Identity and its verification

By

Nicholas Bohm and Stephen Mason[1]

This article was published in the *Computer Law & Security Review*, Volume 26, Number 1, January 2010, 43 – 51

ABSTRACT

The European Commission's eJustice Strategy seems to contemplate that all lawyers will be issued with an 'identity card' card, perhaps intended to include a key for making digital signatures. The Council of Bars and Law Societies of Europe (CCBE) is proposing to introduce such a card. The purpose of this article is to clarify what 'identity' is and what is involved in verifying it, and to offer some general observations about identity cards. Although written with the eJustice proposals in mind, nevertheless the purpose of this article is to address the topic in its widest sense, which means it affects identity and its verification, whatever the circumstances.

Keywords: Identity; identity relationships; verification; 'identity card'

1. Names and identities

Human individuals have continuity of personal existence: you are today the same person you were yesterday, and indeed you remain all your life the same person you were on the day of your birth, despite the many changes that have occurred in you since that day.[2] This fact of the human condition results in the usefulness of human names. But naming conventions are social artefacts suited to the social contexts which gave rise to them, and in rapidly changing times those conventions may become poorly suited to their current context. Names which once served to distinguish their bearers from all others within a small community are no longer effective even amongst the employees of a major business – there are just too many with the name 'John Smith'. Nor can it be assumed that an individual has a single unique name – the same person may be called 'Dad', 'Bill', 'Darling', 'William Hughes' and 'Professor Colonel The

---

[1] The authors thank Clive Freedman, Matthew Lavy, Professor Ross Anderson, Colin Whittaker and the anonymous reviewer for their comments on this paper. The views expressed and conclusions reached remain the sole responsibility of the authors.

[2] In the case of the Kumar of Bhawal, the court had to determine whether a man who suddenly appeared in 1920 purporting to be the Kumar was in fact the same person as one who had apparently died in May 1909, for which see Partha Chatterjee, *A Princely Impostor? The Kumar of Bhawal and the Secret History of Indian Nationalism* (Permanet Black, 2004); for a case illustrating the problems associated with establishing identity, see *O'Hara v The Secretary of State for Education and Skills* [2006] 858.PT.

Reverend William Hughes', depending on the context. Within each of those contexts, the name used may be unique – children usually call only one person 'Dad', for example. But a name that is unique in one context may well not be unique in a different context – a shout of 'Dad' at a school concert is likely to attract more than one father's attention, and there is almost certainly more than one 'William Hughes' (though an academic colonel in holy orders of that name might well be unique).

To deal with the problem that many names are probably not unique in many contexts, additional discriminators are often added, such as an address, a date of birth and sometimes an occupation. 'William Hughes of The Rectory, Wimblefield, Clerk in Holy Orders' would not be untypical. The armed forces often have this problem, and where there might be several 'Jones' in one regiment, each with identical initials, they will usually be identified by their surname followed by the last three numbers allocated to them after joining up.

A rather different problem arises where a person uses different names for different purposes. There are perfectly good reasons for this, such as where an author writes fiction, but does not wish their activities in a private capacity to be confused with their activities as a creative writer. Consider the author of the Smiley spy stories, whose nom de plume is John Le Carré, but who uses the name David Cornwell outside the literary field. It is conventionally said in such cases that 'David Cornwell' is his 'real' name; but this mistakes both the fact and the law of what a name is. (The author is perfectly at liberty to use a pseudonym, but the use of an assumed name does not of course relieve him of the obligation to ensure that the income tax authorities are aware that the different names under which he writes represent only one person entitled to only one set of reliefs and allowances.) Far more people know the author in question as 'John Le Carré' than know him as 'David Cornwell', and there is nothing in the least unreal about this name. A name is simply what a person is called by a non-trivial number of people on a continuing basis, and requires no sanction in registers of births or baptism or national insurance numbers for its 'reality', nor any prescribed formality for its adoption (although formalities may of course help when it comes to providing evidence). It is worth noting that this is not an isolated example. As well as novelists, other writers such as journalists often use pseudonyms, sometimes using several; and so do many actors and other stage performers.

It is sometimes thought that a person's 'real' name and their identity consist of the name which they were registered at birth. The reader will immediately note that this approach fails in the case of those women who, upon marriage, take their husband's family name. The same applies to those who change their gender from that which is recorded at birth, to those who decide to change their name from that recorded on their birth certificate (whether in accordance with prevailing social conventions or otherwise), and to those who may be known by more than one name or series of names. Among many examples are people from China who may decide not to use their given Chinese names, but instead use other names taken from the language of their host country.

