Liberty, Security, Identity

A response to the Government's Consultation Document[1]

David Llewellyn-Jones
david@flypig.co.uk
http://www.flypig.co.uk/
7th October 2002

Overview

In general a conflict exists between those that seek increased security and those that champion civil liberties. As much as anywhere else, this conflict surfaces in the discussion of identity cards. The argument in favour of identity cards centres on the need to improve the security of citizens and protect against identity fraud. Those that argue against maintain that any requirement that people must obtain an identity card constitutes an unnecessary intrusion into their personal lives.

This conflict may *seem* insurmountable, but in this document I will argue that an ideal middle ground does exist. The beauty of the system proposed here is that it does not constitute a compromise between the two positions, but instead provides a genuine solution. From the point of view of security, the system will allow a person's identity to be established without any increase in doubt compared to a conventional identity card scheme, whilst from the point of view of civil liberties, it ensures that it is the individual who retains complete control over their own personal information.

Let us consider the two issues separately for the time being. As far as ID cards are concerned, the crucial issues which concern civil libertarians are the following:

i) any central database of information places too much power in the hands of certain individuals or organisations;

ii) identity card schemes in general move the use of personal data from the control of the individual and into the control of some other party.

Many would argue that these issues can be avoided by the introduction of sensible legislation. For example, strict controls over accountability and the way the data may be used would be intended to allay any fears that it might fall into the wrong hands or be used for inscrutable purposes. Under the proposed scheme described in the government's consultation paper, such controls would fall under the jurisdiction of the Data Protection Act 1998. Unfortunately this misses the point: the introduction of any ID system rests on the presumption that a significant number of people exist who are willing to break the rules. It would be duplicitous of the government to suggest that this applies to the general community but not to itself, so any system which is to truly avoid the above issues must provide a genuine guarantee that this will be the case.

From the point of view of the government, the important issues are very different. In the government's consultation document[2] it is stated that an entitlement card scheme should:

i) provide people who are lawfully resident in the UK with a means of confirming

[1] 'Entitlement Cards and Identity Fraud - A Consultation Paper', July 2002. To obtain the document see http://www.official-documents.co.uk/document/cm55/5557/5557.htm or http://www.homeoffice.gov.uk/dob/ecu.htm.

[2] The list of issues can be found at the top of page 7.

their identity to a high degree of assurance;

ii) establish for official purposes a person's identity so that there is one definitive record of an identity which all government departments can use if they wish;

iii) help people gain entitlement to products and services provided by both the public and private sectors, particularly those who might find it difficult to do so at present;

iv) help public and private sector organisations to validate a person's identity, entitlement to products and services and eligibility to work in the UK.

The system described here is intended to genuinely avoid the civil liberties issues whilst at the same time goes a significant way towards addressing the motivations given above. Only the requirement (ii) that the scheme should establish a single definitive record for use by the government is left unfulfilled.

In order to explain how such a system would be put into practice, it will be necessary to explain some details about public key cryptography. These will be explained in the next section, but just before we proceed to these it may be useful to give a brief outline of some of the key points of the system which allow the criteria above to be satisfied. These can be summarised as follows:

- all of the data provided by individuals would be held *only* on the card itself, it would not be kept on any central database;
- the data on the card would only be accessible by those that already knew it, in particular, this ensures that the cardholder maintains control of who she chooses to provide the data to;
- the data on the card remains intrinsically tied together at all times, so that if the card contains a photograph and a name then you are guaranteed that the name belongs to the person matching the photograph;
- it is not possible to forge a card. The data on the card is secure both in that it cannot be casually read, and in that it can only be copied in an entire unit. The name can never become separated from the photograph, and so on;

In order to achieve this, a number of techniques are utilised. The first ensures that the data cannot actually be read from the card. Instead it can only be 'verified'. That is, you can ask a question of the card and receive a 'yes'/'no' response; for example, you can ask whether or not the address held on the card is say '46 Ladbroke Grove, Ladbroke, Ladbrokeshire, UK', and obtain an affirmative or negative response. In this way the data can only be used to verify what you already believe you know.

