificates often have an expiry date. This needs to be monitored automatically by the mobile phone operating system so that the bearer can be alerted in advance that a certificate is about to run out and can take action accordingly.
- 6.3.17 Digital certificates sometimes need to be revoked. Visa, for example, may want to revoke a card if the account holder has not made his monthly payments for some time. Subject to the agreed protocol, Visa could do so by issuing a new digital certificate, with no right to buy on credit, which replaces the old one.
- 6.3.18 Although a certificate authority may revoke the certificate on your mobile phone, they will not be able to over-write any copies you have made on your PC. They will, therefore, have to maintain certificate revocation lists. These will have to be checked by the suppliers of goods and services whenever you try to use your entitlement to see whether it has now lapsed.
- 6.3.19 Certificate revocation lists need to be checked whenever someone tries to use an entitlement³⁵, whether using a digital certificate or a material one. Consider the example of a football hooligan banned from overseas travel to football matches. His name will appear on a certificate revocation list. This list must be checked, whether he is travelling on a digital passport or a material one.
- 6.3.20 People may need to delete digital certificates from their mobile phones. This facility should be carefully protected so that the bearer cannot delete them by mistake. For obvious reasons, there is no need to provide insert and amend facilities for digital certificates.
- 6.3.21 The facilities required for digital certificate management on mobile phones arise from consideration of just a few use cases – getting through immigration, paying for groceries, obtaining roadside assistance, and so on. The list will grow as a more comprehensive review is conducted.

6.4 Software facilities

- 6.4.1 The question now is to what extent mobile phone operating systems and telecommunications technologies can cope with these requirements.
- 6.4.2 Bringing together the points above, mobile phones will need to have facilities to:

³⁵ The biggest revocation list in the world is apparently the list of lost and stolen credit cards. The question arises whether the list should be centralised at the revocation authority or distributed. The credit card revocation list is successfully distributed, see Anderson *et al* (1998).

- 1 Receive a digital certificate over the mobile phone network, store and manage it.
- 2 Display the contents of the certificate.
- 3 Copy a digital certificate to another mobile phone³⁶.
- 4 Receive a digital certificate from another mobile phone.
- 5 Manage a second person's digital certificate on the same mobile phone.
- 6 Copy a digital certificate to a PC:
 - ... for backup.
 - ... so that the user of the PC would have strong identity authentication.
 - ... to provide a copy of the bearer's public key in exchange for a boarding pass.
 - ... to have work entitlement checked with DWP.
- 7 Receive a digital certificate from a PC:
 - ... when restoring from a backup.
 - ... when transferring from one mobile phone to another via a PC.
- 8 Check for dependencies, e.g. a Visa certificate can only be stored if there is already a UKPS certificate.
- 9 Regularly check a stored digital certificate and alert the bearer to its impending expiry.
- 10 Overwrite/revoke an existing certificate.
- 11 Delete a certificate.
- 12 Respond to a broadcast request/invitation to:
 - ... pay for something from a cash register.
 - ... open the door.
 - ... switch on the lights.
 - ... prove the entitlement to get into a major event such as the FA Cup Final.
 - ... prove membership of a given trade union.
 - ... prove the bearer's age.
 - ... prove that the bearer may borrow a book from the library.
 - ... list medicines to which the bearer is allergic.
 - ... specify the organ donation wishes of the bearer.
 - ... vote for a candidate on a (digital?) ballot paper.
- 13 Conduct a communications session with:
 - ... a credit card company to authorise payment using a digital credit card.
 - ... a loyalty card company to use points or to accrue points.
 - ... a bank to authorise payment using a digital debit card.
 - ... an electronic cash service to pay for something.
 - ... an automobile association to obtain roadside assistance.
 - ... an immigration service to obtain entry into a country.

6.4.3 That is the demand side.

³⁶ There might also be a facility to copy your public key to someone else's mobile phone, comparable to exchanging business cards, a facility previously available on the old Palm III personal digital assistant, circa 1997.

- 6.4.4 On the supply side, mobile phones are computers with powerful telecommunications facilities. They have processors and memory. They have peripherals like keypads, speakers and screens. They have an operating system³⁷ and applications that run under it.
- 6.4.5 In many cases mobile phones provide an open platform capable of expansion – other organisations, not just the handset manufacturer, can develop applications, written principally in the Java or C++ programming languages, which can be downloaded to expand the facilities already on the phone, see for example Nokia (2003b and 2002a).
- 6.4.6 Some digital certificate management facilities are already provided and used, see for example Symbian (2002) or scroll through the menu options of your own mobile phone.
- 6.4.7 Issuing a digital certificate and many of the other functions listed above require a mobile phone to react to an event and take action on the basis of commands issued remotely while the user remains passive. This is not a new facility. It happens every day already. Just consider:
- People can send you SMS text messages (short message service) and MMS multimedia messages (multimedia messaging service) and, with no action required by you, the message is stored and you are alerted to its existence.
 - You are alerted when someone has sent you a voice message.
 - The phone rings when someone calls you without your having to do anything.
- 6.4.8 Checking the expiry of a digital certificate requires a mobile phone to take regular action. Again, it happens every day. The mobile phone:
- ... monitors the battery and alerts you when it needs re-charging.
 - ... communicates with the mobile phone network, associating with base stations, monitoring signal quality and roaming from one operator to another.
- 6.4.9 Authorising a credit card payment and calling for roadside assistance from an automobile association require communications sessions and are not dissimilar to:
- ... having a voice conversation with someone or a text chat.
 - ... registering your pay-as-you-go card or using a debit card to (pre-)pay for your calls.
 - ... downloading a game or a ring-tone.

³⁷ According to a talk given at the London Business School (LBS 2003) by the Chief Executive Officer of Symbian, of the 400m new handsets sold every year worldwide, the operating system on 397.3m of them is supplied by the handset manufacturer. Symbian, Palm, Microsoft, Apple and "Linux/GNU" share 0.675% of the new handset market between them.

- ... logging on to a WAP service to find the time of the next train to Cambridge, see Kizoom (2000).
- 6.4.10 It takes about 18 months at the moment (LBS 2003) from the initial design of a new handset and operating system facilities to their appearing on the market. The three years planned for deployment of the dematerialised ID scheme would allow for two complete iterations of the handset development process.
- 6.4.11 There are some facilities obviously missing from standard mobile phone operating systems which will be required by dematerialised ID:
- There is no facility to enforce dependencies between certificates³⁸.
 - There is no facility at the moment to distinguish different users who share one phone, needed in future if a father, say, has his three children's UKPS digital certificates stored on his phone.
- 6.4.12 The concept exists on PC email clients, where there is usually an identity-switching function. But PCs are regularly used by several people. The cases where a mobile phone has a use for several people are rarer.
- 6.4.13 Symbian could write an identity-switching application and release it on a few phones. Once this component has been tested and proved, it could be adopted by the major mobile phone operating systems.
- 6.4.14 Further research needs to be done to compile a comprehensive list of outstanding facilities. It is highly likely that the manufacturers could supply these facilities in the timescales available and at no cost to the UK Treasury.