What these examples serve to show is that identifiers (such as names and other attributes) represent attempts by society to provide an infrastructure for referring tolerably unambiguously to a person in the contexts in which that person moves. Instead of being unique, i.e. sufficient to distinguish the bearer of a name from every other person, names have usually been no more than relatively unique, that is sufficient to distinguish the bearer name from others with whom he or she is in practice likely to be mistaken.[3] In a shrinking world (with an increasing population), names that were once adequate identifiers have become increasingly unreliable, although this depends on the context: most children only have one person they call 'Dad', although there are plainly a number of children who may have more then one stepfather figure. Those who maintain large collections of the names of the people with whom they deal have adopted a variety of strategies for rendering the names unique (or sufficiently unique for their purpose). To names can be added some combination of identifiers such as occupation, title, sex, date of birth, place of residence and arbitrary number. These strategies can help to answer the question, 'Which John Smith did you mean?' But some of these additional identifiers change over time (as do names in some societies), and this is a major source of the problems that arise when identity is confused with identifiers. Using a

[3] See Peter G. Neuman, *Computer Related Risks* (ACM Press, 1995) 6.5-6.6 for examples of problems that have occurred with failing to identify the correct person.

person's name and address to identify them may be a suitable strategy for a given purpose (even though the information will be used for a purpose other than that for which it was recorded), for example; but to conclude from the use of this strategy that a person who moves house changes his identity would be fatuous. Yet this is effectively the mistake that would be made by someone who demanded evidence of a person's name and address to establish his entitlement to a claimed benefit that accrued when he had some other address, and sought to deny the claim on account of the discrepancy. And there is an increasing tendency to confuse a person's knowledge of an identifier with evidence that the person with the knowledge is the person to whom the identifier relates.

1.1. Proving a relationship between the identifier and the person

A person born in the United Kingdom has an entry in the register of births (open to public inspection) showing his date and place of birth and his mother's maiden name (if known – the person recorded in the register might have been abandoned); and yet many organisations regard knowledge of these facts as evidence that the person who knows them is the person to whom they relate. The use of arbitrary numbers as identifiers (such as passwords for online banking) may appear to solve this problem, but a little reflection shows that this solution carries a high price. If knowledge of the number is to be evidence that the person who knows it is the person to whom it relates, then a person must have a different secret number for every other person to whom he may need to prove his 'identity'. Even if managing numerous secret numbers securely were easy for individuals (which it is not),[4] each number is known both to the individual and to the organisation to which he may have to prove his knowledge. It is gradually becoming better understood that many organisations are very bad at managing private information of this kind: risks of compromise are unacceptably high. And when organisations wish to rely on a shared secret of this kind to authenticate transactions, they tend to blame the individual if the secret becomes known to others, thereby throwing the risk of identity fraud on to the person who has been impersonated, and adding injury to insult.

2.1. The nature and verification of identity

These familiar problems of using names as identifiers are not easy to solve. They are made harder by the adoption of poorly conceived practical solutions. Some of the difficulties of discussing these problems arise from the use of unsatisfactory terminology and concepts. Because we use names to identify ourselves, it seems natural to regard a person's name as her identity; or her name coupled with a sufficient collection of other attributes to render the collection probably unique for the purpose at hand. If that is what 'identity' means, then a duty to verify a person's identity is discharged by collecting evidence that she bears a particular name, receives electricity bills at a particular address, and otherwise fits the required pattern of attributes. The problems outlined in the preceding paragraphs, together with the unreliability of some of the available evidence, account for many spectacular failures of this box-ticking approach.

Instead of seeing 'identity' as a collection of more-or-less verifiable attributes of a person, we suggest that it is much more productive to see it as a relationship. In the context of determining whether a person is a qualified solicitor, for example, it is relevant to know whether the person purporting to be the solicitor is the person named in the relevant roll. The identity to be verified is that between the person whose name is noted on the roll, and the person purporting to be the solicitor in question. It is perfectly possible that he is the same person even though his name and address are different; and equally possible that he is not the same person even though his name and address appear to be the same.

Another example is the case where a patent is to be transferred from the person named in the register to a transferee. The transferee requires to derive a satisfactory title to the patent. They need to establish a link, in the form of an identity relationship, between the person named in the register and the person they are dealing with (disregarding, for the purposes of the example, intermediate unregistered dealings). Evidence of the transferor's current name and address (or other credentials) may or may not be useful for

---

[4] For which, see Wendy Moncur and Dr Grégory Leplâtre, 'PINs, passwords and human memory' *Digital Evidence and Electronic Signature Law Review* 6 (2009) 116-122.

establishing the link. For instance, the purported original of a utility bill may be one item of evidence used to link the purported transferor to the name and address in the register. Those who demand utility bills for such purposes commonly require a recent bill[5]. But if the transferor has moved since acquiring the patent, and has failed to update the register, then a bill dating from before the move might be much more useful evidence that the person who presents it is in fact the person appearing in the register. (And it should be noted that to provide a new utility supplier with a name for your account, you just have to supply a name. The utility company has no interest in any identity relationship between the person they are now dealing with and any entry in a register or other manifestation of prior activity, nor can it be expected to assume responsibility for any kind of verification based on its bill).

A final example is the case where an individual is prosecuted for driving while disqualified. It might be necessary to prove that the person before the court is the same person as was previously disqualified (i.e. that there is an identity between the two). If this can be proved, it does not matter whether they have the same name, address or occupation as when they were disqualified previously.[6] The same problem occurs where a person is alleged to have broken a community rehabilitation order, and it is necessary to prove that that person was the same person upon whom the original sentence had been passed.[7] The significant feature of the footnoted cases is that the court (rightly) requires a true identity relationship to be established, not a mere correspondence of identifiers.