The second technique ensures that all of the data is 'signed' in its entirety using a government digital signature. Changing any aspect of the data, no matter how slight, would 'destroy' this signature, and only the government would have the means to produce such a signature. In this way, if the data is copied it must be copied in full and hence no counterfeit card would be of any use, assuming suitable biometric data is held on the card.

Both of the techniques have been well known and widely used for some time and stand up to mathematical scrutiny. That is, they are guaranteed to adhere with a level of certainty which can be determined mathematically.

[3] For a more complete exposition of public key cryptography, many excellent texts exist. For a non-technical discussion, see S. Singh, *The Code Book* (Fourth Estate, 1999) whilst N.

Public Key Cryptography[3]

Public Key Cryptography relies on the notion of an ‘asymmetric encryption key’, something which was first proposed in 1975 by Whitfield Diffie in collaboration with Martin Hellman and Ralph Merkle. The first workable public key encryption system was subsequently introduced by Ron Rivest, Adi Shamir and Leonard Adleman (RSA) in 1977[4]. RSA has remained one of the most popular public key cryptographic systems, largely due to the work of Phil Zimmermann on his PGP encryption software. This has been successfully and widely used, especially for secure encryption via email and over the internet, and a great deal of work has gone in to ensuring that it remains a secure system. The risks involved in using such a system would therefore be minimal.

In contrast to standard encryption techniques which use only one ‘key’, public key cryptography uses two: a public key and a private key. A key is basically a password which is used to scramble the information which you want to encrypt. Standard cryptography uses the single key to both encrypt and decrypt the message (hence it is termed ‘symmetric’ encryption). With public key cryptography, however, only the private key can be used to *decrypt* data, whilst the public key can only be used to *encrypt* data. Because of this, the public key is generally made widely available so that any one can encrypt a message. However, an individual would always keep their private key a secret. In this way, only someone with access to this private key can unscramble the data encrypted using the corresponding public key.

The best way to demonstrate the method is often using an example. So, suppose Alice wished to send a secret message to Bob, the usual course of events could therefore go something like this:

Alice obtains Bob’s public key, which Bob has made available to anybody who wants it, and then she encrypts her message using this key. Alice can then send this encrypted message to Bob. Now in order to decrypt the message it is necessary to use Bob’s private key. However, this is not generally available (not even to Alice) so nobody except Bob (not even Alice) is able to read the encrypted message. Bob, however, has a copy of his private key, so he alone can decrypt the message and read what it was that Alice sent to him.

There is one other important aspect of public key cryptography which is worth mentioning. Using a private key it is also possible to ‘sign’ a piece of data. This signature will change depending on the data that is being signed and the private key used. For any given private key, a signature can be produced for a piece of data only if you are in possession of the private key. The corresponding public key can be used to *verify* the signature, but not to produce one. Verifying a signature tells you whether or not the signature for a given piece of data was produced using the private key which corresponds to the public key you use for the verification. What this means is that it is possible to guarantee that a piece of data has come from where it claims.

Again an example may be helpful. Suppose Bob wants to send a piece of data to Alice so that Alice can be sure that Bob sent it to her. Bob would use his private key to produce a signature for the piece of data. He would then send both the data and the signature to Alice. Since only Bob possesses his private key, nobody else would be able to produce such a signature. But how does Alice know this? Well, she uses the public signature to verify that

Koblitz, *A Course In Number Theory and Cryptography* (Springer, 1987) provides a mathematical treatment. A web search will also produce many excellent discussions.

[4] It has recently been claimed that the system was in fact originally conceived in the late 1960s and early ’70s at GCHQ by James Ellis, Clifford Cocks and Nick Patterson.

the signature which Bob sent to her was produced using his private key. Suppose someone had intercepted the data and changed it before Alice was able to receive it. Well, in this case, since the signature depends on the data, the signature and data would no longer match. Only if a new signature was produced using Bob's private key would the data and signature once again match, but our interceptor would not have access to Bob's private key so would be unable to produce such a signature. Alice, on receiving the intercepted data, would find that the public key no longer verified the signature for the data and she would therefore know that the data had not genuinely come from Bob.