6.5 Telecommunications facilities

- 6.5.1 Mobile phones in the UK are moving along an upgrade path from the second generation (2G) telephony protocol GSM, through 2.5G GPRS towards 3G UMTS/CDMA.
- 6.5.2 People have, until now, changed their handset fairly frequently, perhaps once a year. That may not continue. In order to implement dematerialised ID, it will for some years be important, therefore, to ensure that the software facilities required are backwards-compatible with GSM and not restricted to 2.5G or 3G phones.
- 6.5.3 More and more, mobile phones support multiple communication protocols:
- In addition to the telephony protocols above, some of them support WAP, TCP, IP and HTTP for wide area networking over the Internet.
 - See Nokia (2002f) for a discussion of how secure virtual private network communications can be implemented on mobile phones.

³⁸ There is, however, a template in the software components industry. Microsoft DLL files used to be issued with DEP files, which listed dependencies. The lessons learned more recently about the deployment of software components may be useful to this digital certificate issue.

- For local or personal area networking some of them support 802.11, Bluetooth, IrDA and USB.
- 6.5.4 The personal area networking facilities are of particular interest here. If you are at the immigration desk at an airport and your mobile phone has successfully connected via Bluetooth, say, to the immigration officer's PC, then your photograph will appear on his screen.
- 6.5.5 Or will it? Why wouldn't the photograph of the man behind you appear? His mobile also may have connected to the PC. If you are asked on your mobile in the check-out at Sainsbury's to pay £101.74, is that your bill or the bill of the man in the next aisle? Some of these networking technologies are too good. They work over too wide a range.
- 6.5.6 This problem needs to be solved. Some of the candidate technologies are reviewed below.
- 6.5.7 Infra-red (IrDA) is out of favour at the moment but as it was designed precisely so that one device and one device only can connect to one other device at a time over a very short range. Dematerialised ID may resurrect interest in infra-red, see [Counterpoint](#) and [IrDA \(2003\)](#).
- 6.5.8 IrDA has largely lost mobile phone market share to Bluetooth³⁹. Bluetooth is the more common technology now. It may be used to connect the handset of a mobile phone to a wireless earpiece, for example, or to copy telephone numbers from a personal digital assistant to the mobile phone. From that point of view Bluetooth is more likely than IrDA to provide the basis for a solution to the one-to-one-only problem above, see [Bluetooth \(2003\)](#) and [NewsTrove \(2002\)](#).
- 6.5.9 802.11 could also be considered for the same reason, its growing prevalence. WiFi hotspots are gradually being installed in more and more public areas such as hotels and airport lounges, see [Keene \(2003\)](#), [Ward \(2003a\)](#) and [Wi-Fi \(2003\)](#).
- 6.5.10 RFID may be a candidate technology. Low frequency RFID tags (100-500kHz), also known as "transponders", have a range up to 10", require no power source of their own (they use a current induced by the tag reader) and are cheap – they currently cost 40¢ each and the RFID industry is aiming for 5¢, see [HID Corporation \(2002\)](#), [RFID Wizards \(2003\)](#), [Philips \(2002\)](#) and [AIM Global Network \(1999\)](#).
- 6.5.11 Further research is needed to devise a reliable one-to-one-only link so that it is your photograph that is displayed and your groceries bill that is paid, not someone else's. Clearly there is a wide variety of technologies to choose from. As it happens, costs are not high. Often service suppliers already have the technology installed on their computers.

³⁹ It still seems to be supplied with laptops.

- 6.5.12 The solution is likely to involve very low power (short range, cheap, safe/low radiation) uni-directional antennae and Bluetooth. It may be sensible to provide multiple solutions: 802.11 for some devices, particularly laptops; and Bluetooth for others, particularly mobile phones.
- 6.5.13 A solution is likely to be found but, if it is not, then we have an alternative. The scenarios above call for a passive experience on the part of the mobile phone user. He need do nothing for the request to pay his groceries bill to appear on his phone or for his photograph to appear on the immigration service PC screen. The scenario could be changed so that he has to press some buttons on the phone.
- 6.5.14 The cost to most organisations of adding Bluetooth or 802.11 connectivity to their existing equipment, if they don't already have them, is low. 802.11 and Bluetooth access points each cost from £60 upwards and adapters cost from £25 upwards, see [Simply Computers \(2003\)](#).
- 6.5.15 The major cost which dematerialised ID adds will fall on the organisations which become certificate authorities. They will have to buy PKI software and the computers to run it on, employ people to run it and rent high capacity telecommunications facilities. Larger organisations such as UKPS and Companies House would presumably follow this route, while smaller organisations subscribe to a PKI service.
- 6.5.16 These costs will be mitigated by savings on the production and distribution costs of material vouchers, by reductions in transaction costs and by the reduced incidence of fraud – all thanks to the strong authentication of identity provided by PKI.
-

REFERENCES

Comments are added after the reference unless self-explanatory.

URLs have not been typeset. It looks ragged but this way the reader can cut and paste into the browser address bar and go, without having to remove soft hyphens first.

3G (2002) *3G News and Information* [WWW] Available from: <http://www.3g.co.uk/> [Accessed: 16 January 2003]

Acterna (2001) *GSM Pocket Guide* [PDF] Available from: http://www.acterna.com/united_kingdom/technical_resources/downloads/app_notes/gsm_SW-EN-PG02-1100-AE.pdf [Accessed: 18 February 2003]

AIM Global Network (1999) *Radio Frequency Identification – A basic primer* [WWW] Available from: http://www.aimglobal.org/technologies/rfid/resources/papers/rfid_basics_primer.htm [Accessed: 24 May 2003] *AIM = trade association for RFID industry (ISO 14443) also bar codes, biometrics, OCR, ...*

Alpine (2003) *Alpine Electronics, Inc.* [WWW] Available from: <http://www.alpine.com/english/products/products.html> [Accessed: 28 January 2003] *GPS, in-car satellite navigation*

Alvarion (2003) *Broadband Wireless Access* [WWW] Available from: <http://www.alvarion.com/RunTime/HomePage.asp> [Accessed: 15 January 2003] *Incorporates BreezeCOM, 802.11 product suppliers*

Ananova (2003) *Benetton clothing to carry tracking transmitters* [WWW] Available from: http://www.ananova.com/news/story/sm_759516.html?menu=news.technology [Accessed: 6 May 2003] *RFID tags in clothes*

Anderson, Ross J., Crispo, Bruno, Lee, Jong-Hyeon, Manifavas, Charalampos, Matyas, Vaclav Jr, and Petitcolas, Fabien A. P. (1998) *The Global Trust Register* [WWW] Available from: <http://www.cl.cam.ac.uk/users/cm213/Publications/gtr.html> [Accessed: 21 May 2003]

Anhalt, Joshua, Smailagic, Asim, Siewiorek, Daniel P., Gemperle, Francine, Salber, Daniel, Weber, Sam, Beck, Jim and Jennings, Jim (2001) *Toward Context-Aware Computing: Experiences and Lessons* [PDF] Available from: <http://www.cs.cmu.edu/afs/cs.cmu.edu/project/coda-www/mcsa02/PAPERS/anhalt01.pdf> [Accessed: 2 April 2003] *May/June 2001 IEEE Intelligent Systems pp. 38-46 Location-detection 15ft accuracy using 802.11*

Banahan, Mike (2000) *Location Aware Services – Beware* [WWW] Available from: <http://ebusiness.gbdirect.co.uk/ouropinions/locationaware.html> [Accessed: 20 January 2003]

