Framework for Smart Card Use in Government

Consultation Response

Foundation for Information Policy Research

1 Executive Summary

The Foundation for Information Policy Research is an independent non-profit organisation that studies the interaction between information technology and society, with special reference to the Internet, from a broad public policy perspective; we do not represent the interests of any trade group. Our goal is to identify technical developments with significant social impact, commission research into public policy alternatives, and promote public understanding and dialogue between technologists and policy-makers in the UK and Europe.

We welcome the government's initiative in producing draft guidance on the use of smartcards in the public sector. The CCTA document may be a useful move towards weaning the public sector away from its often uncritical acceptance of the claims made by the smartcard industry. The recognition that smartcard security is not infallible, and the attention paid to management issues in section 2.2, are a most welcome first step towards sanity, and deserve greater emphasis.

However, the document continues to make an assumption which is not merely highly suspect but which the industry itself started to abandon some time ago, namely that the main benefit to be expected from smartcards will be a reduction in the number of identity and authorisation tokens which people carry, as a result of integrating multiple functions on a single card.

Following great enthusiasm for multifunction smartcards in the early 1990's, persons with experience of the industry now reckon that the only type of system in which multiple applications on one card have a serious future is where smartcards are used in consumer devices such as mobile phones and pay-TV set-top boxes, where there is only slot space for one card and the system operator's card must be there for the system to work at all. On such platforms, a bank (for example) wishing to offer its services in a way that leverages off the authentication functions in the card, has little choice but to rent card space from the operator.

However, multifunction cards have some critical vulnerabilities. Anyone who wants to provide services via the card is forced to delegate control of access to their information to the card designer or issuer. In addition, multifunction cards deprive the user of a fundamental control against abuse: the ability to decide which card she puts into which reader. These vulnerabilities lead to many complex issues of security, control and liability which we explore below.

Another source of confusion is to describe a card as multi-function when it is not; it may have the single function of saying what your name is, and perhaps your address, this name being used for many purposes which are not recorded in any way on the card itself. A good example is the California non-driving driver's license which is used solely to encourage people to believe a claimed name. Such cards can be useful although their introduction in the UK would be politically fraught: a number of attempts to introduce ID cards in English speaking countries have foundered on extreme public hostility.

Indeed, we suspect that much of the impetus behind the present document is the wish in some quarters in Whitehall to introduce an ID card – but have some third party (such as the banking industry) bear the cost and the political opprobrium. For reasons set out below, this is unlikely to be a good idea.

Government departments should not repeat the usual mistake that civil servants make with computer systems, of trying to kill two birds with one stone. This is a well-trodden road to systems that do not work well or at all, and end up costing a multiple of the original budget. It is far better to set departmental operational needs directly in the light of public opinion and other political and budgetary constraints, and contract for the construction of systems that meet them using tried and tested technology.

FIPR therefore strongly recommends that CCTA advice should:

- issue a strong warning of all the pitfalls with multifunction card technology mentioned in this response;
- be technologically neutral, and in particular it should not encourage the use of smartcards when other technology will do at least as good a job;
- avoid giving system builders the impression that the usual rules of prudent practice in business and administration can be overridden, by invoking potential synergistic benefits from hypothetical future multiple applications to bolster an otherwise flimsy business case.

2 The Report's Assumptions

The report's mission is set out in 1.4:

> Government regards the deployment of multi-function smart cards as a key enabler to the development of electronic commerce and recognises that government applications can act as a key driver towards 'critical mass'.

The bias is implicit elsewhere in the text such as at 2, 'Acquisition Issues':

> Where a requirement for a smart card has been identified, there are in effect three acquisition options:
>
> 1. make use of an existing or planned card scheme, without adding an application or data;
> 2. 'rent space' on an existing card;

3. issue cards oneself, and where possible offset the cost by making space or use available to others.

This prejudges the whole case for and against multifunction cards by making their use an underlying assumption of purchasing policy. This is most unwise, and for at least two reasons.

Firstly, the appropriate technology in many applications will not be the smartcard, or other specific user token, but the digital signature; how the user controls access to the digital signing apparatus is their problem. It has been argued by other government agencies that digital signatures will be the key enabler in electronic commerce; if this turns out to be the case then the details of whether the signing mechanism is implemented on a smartcard or a PDA or in general purpose software may turn out to be a peripheral irrelevance. Digital signatures may be most important on business to government and government to government transactions; the interaction is between organisations rather than between a government department and a specific cardholder. Yet in section 1.4 we read:

> Government recognises that smart cards have an important role to play in many government-government and government-business transactions.

Secondly, the advocacy of multiple applications – which comes at a time when the industry is recovering from a costly and ineffective attachment to the idea – threatens to undermine good practice in the design and acquisition of systems.

For example, in 1.5 we see:

> Multiple applications. Smart cards may carry multiple applications which may, in principle, be added or removed during the card's lifecycle. This can considerably aid the business case for the introduction of card technology, since a single card can be used for multiple functions by multiple organisations.