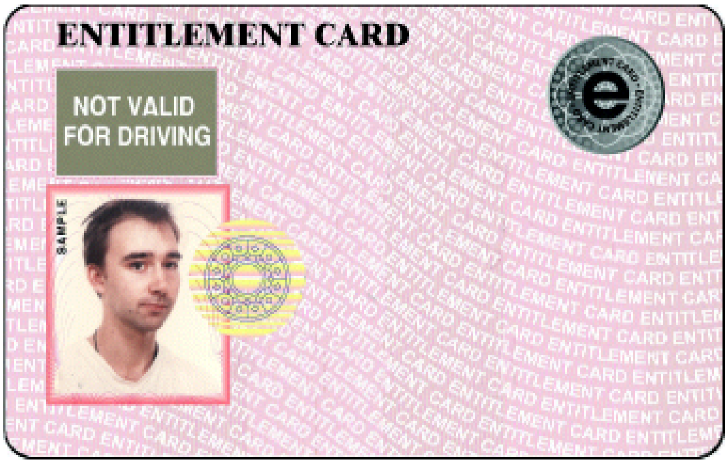
In short, the functions of public and private keys can be summarised as follows:

- a **public key** can be used to **encrypt** data, but not decrypt it;
- a **private key** can be used to **decrypt** data;
- a **private key** can be used to **sign** a piece of data;
- a **public key** can be used to **verify** the signature for a piece of data, but not sign it.

Technical details of the card

Unlike identity cards as they might usually be known, one of the most important features of the card as it is described here involves the fact that no personal information is displayed externally, other than the holder's photograph (see figure 1). It is possible that there are certain other pieces of information which it would be permissible to display, but the description given here is intended to explain the principles involved rather than providing a definitive specification. Instead of having personal information displayed as text on the outside of the card, all of the data would be held internally on a microchip - a so called smartcard - which could be accessed using card reader hardware.

Figure 1 - Example identity card layout



The example card provided has been set up to contain certain pieces of personal information. These are:

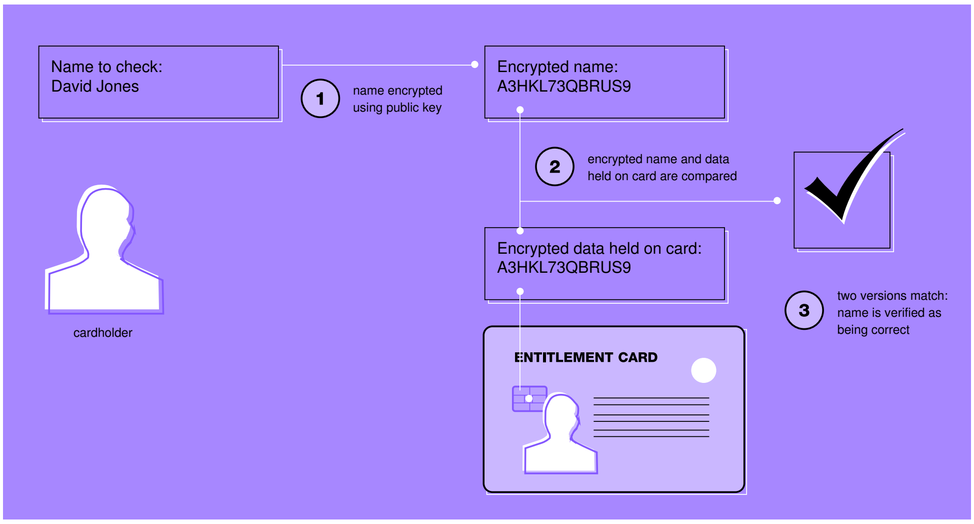
i) name;
ii) address;
iii) date of birth;
iv) place of birth;
v) passport number.

In addition to this the card also contains a digital version of the photograph displayed on the outside. For further information about how to use the example card, see the instruction document ‘**Instruct.pdf**’. There is no reason why the card could not contain other pieces of information, and biometric data such as fingerprint or iris patterns[5].