BBC (2000) *Satellite navigation accuracy boosted* [WWW] Available from: <http://news.bbc.co.uk/1/hi/sci/tech/733292.stm> [Accessed: 30 April 2003] *GPS, military quality now available to civilians*

BBC (2002a) *Baby-sitting via satellite* [WWW] Available from: <http://news.bbc.co.uk/1/hi/technology/2181469.stm> [Accessed: 30 April 2003] *GPS receiver in children's watches*

BBC (2002b) *Experts check passport changes* [WWW] Available from: <http://news.bbc.co.uk/1/hi/sci/tech/1833939.stm> [Accessed: 7 May 2003] *At least three different reasons for changing passports advanced so far*

BBC (2002c) *Hi-tech security flaws exposed* [WWW] Available from: <http://news.bbc.co.uk/1/hi/sci/tech/2016788.stm> [Accessed: 7 May 2003] *47% error rate with irisprints, 80% with fingerprints*

BBC (2002d) *Hi-tech signatures to fight fraud* [WWW] Available from: <http://news.bbc.co.uk/1/hi/technology/2420143.stm> [Accessed: 7 May 2003] *Nationwide Building Society to introduce biometric tests to authenticate signatures*

BBC (2002e) *Invention aims to keep children safe* [WWW] Available from: <http://news.bbc.co.uk/1/hi/england/2268056.stm> [Accessed: 30 April 2003] *GPS device attached to child, location transmitted to parent's mobile*

BBC (2002f) *Mobile phone tracks heartbeats* [WWW] Available from: <http://news.bbc.co.uk/1/hi/technology/2562265.stm> [Accessed: 13 December 2002] *Telemedicine*

BBC (2002g) *Phone firms 'flooded' by crime checks* [WWW] Available from: <http://news.bbc.co.uk/1/hi/uk/2592707.stm> [Accessed: 20 December 2002]

BBC (2003a) *British passports set for high-tech revamp to tackle terror threat* [WWW] Available from: http://news.bbc.co.uk/media/video/39180000/rm/_39180389_passports20_andrew_viram [Accessed: 5 May 2003] *New passports, biometrics*

BBC (2003b) *Children's tracking device invented* [WWW] Available from: http://news.bbc.co.uk/1/hi/england/west_midlands/2927589.stm [Accessed: 30 April 2003] *Geobangle, track children, pets*

BBC (2003c) *Crimewatch* [WWW] Available from: <http://www.bbc.co.uk/crime/crimewatch/index.shtml> [Accessed: 27 January 2003]

BBC (2003d) *Fans warned over fake tickets* [WWW] Available from: <http://news.bbc.co.uk/1/hi/england/london/3017867.stm> [Accessed: 11 May 2003] *Counterfeits of all sorts could be eliminated by PKI*

BBC (2003e) *Five die in gas-filled car* [WWW] Available from: <http://news.bbc.co.uk/1/hi/wales/2890999.stm> [Accessed: 28 March 2003] *Keith Young, located by mobile*

BBC (2003f) *Microsoft bows to EU privacy concerns* [WWW] Available from: <http://news.bbc.co.uk/1/hi/technology/2710389.stm> [Accessed: 30 January 2003] *Passport*

BBC (2003g) *Mobiles used to monitor asthma* [WWW] Available from: <http://news.bbc.co.uk/1/hi/technology/2808603.stm> [Accessed: 3 May 2003] *Telemedicine*

BBC (2003h) *Net security software exposed* [WWW] Available from: <http://news.bbc.co.uk/1/hi/technology/2785145.stm> [Accessed: 20 February 2003] *Faults in SSL*

BBC (2003i) *Anti-fraud credit cards tested* [WWW] Available from: <http://news.bbc.co.uk/1/hi/business/3038875.stm> [Accessed: 19 May 2003] *Credit cards to use PINs*

BBC (2003j) *Raid on 'forgery factory'* [WWW] Available from: <http://news.bbc.co.uk/1/hi/england/2734043.stm> [Accessed: 19 May 2003]

BBC (2003k) *Two jailed over immigration ring* [WWW] Available from: <http://news.bbc.co.uk/1/hi/england/hampshire/dorset/3040637.stm> [Accessed: 19 May 2003]

BBC (2003l) *Fans warned over fake tickets* [WWW] Available from: <http://news.bbc.co.uk/1/hi/england/london/3017867.stm> [Accessed: 11 May 2003]

BCSL (2003a) *Mobile Phones are the ID Cards of the Future* [PDF] Available from: <http://www.bcs1.pwp.blueyonder.co.uk/DematerialisedID/> [Accessed: 29 May 2003]

BCSL (2003b) *AppealNet* [PDF] Available from: <http://www.bcs1.pwp.blueyonder.co.uk/DematerialisedID/> [Accessed: 29 May 2003]

BCSL (2003c) *Dematerialised ID – the Alternative to Entitlement Cards* [PDF] Available from: <http://www.bcs1.pwp.blueyonder.co.uk/DematerialisedID/> [Accessed: 29 May 2003]

Benefon (2003) *Control & Safety for Mobile Professionals* [WWW] Available from: <http://www.benefon.com/> [Accessed: 8 December 2002] *GPS/GSM tracking, Friend Finder, telematics, telemedicine, personal safety*

Bergqvist, Jens, Dahlberg, Per, Fagrell, Henrik and Redström, Johan (1999) *Location awareness and local mobility* [PDF] <http://www.viktoria.se/groups/play/publications/1999/proximityawareness.pdf> [Accessed: 8 December 2002]

Biocentric Solutions (2001) *Why use a biometric and a card in the same device?* [PDF] Available from: <http://www.biocentricolutions.com/media/whitepaper.pdf> [Accessed: 6 May 2003]

Bitpipe (2003) *3G Wireless: White Papers, Webcasts and Case Studies* [WWW] Available from: http://www.bitpipe.com/data/rlist?t=soft_10_100_30_70_8&sort_by=status&src=google [Accessed: 2 May 2003]

Bluetooth (2003) *The Official Bluetooth Website* [WWW] Available from: <http://www.bluetooth.com/> [Accessed: 26 May 2003]

Bridgewater Systems (2003) *802.11/WLAN* [WWW] Available from: http://www.bridgewater.com/solutions/80211_wlan/ [Accessed: 2 May 2003]

Bridgewater Systems (2003) *Road Map to 802.11 Services* [PDF] Available from: [http:](http://)

[//www.bridgewatersystems.com/news_events/specials/80211roadmap2/Roadmap%20to%20802.11%20Services.pdf](http://www.bridgewatersystems.com/news_events/specials/80211roadmap2/Roadmap%20to%20802.11%20Services.pdf) [Accessed: 2 May 2003]

Brudnicki, David (2001) *AT&T Wireless – Third Generation Wireless Technology* [PDF] Available from: [?/sim102001.pdf](http://sim102001.pdf) [Accessed: 19 January 2003]

BT (2001) *ServiceView Digital ID Centre* [WWW] Available from: <https://onsite.trustwise.com/services/BritishTelecommunicationsplcBTServiceView/digitalidCenter.htm> [Accessed: 3 February 2003] *BCSL attempted to get a certificate issued, not quite understanding what the site is for, and was quite properly rejected*