2.2. The practice of identification documents

The greater use of paper in the nineteenth century and the introduction of a permanent record enabled the State to record the life span of an individual more accurately, and to document the principal events in a person's life, such as birth, baptism (if born into a Christian family), marriage and death. It should be noted, however, that in evidential terms, these records merely chronicle various incidents in a person's life. Such records do not link the person to the event that is recorded, although in practice it sometimes seems to be assumed that a causal link between the record and its holder can be relied upon unless there is sufficient evidence to the contrary.[8] This is of course a dangerous assumption.

The most basic of documents, the birth certificate, does not provide evidence that the holder of the certificate is the person whose birth is recorded in it. There is no nexus between the content of the birth certificate and the holder of the certificate, despite any legal presumptions that might apply.[9] Although a

---

[5] It is not well known, but an electricity bill includes a reference number of the meter. Apparently, there is also an independent register of all meters in the United Kingdom. The value of the utility bill in this context is that this, together with other supporting evidence, can be used to provide sufficient evidence to help identify a person purporting to reside at a particular address. However, this information is only useful where those organizations that use utility bills are aware of this fact, are prepared to pay to obtain access to the relevant information, and then conduct checks to detect fraud when it is practised. However, it should be noted that if only the name has been changed in an attempt at forgery, checking the number of the meter will not help. Only a direct check with the issuer of the bill will detect the change.

[6] See *Pattison v DPP* [2005] EWHC 2938 (Admin), in which Mr Justice Newman discussed this issue, and reviewed the following cases: *Ellis v Jones* [1973] 2 All ER 893; *R v Derwentside Justices ex parte Heaviside* [1996] RTR 384; *Director of Public Prosecutions v Mooney* [1997] RTR 434; *DPP v Olakunori* [1998] EWHC Admin 722; *Bailey v DPP* 163 JP 518, 19 June 1998 (Crown Office List); *Whitmarsh v DPP* unreported, 1 March 2000 (Divisional Court). Further cases include *R v Burns* [2006] EWCA Crim 617, [2006] 2 Cr App R 264, [17] and *R v Lewendon* [2006] EWCA Crim 648, [2006] 1 WLR 1278.

[7] *West Yorkshire Probation Board v Boulter* [2005] EWHC 2342 (Admin).

[8] Under English law, non-parochial registers recording births, marriages and deaths, which were previously not kept under public authority or in performance of a public duty, were not receivable as public documents until the passing of the Non-Parochial Registers Act 1840. This Act was extended by the Births and Deaths Registration Act 1858, ss 2-3 to records made before 1840.

[9] Registers of births and deaths are kept under the Births and Deaths Registration Acts 1836 to 1953. Section 34 of the 1953 Act provides, in subsection (2) 'An entry or a certified copy of an entry of a birth or death in a register, or in a certified copy of a register, shall not be evidence of the birth or death unless the entry purports to be signed by some person professing to be the informant and to be such a person as might be required or

birth certificate is a record of the birth of an individual, it does not follow that the person whose name is on the certificate is same person as the individual in whose possession the certificate rests, even if he uses the same name. The most that can be said of certificates of births, deaths and marriages is that if a certificate was issued shortly after the date of the event recorded in it, it is more likely to have been issued to a person closely connected with the event than to a stranger; but a certificate issued shortly before it is proffered cannot benefit from any such probability.

2.3. Extrinsic evidence

In any society that relies on the birth certificate as proof of identity (in the absence of other data, such as a characteristic of an individual: for example, a biometric measurement which is also recorded on the birth certificate or a DNA sample), the tangible link between the birth and the name of an individual is predicated on the existence of the record of their birth. This evidence is erroneously assumed to be the foundation document that links the individual to the name recorded on the birth certificate. More recently, this record has begun to be used as evidence to corroborate the connection between the person named on the birth certificate and the holder when issuing other documents, such as a passport or driving licence, or to open a bank account.

In contemporary society, more diverse types of evidence are available that serve to corroborate or verify the identity relationships of an individual. It might also be observed that the longer a person lives, the more frequently they interact with agencies that create their own records. As a result, the original record of birth as evidence may cease to be relevant because it is too remote, or no such link may have been referred to when further records were created. The recognition of identity relationships often does not depend on evidence of birth. There are a range of records, both public and private, that name an individual and form a pattern of behaviour or history of events, and are available as a means of reference, such as: government records (passport, driving licence, national insurance number); local authority records (records of the names of the occupiers of a dwelling for the purposes of collecting local taxes, registering the occupants on the register of electors); bank accounts; credit reference agency records; Inland Revenue tax notification; telephone and utility payment history; credit card data and other such examples. Where a person's name is relevant to a claimed identity relationship (as will usually be the case), the existence of the claimed relationship can be supported evidentially by referring to such records, although it should be noted that these are records of daily activities or grants of permissions, rather than direct evidence of the name or address of the individual. This is because they contain no assertion about the person to whom they relate, and in particular no assertion addressed to anyone minded to rely on them. The evidence they provide is purely circumstantial.