The photograph (**portrait.jpg**) is the only piece of information which is freely accessible. All of the remaining data has been encrypted using a public-private key pair and then stored on the card (**privdata.dss**), after which the private key was then destroyed. However, the corresponding public key (**public.dss**) has been stored on the card along with the encrypted data. What this means is that the data can no longer be accessed, and because the private key has been destroyed there is now *no way* that the data can be read, thus ensuring the privacy right of the individual concerned. Every card produced would use a distinct (random) public-private key pair to achieve this.

However, since the public key is retained on the card, there exists a way to *verify* the data. Thus, if you believe the card belongs to someone called ‘David Jones’, say, then you can discover whether this is the case or not. This is done be *encrypting* the name ‘David Jones’ using the public key held on the card, and then comparing this encrypted name against the encrypted version of the name held on the card. If the two match, than your belief was correct - the name stored on the card is indeed ‘David Jones’. If, however, the two do not match, then all you know is that the name stored on the card is *not* ‘David Jones’; you cannot actually find out what the name is. Figure 2 depicts the process diagrammatically.

Figure 2 - Verifying data held on the card



The motivation for providing data which can be verified but not read is that of the civil libertarian, who wishes to ensure that control of personal data remains with the individual. By doing this the cardholder has complete control over who has access to the data, since verifying the cardholder’s name (or other details) requires that the cardholder first provides their own name and hence consent for their name (or other details) to be known. Another salutary consequence of this is that, should the card be lost or stolen, it would be useless unless more information was already known about the data held on the card.

[5] For any biometric data other than a photograph, the data should be encrypted along with the other data, so that only verification would be possible.

Nonetheless, the fact that the data held on the card can only be verified, does not reduce the usefulness of the card for proving identity. In any situation where the cardholder wishes to prove their own identity, the card offers them this opportunity. Coupled with the photograph held digitally on the card, they are able to prove indubitably that the name and other details held on the card refer to them. Equally, from the point of view of a service provider — by verifying the data held on the card — they can be certain that any person is who they claim to be.

From the government's point of view, this therefore satisfies the requirements (i) and (iv) outlined in the overview above, that an identity card should provide people who are lawfully resident in the UK with a means of confirming their identity to a high degree of assurance; and that it should help public and private sector organisations to validate a person's identity, entitlement to products and services and eligibility to work in the UK.

The second major feature of the card involves the use of data signatures to ensure that only the government is able to produce identity cards. Normal practice might be to use visual indications or other security features on the external surface of the card to guard against counterfeiting. Examples of these might be the use of holographic images, ultraviolet markings or even straightforward intricate design. The biggest drawback with such methods is that it is always possible to overcome them, given sufficient will and resources on the part of the counterfeiter. The card which is proposed here would not need to make use of any of these methods. Instead each piece of data on the card is signed using a private key which only the government has access to, using the methods described in the section on Public Key Cryptography above. On the example card provided, these signatures can be found in the **signature.dss** file. Using this system it would be necessary to distribute the corresponding government public key as widely as possible, a crucial requirement being that it be supplied with all card reading devices or software. Any card reading device would then be able to verify — using the public key — that the data on the card had indeed originated from a government source.

Since the data is split across several files on the card, it has also been necessary to sign the signature file using the government's private key (this signature can be found in the **sigsig.dss** file). This ensures that there is no way to split the data apart. That is, the photograph held on one card could never be mixed with the other data such as name and address taken from a second card. In this way, although it is possible to copy the entire contents of the card, it is not possible to change it in anyway, ensuring that the copying of card data presents no benefit to potential counterfeiters.

Due to the photographic or biometric data being held on the card, there would be no reason under this system to refuse the granting of multiple cards to any individual, since the card could only be usefully used by the designated cardholder. There would also be no reason to prevent individuals from reading the data from the card, for example if they were to use a card reader attached to a home PC, since not only could the information not be usefully read, but copying the data would present no opportunity for fraud or misuse.

It is worth pointing out that current smartcard technology could be used to produce cards as they are described here and that no new or untested technology is required. The data held on the example card, including the digitally stored photograph and all of the key signatures, measures just over 12kbytes of data. A standard smartcard will often hold at least 16kbytes (as for example is the case with the new smartcard introduced in Austria this year, as detailed in the government's consultation document). Given the extra overhead of digital signatures, there still remains a significant amount of remaining memory which could be left for entitlement information or for use by private sector service providers. Hence the government's stated aim (iii) above that any identity card should help people gain entitlement to products and services provided by both the public and private sectors, would not be compromised.