BT (2003) BBC – *BT scheme to fight ID fraud* [WWW] Available from: <http://news.bbc.co.uk/1/hi/technology/2808281.stm> [Accessed: 5 March 2003] *BT to provide identity database, c.f. Derek Bond, use utility bills, like Experian, and other details*

Business 2.0 (2000) *Wireless Spectrum for Dummies* [PDF] Available from: <http://www.ecompany.com/docs/CheatsheetA12.pdf> and [CheatsheetB12.pdf](http://www.ecompany.com/docs/CheatsheetB12.pdf) [Accessed: 6 May 2003]

BWE (2003) *Broadband Wireless Exchange – 802.16 News* [WWW] Available from: <http://www.80216news.com/> [Accessed: 20 April 2003]

Carnegie-Mellon (2003) *Wireless Andrew* [WWW] Available from: <http://www.cmu.edu/computing/wireless/> [Accessed: 2 April 2003] *802.11 network provides location-detection accurate to 5ft*

CBS (2003) *Watching Your Kids' Every Move* [WWW] Available from: <http://www.cbsnews.com/stories/2003/01/06/eveningnews/main535397.shtml> [Accessed: 7 January 2003] *GPS, US parents tracking their children*

cellular-news (2003) *Wireless Telecoms News and Information* [WWW] Available from: <http://www.cellular-news.com/> [Accessed: 6 May 2003]

CGALIES (2003) *Coordination Group on Access to Location Information for Emergency Services – European emergency number - 112* [PDF] Available from: http://europa.eu.int/comm/environment/civil/pdfdocs/cgaliesfinalreportv1_0.pdf [Accessed: 18 May 2003]

Charny, Ben (2002) *Cingular halts E-911 gear shipments* [WWW] Available from: <http://zdnet.com.com/2100-1105-960743.html> [Accessed: 20 April 2003] *EOTD failing to provide accuracy required by E911*

Cisco (2001) *Wireless Solutions* [WWW] Available from: http://ema-ams2.cisco.com/emaurl/www/ukurl/uk_commercialwireless/dmlandingpage.htm [Accessed 4 July 2001] *Bought Aironet, rival to BreezeCOM*

CitizenCard (2003) *Authenticated Global Photo-ID* [WWW] Available from: <http://www.citizencard.com/> [Accessed: 11 May 2003] *Tie-up with Experian, proof of identity and age with airlines, banks, retailers, 15,000 issued in London, tie-up with SplashPlastic and SwapIt electronic money*

Clarke, Liam (2003) *Top British agent on run after cover is blown*. The Sunday Times: 11 May 2003. Available from: <http://www.timesonline.co.uk/article/0,,2087-676552,00.html>. *Stakeknife, Alfredo 'Freddy' Scappaticci, need for a protocol to create identities*

Clarke, Roger (2000) *Person-location and Person-Tracking: Technologies, Risks and Policy Implications* [WWW] Available from: <http://www.anu.edu.au/people/Roger.Clarke/DV/PLT.html>. [Accessed 20 January 2003]. *Paper includes references to 30 more articles by the same author*

Counterpoint Systems Foundry (no date) *IrDA Infrared Communications: An Overview* [PDF] Available from: <http://www.irda.org/use/pubs/Overview.PDF> [Accessed: 26 May 2003]

CPS (2003) *Cambridge Positioning Systems* [WWW] Available from: http://www.cursor-system.com/innovations_doclibrary.asp [Accessed: 20 January 2003] *EOTD, GSM, accurate positioning*

Crouch, Cameron (2001) *PC World – Will Big Brother track you by cell phone?* [WWW] Available from: http://wireless.itworld.com/4273/PCW010418aid47784/page_1.html [Accessed: 7 January 2003]

CTIA (2002) *Cellular Telecommunications and Internet Association – How Wireless Works* [WWW] Available from: <http://www.wow-com.com/consumer/howitworks/> [Accessed: 6 May 2003]

CW (2003) *Computer Weekly – ID card plan needs focus* [WWW] Available from: <http://www.computerweekly.com/articles/article.asp?liArticleID=118816&liArticleTypeID=20&liCategoryID=2&liChannelID=28&liFlavourID=1&sSearch=&nPage=1> [Accessed: 31 January 2003]

Dana, Peter H. (2000) *Global Positioning System Overview* [WWW] <http://www.colorado.edu/geography/gcraft/notes/gps/gps.html> [Accessed: 19 January 2003]

Deshpande, Sumit (2002) *Computer Associates – Enabling Mobile eBusiness Success* [PDF] Available from: http://wp.bitpipe.com/resource/org_943197149_209/enabling_mobile_ebiz_wp_bpxstream.pdf [Accessed: 2 May 2003] *Taxonomy of the mobile industry*

Dibdin, Peter (2001) *Where are mobile location based services?* [PDF] Available from: <http://mms.ecs.soton.ac.uk/mms2002/papers/4.pdf> [Accessed: 2 May 2003]

divine (2002) *Northern Light Special Edition Wireless Technology* [WWW] Available from: <http://special.northernlight.com/wireless/> [Accessed: 6 May 2003] *Research papers on wireless technology*

Dornan, Andy (2001) *The Essential Guide to Wireless Communications Applications*. Upper Saddle River, NJ: Prentice Hall

DVLA (2001) *Driver and Vehicle Licensing Agency* [WWW] Available from: <http://www.dvla.gov.uk/> [Accessed: 11 May 2003]

e-Envoy (2003) *Office of the e-Envoy* [WWW] Available from: <http://www.e-envoy.gov.uk/> [Accessed: 21 May 2003]

Economist (2002) 'Time for plan B', *The Economist*, 26 September 2002. Also available from: http://www.economist.com/displaystory.cfm?story_id=1353050 *WCDMA doesn't work, try CDMA2000*

e-identitycheck (2003) *Helps guard against identity fraud* [WWW] Available from: <http://www.eidentitycheck.com/id/index.html> [Accessed: 11 May 2003] *On-line identity check for accountholders including photograph, uses digital certificate to check that you are an accountholder*

Ekahau (2003a) *Ekahau – location-enabling Wi-Fi networks* [WWW] Available from: <http://www.ekahau.com/technology/comparison.html> [Accessed: 6 May 2003] *802.11, RFID, accurate positioning*

Ekahau (2003b) *Using WLAN Positioning in a Grocery Store: Requirements, Benefits and Challenges* [PDF] Available from: http://www.ekahau.com/kamppis_kesa/Grocery%20Store%20Whitepaper.pdf [Accessed: 6 May 2003]

Entrust (2003) *Securing Digital Identities and Information* [WWW] Available from: <http://www.entrust.com/index.cfm> [Accessed: 31 January 2003] *As of 29 April 2003, Entrust, Inc., of Addison, Texas, supplies the national root certificate for the UK Government which will be managed by GCHQ. PKI software and services supplier + white papers and news*

ETSI (2000) *Radio Spectrum Matters* [WWW] Available from: http://www.etsi.org/technicalactiv/spectrum%20%20don't%20publish%20yet/frequency_table.htm [Accessed: 26 February 2003]

Experian (2003) *Is this person who they say they are?* [WWW] Available from: <http://www.uk.experian.com/business/products/4.html> [Accessed: 11 May 2003] *Credit referencing, GUS, CitizenCard, e-identitycheck*

Farley, Tom with van der Hoek, Mark (2002) *Cellular Telephone Basics: AMPS and Beyond* [WWW] Available from: <http://www.privateline.com/Cellbasics/Cellbasics.html> [Accessed: 6 May 2003]