The weight to be given to some records that are created that do not rely on the sight of a valid birth certificate can be questioned. In many instances, the issuing agency may have relied on the accuracy of the information provided by the individual, perhaps corroborated by producing a passport or driving licence.[10] Organizations dealing with personal information, such as some credit agencies, will undertake exercises to assess the breadth, depth and quality of the information, and different weightings may be attributed to the source from which the information is obtained. This mechanism demonstrates the reliance society generally places on the various types of documentary evidence that are available to corroborate the bond between a name and an individual. It follows that reliance is also placed on the accuracy of the information recorded in the document. The individual components may not be strong, but taken as a whole, they are capable of providing strong circumstantial evidence. However, most types of documentary material provide relatively weak evidence (depending on the quality of the process by which the document was issued), even disregarding, for the present purposes, the possibility that they may be

---

permitted by law at the date of the entry to give to the registrar information concerning that birth or death.'

[10] This does not exclude documents that are forgeries. Daniel Lawrence, aged 28, used over 100 forged documents to steal almost £1m: Ben Briggs, 'Pay back for fraudster with 100 fake IDs', *The Citizen*, 20 June 2008, on-line at http://www.prestoncitizen.co.uk. It is reported that he used the name Robert Ikunnah, a Nigerian immigrant living on benefits, as well as his own name, posing as a successful businessman. Apparently he took driving tests under the names he used as aliases to give them more credibility.

forged:

a. The birth certificate is a record of a historical event, and lacks any evidence to link the holder to the birth.[11]

b. A passport, even with a photograph and a scanned manuscript signature, is a travel document.[12]

c. A driving licence, again with a photograph and a scanned manuscript signature, provides proof that the person named in the document is permitted to drive certain categories of vehicles.

d. The purpose of a national insurance number is to record national insurance contributions and income tax, and for claiming benefits.

The latter three are based on some evidence to the authority that they related to the person whose name is identified and therefore provide some indirect evidence to that fact. The point is that there are varying degrees of indirect evidence of the holder. The strength of the biographical history acts to bind the individual named in the documents to a historical record of daily events that purport to act to tie the name to the individual. If such records are to have any meaning, it is important that they are accurate if they are to be relied upon to corroborate a person's identity relationship. But their accuracy is hard to assess for those wishing to rely on them.

2.4. The accuracy of other identity evidence

Verification procedures that depend on the production of documents inevitably depend on the genuineness of the documents produced. The widespread availability of good quality scanners and printers makes forged documents easier to produce than ever before.[13] The risk that a utility bill is a forgery, for instance, would be reduced if it were possible to check that it was genuine by referring to its originator. In the case of an electricity bill, for example, it would be necessary to enquire of the electricity distributor whether the customer reference or account number tallied with the customer name and address on the bill. But the probable result of such an enquiry is the response that, 'for data protection reasons', the enquiry cannot (or will not) be answered. Similar considerations apply to other documents commonly produced, such as passports and driving licences, where public sector bodies are the originators and might therefore be expected to be amenable to having such document checked for authenticity and validity.[14]

---

[11] Paragraph 1.1.1 of 'Civil Registration: Delivering Vital Change', London: Office for National Statistics, 2003 incorrectly asserts that the act of civil registration 'provides the individual with a name and identity within society.' This claim implies that the right to give a child a name is granted by the State. This assertion is both incorrect and unacceptable. The consultation document is available in electronic format from http://www.gro.gov.uk/Images/01chapters1-11_tcm69-3577.pdf. There were objections to the proposals to link registers to create a dossier on each individual, and they were subsequently abandoned at the time, but a variation of the plan has since been implemented in the form of a National Pupil Database, containing the school records of the exam results and personal details of every 14-year-old. Each child will be given a lifelong 'unique learner number', and it is reported that employers will be able to check their exam results: 'Anger over pupils database plan', *BBC News*, 13 February 2008, on-line at http://news.bbc.co.uk; Alexandra Frean, 'Every child in school numbered for life', *Times Online*, 13 February 2008, on-line at http://www.timesonline.co.uk.

[12] Although Mr Bond (see further in the text of the article) was in possession of a passport, this document did not serve to establish his identity. Note that s 26(1)(d) of the Identity Cards Act 2006 provides that a United Kingdom passport (within the meaning of the Immigration Act 1971), is deemed to be an identity document but only for the purposes of the offences set out in s 25; Charles Crinion 'Sentencing for Possession of False Identity Documents' [2008] CrimLR 702.

[13] Although modern technology is still not good enough to perfectly reproduce Prussian passports from the mid-nineteenth century, for which see Andreas Fahrmeir, 'Governments and Forgers: Passports in Nineteenth-Century Europe', 218-234 in Jane Caplan and John Torpey, editors, *Documenting Individual Identity* (Princeton University Press, 2001). Forging physical items might be slightly easier – one man was able to produce an estimated 14m £1 coins that were described as being extremely difficult to differentiate from real coins: 'Counterfeiter produced 14m bogus £1 coins', The Guardian, Saturday 15 December 2007, http://www.guardian.co.uk/uk/2007/dec/15/ukcrime.uknews4.