As an additional note, none of the security provided by the card requires that either the data on the card, or information concerning the software and hardware used to read this data need be withheld from the general community. Indeed it is widely acknowledged that the safest method for ensuring that a system is secure, is to make as much information about the system available as possible. In the case of the example card provided, all of the source code for the software required to both create and read the data on the card is given on the card. Making the methods used to encrypt the data available in this way does not in any way reduce the overall security of the system.

The card in use

One of the differences between conventional ID card schemes and that proposed here is that conventional schemes operate using a central database which holds a copy of all of the personal data which is also displayed on the card. For the scheme described in the government's consultation document, in order for an inquirer to ascertain the guaranteed authenticity of a particular ID card, she must contact the central database and request verification of the details contained on the card. With no central database this is of course impossible, however the scheme described here bypasses this need by containing all of the information required to authenticate a particular ID card on the card itself.

A consequence of this is that, in general, the process of proving a person's identity or details using the system described here is somewhat more straightforward.

The government's consultation document describes a variety of situations in which an ID card might be used, and although translating the processes described into equivalents which would apply to the system described here would be possible, for the sake of brevity we present just two cases.

The first case involves that of providing an off-line biometric check. Figure 3 below shows a diagrammatic representation of the process, which corresponds to figure 5.9 on page 59 of the government's consultation document. In order to clarify we will also describe the process briefly here.

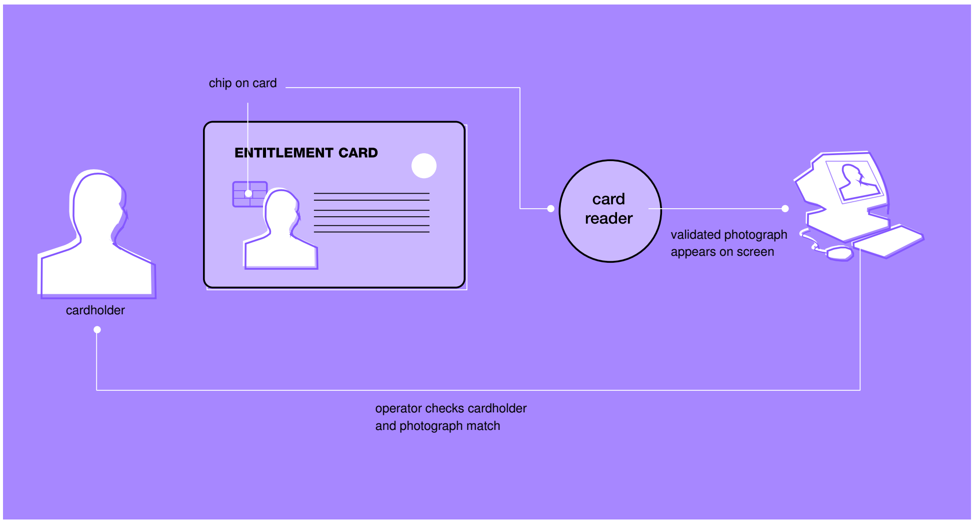
The goal is for the service provider to verify the details of the cardholder, so that they can be certain of the person's identity. The cardholder therefore supplies their identity card to the service provider, who uses a generic card reader connected, for example, to a standard PC to read the digital photograph data from the card. The image would be displayed on the service provider's screen, so that they can check that the card is genuinely that of the cardholder. Since the data is signed and the signature is also stored on the card, the service provider is also able to be certain that the ID card is authentic and was genuinely produced by the government. Other forms of biometric data could be used, other than a digital image of the cardholder. Examples might be fingerprint or iris patterns, although special hardware would also be required in order to obtain the fingerprint or iris pattern of the cardholder[6].