FCC (2001) *Federal Communications Commission – Fact Sheet: E911 Phase II Decisions* [PDF] Available from: http://www.fcc.gov/Bureaus/Wireless/News_Releases/2001/nwl0127a.pdf

Fildes, Christopher (2002) Show us your gas bill, Ma'am. *The Spectator*, 1 June 2002. Also available from: <http://www.telegraph.co.uk/money/main.jhtml?xml=/money/2002/06/01/ccfild01.xml>

Finland (2003a) *Finland: Electronic identification to mobile phone* [WWW] Available from: <http://e.finland.fi/netcomm/news/showarticle.asp?intNWSAID=9333> [Accessed: 29 January 2003] *Identity = mobile phone + digital certificate*

Finland (2003b) *Handsets help to unstick jams* [WWW] Available from: <http://news.bbc.co.uk/1/hi/technology/2680561.stm> [Accessed: 22 January 2003]

Frean, Alexandra (2003) *Britons are enslaved by the mobile telephone*. The Times: 10 May 2003. Available from: <http://www.timesonline.co.uk/article/0,,2-674844,00.html>. *Henley Management Centre report, people identify with their mobiles*

Gartner (2002) *Location-Aware Society* [WWW] Available from: <http://164.100.10.143/Datapro2/research/108500/108554/108554.html> [Accessed: 2 February 2003] *Not accessible now*

Gartner (2002) *When to seek high accuracy in mobile location services* [WWW] Available from: <http://164.100.10.143/Datapro2/research/108400/108413/108413.html> [Accessed: 2 February 2003] *Not accessible now*

Gibson, Nick (2002) *Guide To – 3G – United Kingdom* [WWW]. Available from: <http://www.commstrade.com/editorial/ItemDetail.asp?ItemID=3107>. [Accessed 15 January 2003]

GIS Lounge (2003) *Uses for GPS* [WWW] Available from: <http://gislounge.com/features/aa050901a.shtml> [Accessed: 7 January 2003]

GlobalSign (2002) *Digital Certificate and PKI Solutions* [WWW] Available from: <http://www.belsign.be/> [Accessed: 25 March 2003] *PKI trusted third party*

GPS Future (2002) *GPS Stuff* [WWW] Available from: <http://www.gps-future.com/> [Accessed: 7 January 2003]

Harrison, Angus (2002) *E-OTD Location Technology in Trouble* [WWW] Available from: <http://www.commstrade.com/editorial/ItemDetail.asp?ItemID=4147> [Accessed: 4 February 2003]

Hedy Lamarr (2001) *From Strapless to Wireless* [WWW] <http://www.hedylamarr.org/hedystory5.htm> [Accessed: 22 January 2003] *Frequency-hopping*

Heer, J. De, Peddemors, A.J.H. and Teeuw, W.B. (2002) *To be or not to be in control that is the question* [PDF] Available from: http://www.pampas.eu.org/Position_Papers/Telematica.pdf [Accessed: 8 December 2002]

Hellen, Nicholas and Winnett, Robert (2003) *Jobless get free mobile phones to find work*. The Sunday Times: 4 May 2003. Available from: <http://www.timesonline.co.uk/article/0,,2087-668524,00.html>. *Resentment at people being given free mobile phones*

HID Corporation (2002) *MFare Reference Guide* [PDF] Available from: <http://www.hidcorp.com/pdfs/smart/MRG-EN-US.pdf> [Accessed: 24 May 2003] *Electronic*

cash for vending machines, bus/train fare collection, airline ticketing, prepaid metering, phone cards, toll roads, ID cards, university cards, 16 applications per card.

Home Office (2000) *Regulation of Investigatory Powers Act* [WWW] Available from: <http://www.homeoffice.gov.uk/> [Accessed: 13 January 2003]

Home Office (2001) *Anti-Terrorism, Crime & Security Act 2001* [WWW] Available from: <http://www.homeoffice.gov.uk/terrorism/govprotect/index.html> [Accessed: 6 May 2003]

Home Office (2002) *Entitlement Cards and Identity Fraud – a Consultation Paper* [PDF] Available from: <http://www.homeoffice.gov.uk/comrace/entitlements/fraud.html>. [Accessed: 31 January 2003]

Hopkins, Nic (2003) *Microsoft risks fines over e-commerce security flaw*. The Times: 10 May 2003. Available from: <http://www.timesonline.co.uk/article/0,,5-675045,00.html>. *Problems of Passport/Mobile Personality applications*

IBM (2000) *PKI: A Primer* [WWW] Available from: <http://www-106.ibm.com/developerworks/security/library/s-pki.html> [Accessed: 3 February 2003]

IBM (2003a) *e-Suds* [WWW] Available from: <http://www-1.ibm.com/industries/wireless/doc/content/casestudy/298103104.html> [Accessed: 3 May 2003] *Cashless payments, RFID et al*

iDentacard (2003) *Home of the world's most effective fake ID's!* [WWW] Available from: <http://www.identacard.co.uk/newsite/cards.html> [Accessed: 17 May 2003]

Identix (2002) *Identix Inc. – FaceIT Technical Specifications* [WWW] Available from: http://www.identix.com/newsroom/face_ts.html. [Accessed: 14 January 2003] *Biometrics*

IEC (2003) *International Engineering Consortium – W-CDMA* [WWW] Available from: <http://www.iec.org/online/tutorials/wcdma/> [Accessed: 18 February 2003]

IEEE (2001) *802.15 Wireless Personal Area Networks* [WWW] Available from: <http://www.ieee802.org/15/about.html> [Accessed: 20 April 2003]

IEEE (2003) *802.16 Wireless Metropolitan Area Network* [WWW] Available from: <http://www.ieee802.org/16/> [Accessed: 20 April 2003]

InterTrust (2003) *Trusted Computing* [WWW] Available from: <http://www.intertrust.com/> [Accessed: 9 February 2003] *Research and development, digital rights*

IrDA (2003) *Infrared Data Association* [WWW] Available from: <http://www.irda.org/> [Accessed: 26 May 2003]

ITC (2003) *What is PKI* [WWW] Available from: <http://www.itc.virginia.edu/desktop/pki/pkiWhat.phtml> [Accessed 3 February 2003] *Department of Information Technology and Communication, University of Virginia*

ITToolbox (2003) *Wireless Knowledge Base* [WWW] Available from: <http://wireless.ittoolbox.com/> [Accessed: 6 May 2003]

ITU (2002) *International Telecommunication Union – What is IMT-2000?* [PDF] Available from: http://www.itu.int/osg/imt-project/docs/What_is_IMT2000-2.pdf [Accessed: 21 January 2003]

James, Jennie (2002) *Time Europe – A Call For Help* [WWW] Available from: <http://www.time.com/time/europe/magazine/article/0,13005,901020311-214207,00.html> [Accessed: 7 May 2003] *50% reduction in stolen mobile phone in Amsterdam achieved by text-bombing stolen numbers, not always in interests of network operators to block calls to stolen phones, stolen handsets have IMEI reset to legitimate *#06# number*

Justnet (2001) *Justice Technology Information Network* [WWW] Available from: <http://www.nlectc.org/justnetnews/10042001.html#story8> [Accessed: 7 January 2003] *Ultimately, an arm of the US Department of Justice, synopses of stories + links*

