



Response To:
'Entitlement Cards and Identity Fraud
A Consultation Paper'

John R T Brazier
Professional Projects Co Ltd
19 Barttelot Rd
Horsham
RH12 1DQ



Contents

INTRODUCTION	3
CONCLUSION	3
APPROACH	3
THE PURPOSE OF THE CARD	3
THE FUNCTION OF THE CARD.....	4
SECURITY.....	5
BIOMETRICS.....	6
COSTS	6
TRUST AND LEGAL ISSUES	7
CONCLUSION	8



Introduction

This document is a response to *'Entitlement Cards and Identity Fraud: A Consultation Paper'*, published in July 2002 by the Secretary of State for the Home Department. It provides a clear conclusion and discusses how it was arrived at.

Conclusion

It is the recommendation of Professional Projects Co Ltd, and the author, that the Government does not proceed with any entitlement card scheme with the consultation paper as its basis. The reasons for this may be encapsulated as:

1. The scheme is unclear in its aims.
2. The scheme is compromised in its implementation.
3. The scheme is not secure.
4. Biometrics are flawed, possibly leading to the exclusion of a proportion of the population.
5. The costs are probably greatly underestimated.
6. There is not a high enough trust level for the scheme to be implemented.

Approach

In analysing the consultation paper, and in preparing the response, it was decided to deal with several major themes that run throughout the paper and give a response to the overall thrust and position of the document. The consultation paper is a long and complex document, and raises many issues that should be discussed. For our purposes, however, we believe that the main threads deserve treatment on their own. Delving into too much detail in this response would tend to dilute the core issues that must be addressed before any such scheme might proceed.

This response now deals with six basic topics. It is proposed that the discussion of these topics leads ineluctably to the conclusion given above, and thus obviates the need for further analysis at present.

The Purpose of the Card

The first issue is raised right at the start of the executive summary, and runs throughout the document. The purpose of the card is to establish identity, of individuals, 'to a high degree of assurance'. This is clear. The concern arises as to why one should wish to do such a thing.

From the point of view of Government, one can see reasons for establishing identity. But from the point of view of individuals and private sector organisations such a need is much less clear. Two points need to be borne in mind:

1. Individuals and private sector organizations use cards much more for authorization purposes than identification purposes, especially with regard to financial transactions. A merchant wants to know the card is valid, and the transaction will go through. For the transaction, the merchant has little interest in the actual identity of the purchaser (which is why corporate cards and other



- such instruments may exist). A merchant may wish to know more about the purchaser to sell more goods to them, but this is not the same motivation as the one that drives the card check.
2. Individuals will not take cards or other tokens and carry them about if there is no benefit to them. They certainly will not pay for such a card.

Thus the proposal has had to find a reason why British subjects should want to carry a card. The concept of an 'Entitlement Card' is thus mooted, but it is accepted even within the paper that such an inducement may not be enough (paragraph 3.7, for example, admits that most people's interaction with government is relatively infrequent). Thus the purpose of the card is widened throughout the consultation paper. Such purposes include:

1. Unique identification.
2. Immigration control.
3. Driving license.
4. Passport.
5. Stopping identity theft.
6. Getting VAT numbers.
7. Allowing access to an unspecified number of Government services.
8. Library book control.
9. Providing an unspecified number of unspecified private sector services.

The system as proposed would also have most of the population having not one, but two cards. We would suggest that such an inchoate definition for what the card is meant to achieve and provide will guarantee it to fail.

The card will either try to be all things to all men, and will be nothing to everybody, or it will be a simple identity card, which will have limited takeup. Thus the implementation is doomed to failure, as the goals are either unclear or unpopular.

The Function of the Card

The actual functioning of the card has become compromised because of the lack of clarity in its purpose. If it is not a simple card (which might well have poor takeup), the concept would appear to be that of a multifunctional card, providing an expandable and flexible range of goods and services.

Aside from the perils of allowing such scope creep even before the design phase, the lack of definition of functions, coupled with the fact that it is very unclear how 'smart' the smart card will be (except for the two classes 'simple' and 'sophisticated') leads to a number of problems.

1. It will be difficult or impossible to design a card with unknown future functions. This is especially the case as the paper is not at times clear when services are envisioned as being solely public sector, and when they are provided by private sector companies.
2. There is no provision for security in the smart card and its allied database – certainly not in the costs. A multifunction smart card could well become a serious security target. This point will be further discussed below.



3. Without good technical design, any such multifunctional card is likely to be suboptimal in each of its functions. This will prevent any benefits being accrued from the card, as it will not be the instrument of choice for many of its functions.

Thus the card design is likely to be compromised, which could lead to a major technological fiasco. The recent case of the withdrawal of £5 notes does not make one optimistic for the development and introduction of such cards.

Security

There is little or no discussion of real security in the paper. Yet the fact is that a simple card will be inherently insecure, whilst the risks of security failures in a system based on sophisticated cards linked to a central database are huge:

1. The central database will become a prime target for criminals both within and without the establishment. Compromise of the central database has the potential to undermine the entire system.
2. Individual cards will become targets, either to recover their contents, or to corrupt their workings (especially in the case of sophisticated cards). It is possible to envisage a sophisticated card having data interaction with terminals to be corrupted by a computer virus: whilst this threat may be currently unlikely, so it was until recently with Personal Data Organisers. An attack of this sort could completely compromise the system.
3. The idea of multifunction cards aggravates the problem. How are the cards to have their functions isolated from each other? It is well known that multifunction, open systems are not secure, which why the military and security agencies carefully segregate their high-security systems.
4. The other problem of multifunction cards is that compromise of one function will compromise the whole card. This would lead to a hugely increased turnover of cards as they are successfully compromised by criminals or by accident.