[14] The Government offers a 'Passport Validation Service' for a substantial fee to private sector

2.4.1. Accuracy of the record

If identity relationships are to be accurately authenticated, the weaknesses in the process of recording information must be rectified, as demonstrated by the case of Mr Derek Bond in 2003. Mr Bond, aged 72 at the time, was arrested and held in prison in South Africa for a number of weeks at the request of the Federal Bureau of Investigation, because the Bureau wrongly insisted that he was a person named Derek Sykes, who was wanted in connection with a scheme that defrauded people of millions of dollars.[15]

The process of recording information must be accurate and easily altered if errors occur, which is inevitable, given the propensity of human beings to make mistakes or be in a position of trust that enables them to deliberately alter the record. To ensure documents are issued and records created that can be used to verify claimed identities of an individual, care must be given to the process by which records are produced and corrected. Although the information contained in commercial databases is not subject to the legal presumptions that apply to some government documents, nevertheless many commercial databases are used in commerce and by governments as a means of checking claimed identity.

2.4.2. Using attributes of life to make appropriate links

In everyday life, it is not always necessary to have a precise and accurate knowledge of whom we are dealing with. Commercial organizations undertake, either consciously or unconsciously, a cost/benefit analysis. This is what the banks do when they decide on the value below which they do not check the signature on a cheque presented for payment: below some value, it costs them more to check signatures than to bear the cost of forgery. We could supply a spot of blood when we buy a house, and then a DNA comparison would show we are the same person when we sell; but this would throw the cost of HIPS into the shade (quite apart from any question of social acceptability). The police record a characteristic of an individual by taking the fingerprints of disqualified drivers, which would provide quite good evidence to support the relevant identity for a later charge of driving whist disqualified if it is necessary.

Making the link between a name and a purported identity can be carried out by reference to a passport, 'ID' card, utility bill, the electoral roll and other records. Some evidence of commonality in such identifiers may often provide adequate evidence of something or other. But usually what such an exercise provides is evidence of due (but pointless) diligence by the enquirer. Therefore it probably means that we only need to prove our identity for very serious things (whatever they might be), and the rest require a lower level of proof (for instance, of age when buying alcohol), with the relier accepting the risks. Sometimes there will be a check for an identity, such as when the trader looks up a credit record and finds it adequate for her purposes, and needs to satisfy herself that it relates to the person she is about to deal with – is he 'identical' with the subject of the record? At other times there is merely a check of the means of means of payment – is the currency note forged, is the card reported stolen – and no true check for any identity, even if a name and address are demanded. Usually the trader only wants to know if the means of exchange is good, not who she is selling to.

2.5. The registration process

Verifying identity relationships accurately, therefore, requires validation (confirmation that a person with a particular set of identity characteristics exists) and verification (confirmation that a person is who they claim to be). In most instances, documents issued by governments are accepted as convincing evidence of what they are assumed to assert. The various types of evidence adduced to validate and verify identity claims has to be checked. This can be undertaken by referring to the various commercial agencies that offer such services.

It should be noted that there is an important distinction between collecting and providing evidence about

---

organisations, primarily in the financial sector – see http://www.ips.gov.uk/identity/working-pvs.asp.

[15] 'Pensioner freed after FBI bungle', *BBC News*, 26 February 2003, on-line at http://news.bbc.co.uk; Terry Kirby, 'Briton, 72, arrested on FBI warrant is a victim of identity fraud, family says', *The Independent*, 26 February 2003, on-line at http://www.independent.co.uk; Steven Morris and Rory Carroll 'The name's Bond - but is he a fraudster wanted by the FBI or a Bristol family man?', *The Guardian*, 26 February 2003, on-line at http://www.guardian.co.uk.

a relevant identity relationship (a process sometimes called 'authentication') on the one hand, and on the other the provision of some legally binding assurance about that relationship from a trustworthy third party (sometimes categorised as 'certification' or some other kind of assurance). The sources of evidence will generally have no liability for errors in it. For instance, utility companies cannot be expected to assume responsibility to third parties who treat their invoices as evidence of their customers' names, nor does the Government make any promise to those who rely on information in the passports it issues. Certification will usually be different: the certification authorities who issue certificates for the verification keys used in digital signature systems require their customers (the makers of signatures) to accept elaborate contractual terms, and endeavour to make those terms binding also on relying parties. The difficulty which certification authorities encounter in limiting their liability to relying parties provides them with the incentive to transfer as much risk as possible to their customers.[16] It is in the context of this distinction that we discuss identity cards, and in particular identity cards for lawyers.