Kanaracus, Chris (2002) *Your Cell Phone Is Watching You* [WWW]. Available from: <http://www.alternet.org/print.html?StoryID=12776>. [Accessed 7 January 2003]. *Mobile phones track you cell by cell and, with E911, more accurately still*

Keene, Ian (2003) *Computer Weekly – Will Wi-Fi eclipse the promise of 3G* [WWW] Available from: <http://www.computerweekly.com/articles/article.asp?liArticleID=119648&liArticleTypeID=13&liCategoryID=1&liChannelID=7&liFlavourID=1&sSearch=&nPage=1> [Accessed: 3 May 2003]

Kenwood (2003) *Excelon* [WWW] Available from: <http://www.kenwoodusa.com/excelon/excelonNav.jsp> [Accessed: 23 January 2003] *GPS, in-car satellite navigation*

Kizoom (2000) *Train Times* [WAP] Available from: <http://rail.kizoom.co.uk/html/index.jsp> [Accessed: 16 December 2002]

Laroche, Marc (2000) *Common Criteria Ecaluation for a Trusted Entrust/PKI™* Entrust, Inc.: Addison, TX Also available from: http://www.entrust.com/resources/pdf/criteria_eval.pdf

LBS (2003) *London Business School – David Levin, CEO Symbian* [Seminar] Available from: <http://search.london.edu/forumhit.html?url=http://forum.london.edu/lbsevents.nsf/httpEvents/6A7779C030594A4480256CD20066673F;OpenDocument> [Attended: 15 May 2003] *According to Levin: "Ibn mobiles in use worldwide, 400m replaced each year, on 397.3m of those the operating system is provided by the handset manufacturer, 2.1m of the rest have SymbianOS, they need 20m p.a. to break even, their competitors are Palm, Microsoft and Linux, Linux only provides about 15% of the functionality needed by a mobile phone operating system, Palm is toast and Microsoft don't know anything about mobile phones, only PCs"*

Levijoki, Sami (2000) *Privacy vs Location Awareness* [WWW]. Available from: http://www.hut.fi/~slevijok/privacy_vs_locationawareness.htm. [Accessed 7 January 2003]

Liberty (2003) *Liberty's Response to the Home Office Consultation 'Entitlement Cards and Identity Fraud'* [PDF] Available from: <http://www.liberty-human-rights.org.uk/issues/id-cards.shtml> [Accessed: 7 May 2003] *Cards won't solve the problems identified, which keep changing, and haven't solved them in countries which have them*

MacKay, Niel (2003) *Named: British double agent who murdered for the IRA. The Sunday Herald: 11 May 2003.* Available from: <http://www.sundayherald.com/33815.Stakeknife,Alfredo'Freddy'Scappaticci,needforaprotocoltocreateidentities>

Maney, Kevin (2000) *USA Today – Tag it* [WWW] Available from: <http://technology.cincinnati.com/cgi-bin/technology/techwrapper.pl?URL=http://www.gannettonline.com/e/trends/15000677.html&AFFIL=CIN> [Accessed: 6 May 2003] *RFID tags track everything from aeroplanes to egg cartons*

Mayfield, Kendra (2002) *Wired News – Radio ID Tags: Beyond Bar Codes* [WWW] Available from: <http://www.wired.com/news/technology/0,1282,52343,00.html> [Accessed: 6 May 2003] *RFID tags for tracking, manufacturing, retailing, including payments via mobile phone*

Microsoft (2002) *.Net Passport* [WWW] Available from: <http://www.passport.net/Consumer/default.asp?lc=2057> [Accessed: 6 May 2003]

Middleware (2003) *The Petstore Revisited* [WWW] Available from: <http://www.middleware-company.com/j2eedotnetbench/> [Accessed: 4 April 2003]

MMC (2003) *Make My Calls, Inc.* [WWW] Available from: <http://www.auto-dialers-done-right.com/> [Accessed: 16 February 2003] *Autodialers*

mmO₂ (2003) *Preliminary Results For The 12 Months Ended 31 March 2003* [PDF] Available from: <http://www.mmo2.com/docs/investor/downloads/PrelimsRelease-final-Print.pdf> [Accessed: 22 May 2003]

Moss, David (2003) *AppealNet* [WWW] Available from: <http://www.bcs1.pwp.blueyonder.co.uk/AppealNet/> [Accessed: 27 January 2003] *Increase crime clear-up rates*

NCIS (2002) *UK Threat Assessment of Serious and Organised Crime 2002* [FTP]. Available from: http://www.ncis.gov.uk/UKTA2002_1.pdf. [Accessed 17 January 2003].

Netscape (1999) *How SSL Works* [WWW] Available from: <http://developer.netscape.com/tech/security/ssl/howitworks.html> [Accessed: 5 February 2003]

NewsTrove (2002) *Bluetooth* [WWW] Available from: <http://bluetooth.newstrove.com/> [Accessed: 6 May 2003]

Nexus (2003) *Secured IT Solutions* [WWW] Available from: http://www.nexus.se/english/info/?main=v_sakrade&nav=verksamhet&sub=sakrade&advert=sakrade [Accessed: 7 May 2003] *PKI, tie-up with Sonera SmartTrust, acquired Blueice Research and thus Multipass, BankID?*

NIST (2001) *NIST PKI Program* [WWW] Available from: <http://csrc.nist.gov/pki/welcome.html> [Accessed: 3 February 2003]

NIST (2002) *FIPS PUB 140-2 – SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES* National Institute of Standards and Technology: Gaithersburg, MD. Also available from: <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>

Nokia (2001) *Nokia mPosition Solution for E-OTD* [PDF] Available from: http://www.nokia.com/pc_files_wb2/EOTDdatasheet.pdf [Accessed: 2 February 2003]

Nokia (2002a) *A brief introduction to MIDP programming* [WWW] http://forum.nokia.com/html_reader/print?max_page_nbr=8&fileID=2106 [Accessed: 17 December 2002]

Nokia (2002b) *Browsing on mobile devices* [PDF] Available from: [http://www.nokia.com/?/XHTML_White_Paper\[1\].pdf](http://www.nokia.com/?/XHTML_White_Paper[1].pdf) [Accessed: 17 December 2002]

Nokia (2002c) *Mobile Personality* [PDF] Available from: http://www.nokia.com/downloads/aboutnokia/press/pdf/mobile_personality_brochure_a4_092002.pdf [Accessed: 2 February 2003] *Equivalent to Microsoft Passport*

Nokia (2002d) *Presence* [PDF] Available from: <http://www.nokia.com/?/Presence.pdf> [Accessed: 17 January 2003] *C.f. Friend Finder*

Nokia (2002e) *WAP Service Developer's Guide for Nokia Series 30 Phones with WML Browser* [PDF] Available from: [http://www.nokia.com/?/WAP_Serv_Dev_Guide_Nokia_Series_30_WML_v1_0\[1\].pdf](http://www.nokia.com/?/WAP_Serv_Dev_Guide_Nokia_Series_30_WML_v1_0[1].pdf) [Accessed: 17 December 2002]

Nokia (2002f) *The Evolution of Mobile VPN and its Implications for Security* [PDF] Available from: http://www.nokia.com/downloads/solutions/business/mVPN_Whitepaper.pdf [Accessed: 25 May 2003]