Having established that the card is genuine and that it belongs to the cardholder, the service provider as yet has no further details about who the cardholder actually is. This is because the data on the card is encrypted, and it is not possible to read it directly. So suppose the service provider wished to know the name and address of the cardholder. The cardholder would then have to supply her name and address, and the cardholder could then

[6] For any biometric data other than a photograph, the data should be encrypted along with the other data, so that only verification would be possible.

verify that these details applied to the cardholder by checking it against the encrypted data held on the card (as in figure 2 above). In this way the service provider can be certain that they have the cardholder's correct identity and details, whilst at the same time the cardholder retains control over what particular data the service provider is able to ascertain.

Figure 3 - Off-line biometric check


chip on card
ENTITLEMENT CARD
card reader
validated photograph appears on screen
cardholder
operator checks cardholder and photograph match

The second example involves the validation of on-line transactions. In this case the cardholder, in conjunction with a home card reader, would send all of the data held on the card to the service provider on-line. In contrast to what might normally be the case, this data is effectively useless to the service provider without further assistance from the cardholder, since they are unable to actually read the encrypted data which has been sent to them.

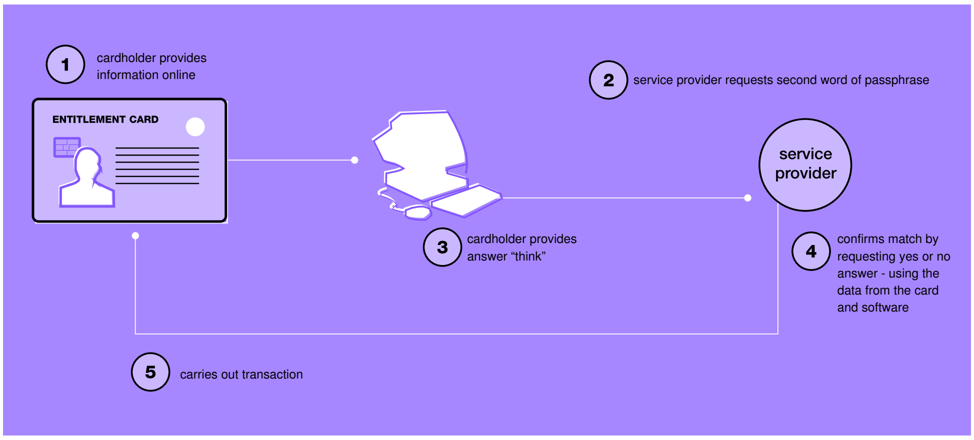
The cardholder would therefore have to supply additional information, such as her name and address, and the service provider would then be able to verify that the name and address were indeed genuine. However, in itself this would not prevent someone from using a stolen card on-line, although it would not be possible for a stolen card to be used effectively, since the address on the card could not be changed by the thief.

As with the scheme described in the government's consultation document, it would be possible to store an extra passphrase on the card in order to guarantee that the person using the card was indeed the correct cardholder. The process involved is shown below in figure 4, which corresponds to figure 5.8 on page 58 of the government's consultation paper. In this case the service provider would also ask the cardholder to provide one section of their overall passphrase, such as the second word. Having transmitted the data, the service provider would already be in possession of an encrypted version of this passphrase, but would not be able to decrypt it and hence could not know what the passphrase actually was. The cardholder would then provide the second word of their passphrase (in this case 'think') and the service provider could then use the card to validate that this was indeed the second word of the passphrase stored on the card.

In the same situation, under the scheme described in the government's consultation paper, the service provider would be unable to verify the passphrase simply using the data on the card, since the passphrase would not be stored on the card. Instead, she would have to rely on contacting the central register, which would then provide the same service: replying 'yes' or 'no' to the question of whether this was indeed the second word of the person's registered passphrase.

Obviously, by avoiding any recourse to a central register, the whole process of validating the passphrase becomes significantly simplified. Nonetheless the system is no less secure if the data is held on the card in the way described here.

Figure 4 - Using secret card-holder information to validate on-line transactions


1 cardholder provides information online
ENTITLEMENT CARD
2 service provider requests second word of passphrase
service provider
3 cardholder provides answer "think"
4 confirms match by requesting yes or no answer - using the data from the card and software
5 carries out transaction

Whilst considering the manner in which on-line transactions are carried out, it is worth pointing out that, since under the system proposed here the duplication of data held on an ID card does not pose a security risk, there is no reason why a person should not be entitled to store an exact copy of the data held on their ID card, perhaps on their home computer or on a floppy disc. Hence it would not be necessary for an individual to have access to an on-line card reader in order to access on-line services in this way, since she could simply use the copy of the data stored on her computer or on a floppy disc.