3. Identity cards

It may be tempting to suppose that 'identity cards' provide the solution to determining identity claims. In some cases, and under some rather stringent conditions, they probably could. In cases where an identity card is relevant, it may establish the officially registered name and address of its holder. It will only provide rigorous evidence if the person checking the card is able to perform the biometric checks necessary to establish the connection between the card and the purported true holder. Checking photographs visually is notoriously unreliable, especially for non-experts in the art.[17] Expensive equipment may be required for other biometric checks, and the cost of maintaining properly authenticated communications with the relevant central database is unknown. Even so, the only way to establish that the holder of the card is the same person as the one named in a register is to ensure that the original entry in the register contains a reference to an unchanging identity number, itself verified at the time of the original registration by production and checking of an 'identity card'. It is not yet known whether there will be identity numbers for the proposed UK database – successive passports, for example, have different numbers. Even if unique numbers are allocated (to which there would be strong privacy objections), this would only be useful if identity cards were required for the making of all new registrations, at least by those who are required to have identity cards. And of course many registrations are in the names of persons who are not required to have identity cards, such as bodies corporate, or foreigners.

3.1. ID cards for lawyers

The EU, through the CCBE, intend to introduce identity cards for all lawyers across the EU. It is probable that practitioners specialising in criminal matters may well consider that such a card will be useful to them, because they already have to take their passport along to a prison to gain entry, and if the proposed card is acceptable to the Home Office, this may be more convenient than travelling with their passport each time they visit a client in prison. Another argument for such a card is to enable each lawyer to have their practising certificate with them at all time, located on the card in digital format. This is being considered by some as a means of reducing the costs of issuing practising certificates. If the physical item of a practising certificate is so important, it raises the question what the practising certificate is for and who needs to see it – has a client ever asked to see your practising certificate? Probably never, but there is a reason for this: the person a client speaks to generally shows clear signs that they are who they purport to be (with rare exceptions): they have an office; they have a staff (even if only a single secretary); they have personal knowledge of the law (which may not be accurate, but nevertheless it is there), and a solicitor will put in motion a referral to a barrister if necessary, so the barrister's position is reinforced through the introduction by the solicitor. The extrinsic evidence does not stop there, but nevertheless this is sufficient to demonstrate the apparent irrelevance of the need for a physical item of paper, or digital

---

[16] For a more detailed treatment of the complexity of digital signatures, see Lorna Brazell, *Electronic Signatures and Identities Law and Regulation* (Sweet & Maxwell, 2nd edition, 2008) and Stephen Mason, *Electronic Signatures in Law* (Tottel, 2nd edition, 2007).

[17] R Kemp, N Towell, G Pike, 'When Seeing Should Not Be Believing: Photographs, Credit Cards and Fraud,' in *Applied Cognitive Psychology*, Volume 11(3) (1997), pp 211-222.

document, upon which to store the practising certificate.

However, let us, for the sake of argument, agree that it is necessary to issue a document called a practising certificate. Assume, for the sake of argument, that a client wishes to test the accuracy of the information stored in the practising certificate, and to gather sufficient evidence to satisfy themselves that the person sitting opposite them and claiming to be a solicitor is indeed the same person whose name is printed on the practising certificate. A telephone call to the Law Society will not be sufficient for the client or the Law Society. The client may know the correct telephone number of the Law Society, but (this example is highly unlikely) they may speak to somebody who will tell them false information; alternatively, they may be informed that a person with the name of the practising certificate is recorded as being included on the roll of solicitors, but the client may not ask such questions as how many solicitors have the same name, when was the person whose name is on the practising certificate admitted as a solicitor, and whether the person named on the roll and the practising certificate are registered at the particular geographical location at which they are situated. Further, the client may not have any physical evidence of this discussion to corroborate the information that might have been conveyed. The Law Society may be most unwilling to corroborate the details of a practising certificate against a named solicitor, on the basis that they do not know whom they are speaking to, and it may be that the person is seeking sufficient information to impersonate the solicitor in question. Altogether, this could be a most unsatisfactory situation for both the client and the Law Society, especially if a request was made every time a solicitor was instructed.

Now consider the position where the certificate is stored in digital format in an identity card. By itself the use of a plastic card may make forgery rather harder than it is with paper certificates, since the everyday availability of colour printers is not matched by the availability of equipment for making copies of plastic cards. But proponents of identity cards are not usually satisfied with this modest improvement in security. They seek to establish strong links between the card and its issuer (so that forgery is made harder), and between the card and its holder (so that one person cannot use another's card). Without these strong links, identity cards can achieve only a marginal improvement in security for those relying on practising certificates (hardly anyone) against being deceived by a forgery (correspondingly rare).

There is no easy way to make the links, however. Good quality forgeries, even of passports, are hard for experts to detect, and impossible for laymen. Microprocessor technology can solve this problem, but only where the person who wishes to test the genuineness of a card has available a reliable reader. A cash machine can check that the chip card presented to it has a genuine chip issued by a participating bank. A client in a lawyer's office has no such machine – and if the lawyer offers the client the use of the lawyer's machine, how does the client know whether the machine can be trusted? If legal professions issue identity cards, will the rest of the world install the equipment required to check that they are genuine? And will that equipment be trustworthy, or will it instead be exposed to being subverted so as to steal lawyers' credentials?[18]

Even if those to whom identity cards are offered by lawyers are assumed to take the risk of forgery of the cards, how are they to be sure that the card, even if genuine, is being presented by the person named in it? The card may bear the holder's photograph; but, as suggested above, non-experts find it very difficult to detect discrepancies between photographs on cards and the appearance of the holder. Such discrepancies would be easier to detect if the card could be inserted into a reader with a screen that displayed a full size picture, but few clients would have such a machine available. Other methods for linking the card to the proper holder involve storing in the card digital representations of the proper holder's fingerprints, iris patterns or DNA; these vary in their inherent reliability, though this can be very high in some cases, but have in common a requirement for procedures for checking the link which are impractical for general use and may be incapable of functioning without significant delay.