Nokia (2003a) *Mobile Commerce FAQ* [WWW] Available from: http://www.forum.nokia.com/main/1,6566,1_80_30,00.html [Accessed: 6 May 2003] *PKI and the Nokia wallet application*

Nokia (2003b) *Java in Mobile Devices* [WWW] Available from: <http://www.nokia.com/nokia/0,8764,5342,00.html> [Accessed: 25 May 2003]

NSA (2003) *The National Security Agency* [WWW] Available from: <http://www.nsa.gov/> [Accessed: 31 January 2003] *"The National Security Agency is the Nation's cryptologic organization. It coordinates, directs, and performs highly specialized activities to protect U.S. information systems and produce foreign intelligence information."*

NTT DoCoMo (2000a) *Current trends in mobile phone usage among adolescents* [PDF] Available from: http://www.nttdocomo.com/reports/No10_Doc.pdf [Accessed: 14 December 2002]

NTT DoCoMo (2000b) *The use of cell phones/PHS phones in everyday urban life: A survey of 1,000 people* [PDF] Available from: http://www.nttdocomo.com/reports/No09_Doc.pdf [Accessed: 14 December 2002]

NUS (2003) *The NUS Card is both an identity card and a key to a wealth of benefits* [WWW] Available from: <http://www.nusonline.co.uk/content/nuscard/default.php> [Accessed: 18 September 2001]

NYT (2000) *New York Times – Something to watch over me* [WWW] Available from: <http://www.endtimeinfo.net/technology/moregps.html> [Accessed: 7 January 2003] *Parents watching their children at amusement parks by GPS-based Digital Angel product, further references to Boomerang www.vehicletracking.com and WhereNet*

Oftel (2003) *Office of Telecommunications* [WWW] Available from: <http://www.oftel.gov.uk/index.htm> [Accessed: 20 January 2003]

OMA (2003) *Open Mobile Alliance* [WWW] Available from: <http://www.openmobilealliance.org/> [Accessed: 7 May 2003] *Open standards for the mobile industry*

OTHER (2003) *the OTHER media* [WWW] Available from: <http://www.othermedia.com/go/Default.html> [Accessed: 18 March 2003]

ParthusCeva (2003) *Semiconductor Intellectual Property* [WWW] Available from: <http://www.parthusceva.com/about/index.html> [Accessed: 20 April 2003] *GPS-based systems*

Penenberg, Adam L. (2001) *Wired Magazine – The Surveillance Society* [WWW] Available from: http://www.wired.com/wired/archive/9.12/surveillance_pr.html [Accessed: 13 January 2003]

PGP (1999) *PGP Desktop Security*. Network Associates, Inc.

PGP (2003) *PGP Corporation* [WWW] Available from: <http://www.pgp.com/> [Accessed: 5 February 2003]

Philips (2002) *Philips' MIFARE[®] Identification Chips just the ticket for London's Oyster Smart Card* [WWW] Available from: http://www.semiconductors.philips.com/news/content/file_910.html [Accessed: 24 May 2003] *Project to use RFID cards to speed up fare payments for London buses and tubes, Project Oyster. Philips own MFARE, see HID Corporation*

Pioneer (2003) *Pioneer North America, Inc. – Satellite Navigation* [WWW] Available from: <http://www.pioneerelectronics.com/Pioneer/CDA/CarProducts/CarAlbum/0,1427,40~4010~4010100,00.html> [Accessed: 28 January 2003] *GPS, in-car satellite navigation*

- Price, Will (2003) *Inside PGP® Key Reconstruction* [PDF] Available from: <http://www.pgp.com/products/whitepapers/PGPKeyRecon.pdf> [Accessed: 27 May 2003]
- Privacy International (2001a) *Privacy and Human Rights 2000 Overview* [WWW] Available from: <http://www.privacyinternational.org/survey/phr2000/overview.html>. [Accessed 29 January 2003]
- Privacy International (2001b) *Technologies of Privacy* [WWW] Available from: <http://www.privacyinternational.org/survey/technologies.html>. [Accessed 29 January 2003]
- Privacy International (2002) *UK National ID Cards* [WWW] Available from: <http://www.privacyinternational.org/issues/idcard/uk/>. [Accessed 29 January 2003] *Not in favour*
- Privacy International (2003a) *2003 UK Big Brother Awards* [WWW] Available from: <http://www.privacyinternational.org/bigbrother/uk2003/>. [Accessed 18 May 2003]
- Privacy International (2003b) *Mondex and Anonymity* [WWW] Available from: <http://www.privacyinternational.org/issues/mondex/index.html>. [Accessed 18 May 2003]
- Qualcomm (2002) QUALCOMM's gpsOne™ Technology for E911 [PDF] Available from: http://www.cdmatech.com/solutions/pdf/gpsone_factsheet.pdf [Accessed: 14 May 2003] *Qualcomm owns a lot of the intellectual property in mobile phone communications*
- Rådman, Lars (2002) *Position Based Services* [PDF] Available from: <http://www.cs.umu.se/kurser/TDBD07/VT02/uppsproj/resultat/uppsats/lars/Position%20based%20services%20reviderad.pdf> [Accessed: 8 December 2002] *Check Rådman references*
- Reading (2003) *What happens when a man is merged with a computer?* [WWW] Available from: http://www.rdg.ac.uk/KevinWarwick/html/project_cyborg_1_0.html [Accessed: 1 February 2003]
- Retainagroup (1998) Mark it. Register it. Retain it. [WWW] Available from <http://www.retainagroup.com/> [Accessed: 1998]
- RFID Wizards (2003) *Implementing RFID Solutions Magically* [WWW] Available from: <http://www.rfidwizards.com/rfidwizards.nsf/bca368ea2a17dac585256c6c0056701c/9ab08a7366fa62df85256c6d006c8b8c!OpenDocument> [Accessed: 24 May 2003] *RFID primer starting this page and continuing*
- Rheingold, Howard (2002) *Smart Mobs* [WWW] Available from: http://www.smartmobs.com/archives/2002_05.html [Accessed: 6 May 2003]
- Rogerson, Steve (2000) *Will 3G learn from WAP's mistakes?* [WWW] Available from: <http://www.computerweekly.com/articles/article.asp?liArticleID=24153&liArticleTyp>

eID=20&liCategoryID=1&liChannelID=2&liFlavourID=1&sSearch=&nPage=1 [Accessed: 3 May 2003]

RSA (2003) *Passwords with a 60-second shelf life* [WWW] Available from: <http://zdnet.com.com/1601-2-996987.html> [Accessed: 22 April 2003]

RSA (2003) *Web Management and Internet E-Security* [WWW] Available from: <http://www.rsasecurity.com/> [Accessed: 21 February 2003]

Sabbagh, Dan (2003a) *T-Mobile to reveal loss of 400,000 subscribers*. The Times: 6 May 2003. Available from: <http://www.timesonline.co.uk/article/0,,5-670783,00.html>. *50m+ active mobile phone accounts in UK/83% of the population*

Sabbagh, Dan (2003b) *T-Mobile claims VAT refund*. The Times: 16 May 2003. Available from: <http://www.timesonline.co.uk/printFriendly/0,,1-5-681682,00.html>.