Once an on-line service provider was satisfied that the card belonged to the cardholder undertaking the transaction, it would then be necessary for the cardholder to provide any further details (such as name or address) required to complete the transaction. The data from the card itself would be inadequate on its own, since the encrypted data cannot be read. Having received any further details, the service provider would be able to use the data from the card to validate that these details were indeed correct.

Again we see that there is a level of transparency which would not pertain if a standard smartcard ID system was used. For the cardholder is never under any misapprehension as to the data the service provider has access to, since any information the service provider obtains must be overtly provided by the cardholder.

Cost

Surprisingly, the cost of introducing the system described here would be potentially cheaper than the example described in the government's consultation document, both in terms of initial outlay and ongoing running costs.

For the most part, the costs would be the same, however the area where significant saving would be made lies in the lifting of a requirement to maintain a central database along with its associated network structure.

The government's estimated costs included £45 million as initial set up costs for a central database, along with £263 million pounds operating costs for the IT infrastructure over the thirteen year period. Removal of these requirements would therefore represent a saving of £308 million pounds over the thirteen years.

The revised costs over the thirteen year period are detailed in figure 6 below.

Figure 6 - Revised cost estimates

Type of card	Original costs (£m)	Revised costs (£m)
Plain card	1318	n/a
Simple Smartcard	1640	1332
Sophisticated Smartcard	3145	2837

Additional cost savings would be enjoyed by public and private sector organisations in relation to employment and identity checks. The system envisaged by the government required that all such checks would involve a premium rate phone call in order for the central register to be accessed. Since under the scheme proposed here these checks could be undertaken in isolation, with the required information being obtainable directly from the data held securely on the card, these phone calls along with their associated costs could be entirely avoided.

Using the figures postulated in the government's consultation document, we find an overall saving for public and private sector organisations undertaking employment and identity checks to accumulate to at least £100.5m over the 5 year period of 2007-13. This compares with a saving of at least £83.82m for the same period under the government's proposed scheme. A breakdown of this calculation is provided in Figure 7 below.

Figure 7 - Employment and identity check cost savings

	Year					
	2007/08	2008/09	2009/10	2010/11	2011/12	2012/13
Costs relating to identity checks (£m)						
Original cost savings	2.5	7.5	12.6	17.6	22.6	25.1
Phone charges	0.4	1.1	1.8	2.5	3.2	3.6
Costs relating to employment checks (£m)						
Phone charges	0.68	0.68	0.68	0.68	0.68	0.68
Total cost savings (£m)						
Original	1.82	6.82	11.92	16.92	21.92	24.42
Revised	2.9	8.6	14.4	20.1	25.8	28.7

With regard to the techniques described in the section on technical details, worries may arise over access to patented algorithms and the costs associated with them. Although patented algorithms are commercially available for implementing public key cryptographic systems, many non-patented and open source alternatives are available and a working system could be implemented without the need to use any patented technology over and above that already required for a smartcard system.

Conclusion

The main features of the identity card system described here are:

- that all information is held on the card; there is no need for a central database;
- that the data is not printed on and cannot be read from the card, only verified;
- that the data is government signed, so that any change to it (such as splitting it up) will render it invalid.

It is hoped that this system of identity cards provides a genuine solution to the problem of reconciling the desires of civil libertarians with the need to maintain security and combat identity fraud. None of the technology described here is next generation or cutting edge, it is widely and easily available now. Testament to this is the fact that a working system has been provided along with this document. Although in practical terms this provided card requires refinement, it is hoped that it will nonetheless ably demonstrate the potential and viability of the system described here.

Given that such a system exists, it would seem that any alternative which either compromises on security, or results in any additional curtailment of civil liberties, would be at best a missed opportunity and at worst a violation of people's entitlements or rights.

For more information, please feel free to contact me:

David Llewellyn-Jones
david@flypig.co.uk
http://www.flypig.co.uk/