These considerations will inexorably drive proponents of lawyers' identity cards to use the problems explained above as an excuse for marketing digital signatures as a purported solution to them. The cards

---

[18] On the subversion of card readers, see Saar Drimer, Steven J. Murdoch and Ross Anderson *PIN Entry Device (PED) vulnerabilities,* http://www.cl.cam.ac.uk/research/security/banking/ped/.

will contain a key for making digital signatures, and a signature validation key itself contained in a certificate digitally signed by the card issuer and attesting to the link between the named holder and the verification key. This does not wholly dispense with the need for the client to obtain equipment to check the validity of the signature made by the lawyer using the card and the signature of the card issuer contained in its certificate; but the equipment needed for these purposes is a personal computer with an Internet connection, which probably reflects the irreducible minimum of what is required (short of special purpose equipment). The lawyer can sign some formal statement, and send the client the signed statement and the certified verification key. The client can check that the statement was signed by the signature key corresponding to the verification key provided, and can check the signature of the card issuer on the certificate by going to the issuer's website to retrieve its verification key in turn.

Security experts will be aware that there are weaknesses in this approach: general purpose computers cannot be regarded as trustworthy in the face of sophisticated attacks, for one thing,[19] and it is not at all easy for the client in the example to be sure they have reached the genuine website of the card issuer to obtain the genuine verification key, for another. But we see more fundamental objections to such an approach, the most obvious being that not one client in a million is likely to be able to carry out the procedures required with any understanding of what they imply or any confidence in the result. Expecting a client (or anyone else expected to rely on a lawyer's signature) to go through such a procedure seems wholly absurd. To execute a deed used to require the client to place his finger on the seal and utter the words, 'I do this as my act and deed.' The procedure has long been abandoned in the face of ridicule. That ought to be a warning to those hoping to replace it with the convoluted processes required to carry out a diligent verification of a digital signatures.

But there is another, less obvious, objection which ought to be a major concern to lawyers. It concerns liability and the burden of proof. Consider the case where an imposter obtains a genuine passport in your name using a copy of your birth certificate to support his application. Assume that he succeeds in borrowing a large sum of money by impersonating you through the use of the passport, but disappears with the proceeds. You are plainly not liable for the debt, since you did not incur it (and it is for the creditor to prove that you did, not for you to prove that you did not). The Identity and Passport Service (the UK Government agency which issues passports) is not liable either: it did not certify that the imposter was you, nor does it in fact certify anything to anyone (and a claimant against it would certainly carry the burden of trying to prove otherwise). What will the situation be if lawyers' professional bodies issue identity cards to them and issue certificates for their verification keys? The card issuers will face a dilemma. They would like to accept as little liability as is accepted by the issuers of passports (namely none); but in order to make their cards acceptable to official users, and to gain acceptance in the private sector, they will in practice have to accept some level of liability risk (the cost of which will fall either on all their members, or on those of them accepting identity cards).

Card users also face risks. The security of a signature key is no better than the security of the password required to activate it; and because signature processes are carried out using general-purpose computers, malicious software may compromise keys or cause them to be applied to documents of which the user is unaware. Even users who take all due care could find their signature key misused; and of course users could deliberately or carelessly give other people access to their signature key. (In this respect digital signatures are less secure than those made by handwriting: the ability to make a holograph signature[20] simply cannot be transferred from one person to another. Holograph signatures are bound to their makers in a way that technology has so far failed to replicate for their digital counterparts.) Because of their transferability, digital signatures cannot be made acceptable without a legal framework in which persons to whom signature keys are provided (or who publish verification keys for signature keys they have

---

[19] For which, see Daniel Bilar, 'Known knowns, known unknowns and unknown unknowns: anti-virus issues, malicious software and internet attacks for non-technical audiences' *Digital Evidence and Electronic Signature Law Review* 6 (2009) 123-131.

[20] By this expression we mean a signature made by the hand of the signatory. This is to be distinguished from a 'handwritten signature', an expression which (at least in English law) includes a signature written by one person at the direction of another, the latter being treated in law as its maker.

themselves created) are made responsible for the signatures made with those keys. Various mechanisms purport to establish such legal frameworks. One possibility is that a contract between the card issuer and its user binds the user to accept responsibility for signatures made with his key, the term in question being expressed to be for the benefit of all third parties relying on such signatures.