samkruzanar (2002) *USA Technologies debuts e-Port in Asia* [WWW] Available from: <http://ragingbull.lycos.com/mboard/boards.cgi?board=BENGX&read=218> [Accessed: 3 May 2003] *Cashless payments, RFID et al*

Sarvanko, Tomi (2002) *Positioning standards E911, E112 and UMTS* [PDF] Available from: <http://www.telecomlab oulu.fi/home/Radiotekniikka/materiaali/Standardit.pdf> [Accessed: 1 February 2003] *Telematics accuracy*

Security-Online (1997) *Digital Certificate ID Links* [WWW] Available from: <http://www.security-online.com/info/certificates.html> [Accessed: 25 March 2003] *Selection of papers on PKI*

Sheehy, Patrick (1993) *Inquiry into Police Responsibilities and Rewards (Sheehy Inquiry)*. London, HMSO

Simply Computers (2003) *Wireless Networking* [WWW] Available from: <http://www.simply.co.uk/?sn=2084984182> [Prices checked: 26 May 2003]

Singh, Simon (1999) *The Code Book*. London, Fourth Estate Ltd

Smailagic, Asim, Siewiorek, Daniel P., Anhalt, Joshua, Kogan, David and Wang, Yang (2001) *Location Sensing and Privacy in a Context Aware Computing Environment* [PDF] Available from: http://www.cs.cmu.edu/~asim/Location_sensing_S01_v6.pdf [Accessed: 8 December 2002] *Location detection accuracy of 5ft*

Small, Jason, Smailagic, Asim and Siewiorek, Daniel P. (2000) *Determining User Location For Context Aware Computing Through the Use of a Wireless LAN Infrastructure* [PDF] Available from: www.cs.cmu.edu/~aura/docdir/small00.pdf [Accessed: 2 April 2003] *Location-detection 15ft accuracy using 802.11, part of Carnegie-Mellon University's Project Aura investigating distraction-free ubiquitous computing*

SmartTrust (2000) *PKI, Certification Authority and Digital Identity* [WWW] Available from: <http://www.smarttrust.com/digitalidentity/default.asp> [Accessed: 5 February 2003]

Soliman, Samir S. And Wheatley, Charles E. (2002) 'Geolocation technologies and applications for third generation wireless', *Wireless Communications and Mobile Computing*, Vol.2, pp.229-251. Available from: <http://basepath.wiley.com/cda/media/0,,19890,00.pdf>. *The authors work for Qualcomm and account for about 60 of Qualcomm's 800 patents*

Sony Ericsson (2001) *Understanding Networks* [WWW] Available from: http://www.sonyericsson.com/spg.jsp?page=gis&Redir=template%3DPortalPage_1_4%26B%3Die [Accessed: 6 May 2003]

Splash Plastic (2003) *Pay As You Go Online with Splash Plastic* [WWW] Available from: <http://www.splashplastic.com/> [Accessed: 17 May 2003]

Steinfeld, Charles and Kim, Junghyun (2002) *Providing Location and Context Aware Services for Mobile Commerce: Technological Approaches, Applications, and Policy Issues* [FTP] Available from: <http://www.its2002.or.kr/pdf/files/papers/174-Steinfeld.pdf> [Accessed: 6 May 2003] *International Telecommunications Society 14th Biennial Conference, Seoul, South Korea*

Sun (1998) *What's Inside an X.509 Certificate?* [WWW] Available from: <http://java.sun.com/j2se/1.3/docs/guide/security/cert3.html#inside> [Accessed: 9 February 2003]

Symbian (2002) *Certificate Management* [WWW] Available from: <http://www.symbian.com/developer/techlib/v70docs/sdl%5Fv7.0/doc%5Fsource/devguides/securityguide/certman/index.html> [Accessed: 15 May 2003]

Tanikawa, Miki (2002) *International Herald Tribune – With GPS, KDDI finds a new cell-phone audience* [WWW] Available from: <http://www.iht.com/articles/52714.html> [Accessed: 7 January 2003] *KDDI = competitor to NTT DoCoMo, location-aware services based on GPS*

Target (2003) *Target Marketing USA, Inc. – Lead Generation System & Service* [WWW] Available from: <http://www.targetmarketingusa.com/> [Accessed: 15 February 2003] *Autodialers*

TCMS (2003) *Total Call Management Systems Corp. – Autodialers* [WWW] Available from: <http://www.auto-dialers-phone-dialing.com/autodialers-auto-dialers-auto-attendant.htm> [Accessed: 16 February 2003] *Autodialers*

TeletechPlus (2000) *Telemarketing Software* [WWW] Available from: <http://www.teletechplus.com/icc.htm> [Accessed: 16 February 2003] *Autodialers*

Thawte (2003) *Digital Certificates from Thawte, the Global Certificate Authority* [WWW] Available from: <http://www.thawte.com/> [Accessed: 25 March 2003]

TTI (2001) *Talking Technology International, Inc. – Autodialer and voice mailer systems* [WWW] Available from: <http://www.tti.net/telemarketing/auto-dialer.html> [Accessed: 16 February 2003] *Autodialers*

Udell, John (2003) *Infoworld – Converging on identity* [WWW] Available from: http://www.infoworld.com/article/03/01/31/05identity_1.html [Accessed: 6 May 2003] *ID card, mobile phone, digital certificate, tracking, E911 – same day as BCSL submission to Home Office*

UK Police (2003) *Non-Emergency Crime Notification* [WWW] Available from: <http://www.online.police.uk/english/default.asp> [Accessed: 17 January 2003]

UK Police (2003) *UK Police Appeals* [WWW] Available from: <http://www.police.uk/appeals.html> [Accessed: 17 January 2003] *Previously listed incidents under investigation where Police appealing for help from public, now discontinued, site refers user to Crimewatch or local police force websites, e.g. <http://www.met.police.uk/appeals/index.htm>*

UKPS (2003) *UK Passport Service* [WWW] Available from: <http://www.ukpa.gov.uk/> [Accessed: 11 May 2003]

USA Technologies (2003) *e-Port – Vending Services* [WWW] Available from: http://www.usatech.com/vending_overview.html [Accessed: 3 May 2003] *Cashless payments, RFID et al*

VeriSign (2003) *VeriSign, Inc.* [WWW] Available from: <http://www.verisign.com/> [Accessed: 25 March 2003]

Victory (2001) *Victory Enterprises, Inc. – Automated phone calls* [WWW] Available from: <http://www.victorystore.com/phone/index.html> [Accessed: 15 February 2003] *Autodialers*

Ward, Mark (2003a) *BBC – Wireless net marches forward* [WWW] Available from: <http://news.bbc.co.uk/1/hi/technology/2783923.stm> [Accessed: 20 February 2003] *Wi-Fi – why are T-Mobile funding hotspots?*

Ward, Mark (2003b) *BBC – Questions over eye scan plan* [WWW] Available from: <http://news.bbc.co.uk/1/hi/technology/3003571.stm> [Accessed: 7 May 2003] *Iris-prints have 6% error, not 0.5%. No large databases available to see track record. It would only take one rumour that they're bad for you ... 240m travellers p.a. through US, 90m through UK. No good for checking a line-up. Could take 10 times as long to get through arrivals. No internationally agreed standards.*

Wi-Fi Alliance (2003) *Wi-Fi News and Information* [WWW] Available from: <http://www.weca.net/OpenSection/index.asp> [Accessed: 2 February 2003]