In other words, weak business cases may be bolstered by claims of possible synergy with other applications that have similarly weak cases and which may never even come into existence. This repeats a mistake commonly made in the 1960's and 1970's, when weak cases for computerisation of particular administrative functions were justified by saying 'once we have a departmental mainframe we can computerise all sorts of other stuff'. This argument led to enough wasteful projects; but the current argument for multifunction smartcards is even flakier. Its analogy in 1960's terms would be: 'OK, we can't justify computerising this system, but once we have a mainframe we can rent out time on it, or so we hear, so let's just go ahead anyway'.

Casting the analogy in these terms should make the problem clearer. Many government departments would not dream of selling time-sharing services on their mainframes, for perfectly valid security reasons. Why should they sell space on their smartcards? And even if a project can only be justified by cost-sharing with the private sector, a clear business plan - with realistic marketing targets and revenue models - should be an absolute requirement.

3 Historical Background

Smartcards, like videoconferencing and wearable computers, have for at least a generation been marketed as the ‘coming revolution’. Their advocates constantly assure us that the exponential take-off in sales is just around the corner, and that generous government funding – in all forms from research grants to preferential purchasing – is the magic catalyst required to open up a cornucopia of technological, political, social and economic delights.

In fact, smartcard technology is so old that the fundamental patents of Moreno and others have now long since expired.

Smartcards have carved out some interesting and valuable niches, most notably in the subscriber identity module (SIM) cards used to personalise GSM digital mobile phones, and in the subscriber cards similarly used to control subscription to pay-per-view TV set-top boxes. Simple memory cards are used in pay phones, and smartcard chips repackaged as physical keys are used in prepayment electricity meters.

However, over the quarter century in which the smartcard has been the subject of intense marketing activity, it has signally failed to gain global acceptance in many markets for which an engineer might think it suited – such as including car and burglar alarms, building access control, transport ticketing, automatic teller machines and computer logon. It has had mixed success in a number of standalone applications ranging from store loyalty cards through membership cards for leisure activities to internal corporate applications such as catering and the control of photocopiers. A prudent civil servant will ask why this technology keeps falling short of its advertised potential.

In one country where the government has subsidised the smartcard deeply and pushed it vigorously – France – it has achieved slightly higher penetration. For example, all ATMs and point-of-sale devices accept smartcards. But the commercial benefits have been questionable as magnetic stripe cards must still be supported to cater for overseas tourists, and the hoped for reduction in fraud has been disappointing. Spain achieved a better result by the simpler strategy of imposing a zero floor limit, so absolutely all credit card transactions must be verified online. (Indeed, as ‘always-on’ DSL Internet connections become the norm and as new-generation mobile networks come on stream, the benefits of offline authentication will disappear in many sectors and for many applications.)

Yet for about the last twelve years, the smartcard industry has kept on pushing the line that ‘multifunction’ or ‘multiapplication’ smartcards are the future. Rather than having twenty cards in his pocket – bank cards, store cards, work ID cards, photocopier cards, an AA card, a phone card, ... the citizen will have one card on which all these applications can be loaded.

It is extraordinary that such a sustained marketing effort should have been made, firstly in the absence of any notable success and secondly as one would expect it to be in the card industry's interests for each citizen to have twenty cards in their pocket rather than two. But at the technical end it has been used as a justification for developing ever faster, more complex and more expensive smartcard chips while the marketing people have been following the argument found in the CCTA report – namely that even if you cannot make a business case for adopting smartcards, you can always hope to make the sale by pointing to a future revenue stream from 'renting space' on the card to the next victim.

4 What will go wrong

In the experience of the industry, there are many good reasons why these supposed gains will turn out to be illusory. Some of these are highlighted by implication in section 2.2 of the CCTA's report, such as:

1. differing target markets. Combining a bank card, for example, with a prepayment electricity meter card is pointless if the bank customers are precisely those worthy of credit while the prepayment customers are the rest;
2. service level responsibility. If a card has both banking and prepayment meter functions, then will the bank have to operate a 24 hour service in case a breakdown leaves a home dialysis patient without electricity? And who will get sued when things go wrong and someone dies?
3. card cancellation. If the credit card becomes a de facto passport, then will litigation leave the customer stranded in the Sudan, or will emigration force her to get another bank? If military ID and crypto key management are combined with bank card functions (as in Singapore) then will card capture by an ATM pose a threat to military security? How about its use in a shop owned by a foreign national? NATO countries at least used to forbid valuables and classified information from being carried in the same container; the reasons for such policies should not be forgotten.

To these must be added a large number of other issues such as:

4. if a card is shared by two or more organisations, whose logo will go on the front? (At the first academic conference where these issues were discussed, Cardis 94, this was the main objection raised by Philippe Maes, a director of Gemplus)
5. if a card combines the functions of several applications, then how can the customer be sure which application is running at the moment? (this has been the main issue to emerge from German multifunction trials)
6. how does one prevent the many technical attacks that are facilitated by multiple applications, such as power analysis and chosen protocol attacks? None

of the current generation of smartcards is secure against a power analysis attack carried out by a malicious terminal; and smartcard security researchers have raised a whole host of other serious questions in this vein.