For instance, this method (though without express extension for the benefit of third parties) has been accepted by the Law Society of Scotland on behalf of its members in respect of the Automatic Entitlement to Title of Land (ARTL) system run by the Keeper of the Registers of Scotland. Solicitors are required to enter into a substantial agreement with Trustis Limited and the Registers of Scotland in respect of the digital signature key issued to each solicitor for the purposes of using the electronic conveyancing system. Trustis operate under what is called the 'ARTL PKI Base Certificate Policy' (v1.0.doc), in which the solicitor users are referred to as 'subscribers'. The absolute liability of subscribers for all use made of their signature keys appears from clauses 1.3.3 and 4.4.1, relating to the duties of subscribers:

> 1.3.3 A Subscriber is an End-Entity (such as a person or organization) that has applied for, and received a Certificate. It is the Subscriber that contracts with an Issuing Authority for the Issuance of Certificates. The Subscriber bears responsibility for the use of the Private Key associated with the Certificate. The Subscriber may be a Subject acting on its own behalf.
>
> 4.4.1 The Issuing Authority shall undertake to clearly inform the Subscriber that by accepting a Certificate Issued under this Certificate Policy, a Subscriber agrees to, and certifies, that at the time of Certificate acceptance and throughout the operational period of the Certificate, until notified otherwise by the Subscriber:
>
> No unauthorised person has ever had access to the Subscriber's Private Key.

The extent of the responsibility to be accepted may be controversial. Absolute responsibility (with no excuses permitted) requires the user to accept all the technical risks. This is of course attractive to relying parties, but it is hard to see that the user gets a benefit commensurate with the risk.[21] The responsibility may instead be qualified, so that the user is not liable for signatures he repudiates unless the relying party can prove that the user made the signature or that the user's carelessness caused the relying party's loss from relying on the fraudulent signature. This might be acceptable to users, but imposes an impossible burden on the casual relying party (though it might reasonably be accepted by a well-resourced relying party with strong technical competence).[22] It is open to the criticism that it makes digital signatures too easy to repudiate. In consequence it is sometimes suggested that the solution is to make the user responsible for all use made of his key unless he can prove that a particular signature was neither authorised by him nor made as a result of his carelessness. This reverse burden of proof of matters of which there will often be no evidence either way can be criticised as amounting to a disguised imposition of absolute liability.[23]

It should be noted in passing that users must be able to revoke compromised signature keys, issuers must be able to revoke certificates for such keys, and prospective relying parties must be able to check that keys and certificates have not been revoked when they rely on them. Mechanisms to achieve these results

---

[21] Which means the card and every computer it is used in must be guarded with even greater care than your copy of the first edition of the Fitzgerald translation of the Rubaiyat of Omar Khayaam.

[22] This is in fact the qualified responsibility accepted as sufficient for e-Conveyancing in England & Wales by the Chief Land Registrar, as reflected in the applicable forms of Network Access Agreement, for which see www1.landregistry.gov.uk/assets/library/documents/full_network_access_agreement_v2.0.pdf.

[23] Parliament granted the government of the United Kingdom the power to reverse the burden of proof where a Minister considers it appropriate (Electronic Communications Act 2000, s8 and, for tax-related matters, Finance Act 1999, s132) These powers have been exercised for the benefit of certain public sector bodies in relation to their dealings with citizens, but not as between private parties. For examples, see The Housing Benefit and Council Tax Benefit (Electronic Communications) Order 2006 Statutory Instrument 2006 No. 2968 and The Income and Corporation Taxes (Electronic Communications) Regulations 2003 Statutory Instrument 2003 No. 282.

introduce additional risks and costs which must be allocated fairly and transparently by the legal framework: further controversial issues require resolution for this purpose.

These problems are not new, being inherent in the public key infrastructures which have been proposed over the last ten to fifteen years. The fact that public key infrastructures have failed to provide their predicted benefits (outside a limited number of 'closed loop' products) should in our view be recognised as evidence that no satisfactory solution is yet available for the problems we have described.[24]

4. Conclusions

Those faced with the problem of how to verify a person's identity would be well advised to ask themselves the question, 'Identity with what?' An enquirer equipped with the answer to this question is in a position to tackle, on a rational basis, the task of deciding what evidence will be useful for the purpose. Without the answer to the question, the verification of identity becomes a sadly familiar exercise in blind compliance with arbitrary rules.

In short, identity cards will not solve the problem of establishing identity relationships. Identity cards for lawyers will also risk creating costs, burdens and liabilities for lawyers and their professional bodies without conferring any countervailing advantage either on them or on society.

Nicholas Bohm (nbohm at ernest dot net*)* is a retired solicitor and a member of the Law Society's Technology & Law Reference Group. **Stephen Mason** (stephenmason at stephenmason dot eu) (http://www.stephenmason.eu/) is a Barrister and a member of the IT Panel of the General Council of the Bar of England and Wales and the UK representative on the IT Law Committee of the Council of Bars and Law Societies of Europe (CCBE).

[24] Dr. Aashish Srivastava conducted research on this topic for his PhD, and his findings are discussed in his article 'Businesses' perception of electronic signatures: An Australian study' *Digital Evidence and Electronic Signature Law Review* 6 (2009) 46-56.