Another aspect of the security issue is that of data accuracy. Despite assurances, there is no evidence that the central database will be any more accurate than the numerous disparate ones that are currently run (many of which will continue to exist after implementation of the ID card, which will make the situation more, not less, difficult). The author has seen estimates of up to 20% inaccuracy (on a given item per individual) for large population databases. Most people know this from personal experience: despite the proposal's faith in the accuracy of credit reference agencies' databases, most people know of cases where these databases have been seriously inaccurate. Thus there is a high risk that the central register will be yet another not very accurate database, to go alongside the rest.

The clear conclusion is that security just has not been thought about in the proposal. It is not costed, not discussed, and a quote is instructive: although paragraph 84 mentions the words 'in a secure way', the allusion to an unspecified digital signature function with the phrase 'While the



technical issues in including such a function on a card are relatively straightforward,' betrays a serious lack of understanding of the security issues involved.

On this basis it is believed that the scheme, as proposed, would be insecure. This is especially the case as there appears to be no security budget in the costs.

Biometrics

The paper asks if biometric information should be included in the system. There are three points about such systems which should be noted:

1. Their benefit is based on their close tie to an individual. Yet this is also their risk: when ID theft takes place with biometric data, it can become extremely difficult to unravel the situation. This is especially the case if the thief is not present. Recently a researcher has successfully spoofed thumbprints on the majority of systems by using the most basic technology. Thus a poorly implemented biometrically based system could actually be more open to fraud, rather than less. When the fraud does take place, detection can be extremely difficult and rectifying the situation almost impossible. To take an example, if someone has jury-rigged a card to send and register *your* thumbprint when they press *their* thumb on it, what is to be done? Note that this need not be a card: if the transactions are on-line, the criminal may be using a PC to completely simulate the card operations.
2. The false positive/false negative rates are too high. Essentially, biometric systems work well with small, limited populations under controlled conditions. They simply do not have the technological accuracy to work for mass screening (a recent trial at a US airport had to be abandoned due to the high false positive rate).
3. Certain people will tend to generate higher false positives or negatives than others, depending on the system used. These people will tend to be penalised solely by the actual application of the system, leading to their exclusion from the system.

On these three bases, it is concluded that biometric information should not be included in the proposed system.

Costs

Outline costs are sketched out, but it is difficult to counter them because most of the estimates are provided flat, with no justification. These estimates are then typically modified, but with no knowledge how the original was reached, little can be said in detail.

However, a few points raise concerns:

1. The central database is costed at £30M, subsequently raised by 50% for risk. This seems extraordinarily low, given the costs of large database systems in the public sector in the past.
2. There are no costs for security. This could well become a major component of cost in such a system (especially if it had to be retrofitted due to poor design).
3. The estimate for extra staff for 13 years (excluding people actually processing cards) is £62M. This is £4.8M per year or, at a cost of £25,000 a year (probably an underestimate given



average salaries), a total of 191 extra people to manage and administer this entire scheme. This would include IT staff and, it would appear, all the checks (both original validation, including biometrics, and all subsequent queries). This does not seem credible.

4. The overall cost of 140M simple cards over the whole period is estimated at £1318M. This is £9.41 per card. This seems very economical, especially as the cost recovery proposals would provide a profit (many of the quotes are for uplifts, and the new cards are intended to at least replace the driving license if not the passport).

There are other issues (such as card turnover may be much higher due to the way people are much more mobile), but these four examples indicate that the costs have been underestimated, perhaps significantly. In fact, given the past history of large government-led technological projects, the author would not be surprised if the true costs, after any scheme were implemented, were found to be up to an order of magnitude higher. Certainly this scheme should not go ahead on the proposed cost analysis.

Trust and Legal Issues

There are some unfortunate aspects to the proposal that tend to lower the likelihood of its acceptance.

One is the asymmetry between state misuse and private misuse of the system. Paragraph 2.17, for example, promises 'penalties for failure to notify changes to personal details for example change of address or change of name', yet Annex 4 paragraph 40 only provides for 'safeguards on the use of all information held on a central database'. Why are there no penalties for agency misuse, especially where biometric information is involved (and where the consequences could be disastrous for the affected individual)? Police, for example, will misuse the system – they have in the past, and have frequently only been reprimanded for doing so.

Another unfortunate attitude is in Paragraphs 6.13, where it is stated that 'There would be a requirement in law for entitlement card-holders to inform the issuing authority of changes of information held about them on the central register ...'. This is with reference to the fourth data protection principle 'Personal data shall be accurate and, where necessary, kept up to date'. This principle is meant to place an obligation on the data controller, not the data subject. Yet it has, in the proposal, become inverted – and subverted – in its intention.

Recent actions, such as the scope creep carried out by Police Forces in the retention of DNA evidence where people were not charged, show the general attitude of the government departments and functions to data held on its subjects by central authorities. Coupled with the thinking exhibited in this document, identified above, this tends to lower confidence in this scheme, and will raise opposition to it.

Lastly, as an example of this distrust, the author has noted that many opponents to this scheme believe that many problems associated with the proposal do not actually stem from muddled



thinking, but arise from dishonesty. The accusation is that the document is confused because the real intent – an ID card system that will be compulsory, managed and run for the benefit of the law enforcement agencies – cannot be stated and so has had to be camouflaged. Naturally, the author does not credit such suggestions, but they are indicative that the trust in the government is not high enough to implement this scheme without serious and implacable opposition.

Conclusion

The conclusion, based on the arguments above, is that the government should not proceed with this scheme on the basis of the proposal. All factors covered here, including the aim, operation, security, cost and trust in such a system, militate against a successful outcome.