7. there are even simpler, direct attacks springing from the lack of a trusted path between the user and the card. For example, a personal signature card which is also used to sign credit card transactions is vulnerable to an attacker who presents a point of sale terminal to the user which purports to perform a genuine transaction but actually signs another transaction that is seriously to the user's detriment – this might range from a credit card transaction for a large amount up to a remortgage on her house.
8. different applications involve different user behaviour. For example, it is common to hand one's credit card to the waiter in a restaurant in order for a credit slip to be printed out at the till and brought back for signature (even though the banks quietly advise against this, for fear of additional transactions being booked). One would be very reluctant, though, to do this with a card that was also a passport. At the other end of the scale, it is common for people to share low-value cards such as phone cards, copier cards, canteen cards and the like – even with relatively casual acquaintances. If multifunction cards were introduced, we have no idea how social protocols would evolve to deal with them, and how this adaptation might help or undermine a given business or government function.
9. even if the multiple applications are all within the same administrative domain – such as a company or a university – then how do you prevent the introduction of cards being used as a means of centralising activities that would more rationally be decentralised? An example is a proposal to unify the administration of 100+ libraries, 50+ building access control schemes and 50+ catering operations in a UK university. On closer examination, this turned out to be a bid for power by the centre against existing decentralised ways of working, and likely to impose significant costs for little perceptible benefit.
10. the concept of naming is a surprisingly difficult one in distributed systems. Imposing a single concept of naming (the distinguished name in an X.509 certificate) will bring all sorts of problems. For example, some smartcard schemes deliberately use a new pseudonym for each user, rather than (say) the corporate payroll number or patient NHS number, so that specific requirements for anonymity can be dealt with. Even where such requirements are not explicit, there are many protections implicit in existing ways of working, and whose removal can cause serious harm. One case that comes to mind is when a bank moved from indexing its customers by account number to indexing them by name and address, and sent a man's mistress's bank statements to his wife, leading to a divorce. A few publicised incidents of this kind can completely undermine public confidence in a system – and lead to massive claims for damages.
11. cards cause data to be centralised. For example, trials of healthcare smartcards in both Germany and Canada showed a consistent tendency for medical records to be centralised from the GP's surgery (or equivalent) to the local

health authority or insurer. This is for a number of reasons: the card was not large enough to hold the whole medical record so the rest of it was kept online in a database, keeping the databases in surgeries would have been too expensive, giving doctors equipment to reissue lost or damaged cards would have been too expensive – and of course it was the health authority or insurer to whom the sale was being made.

12. even if 'serious' data protection issues such as medical records can be dealt with, why should citizens have to give their home address and telephone number to a bookshop with which they have just done a credit card transaction? Junk mail may be considered less serious than breaches of medical privacy, but it upsets many more people.
13. physical robustness. About 1% of cards fail in service each year, mostly because of static but also from mechanical stress. Failure rates are higher among manual workers because of the greater exposure to both types of hazard. And if cards are used intensively, failure rates climb sharply; most cards are designed for bank card type use (a few transactions a week) but we know of a pilot in which cards were used some twenty times a day for building and computer access – which raised failure rates to 7% per annum.
14. the technical assumptions in the document are likely to turn out to be wrong. For decades there has been conflict between computer company standards and phone company standards; governments have usually backed the latter (e.g., X.400) while the former (such as SMTP) have prevailed in the marketplace. (In one notorious case, government preference for X.400 delayed the NHS network by about five years.) So the CCTA should be more cautious about taking a stand on particular standards than it is in this document (e.g., with X.509). It would be more prudent just to let departments adopt whichever commercial off the shelf technologies are available and suitable.
15. There are also human scale issues. Whichever sort of card you use, it is dangerous to become dependent on the same small object for very many purposes – you could in very serious difficulty if you lose it.

There are probably two minimum requirements for multiple applications to be considered. A proposed system which does not meet them should be scrapped as being too poorly thought out:

- The card issuer must accept legal responsibility for any consequences of functions interfering with each other.
- It should be possible in extremis to revoke the card by physically taking it from the holder without getting sued on account of unwarranted deprivation of functions other than the one being revoked. So it must never be necessary to cancel one function or authority separately from the others.

For a single application on which multiple systems rely, such as the non-driving driver's licence example, there is a further requirement:

- the card issuer must be able to disavow liability for people relying on the data when it is false (which governments can do with ID cards; you can't sue them if you rely on a false passport and come unstuck).

Of course, if the issuer cannot be sued, then this may raise doubts about the quality of the token and about the motivation of the card issuer to ensure that it is difficult to tamper with.

Consideration of these minimum criteria suggests that there will be few circumstances in which sharing a public sector card with a private sector application will be viable.

5 Conclusion

There are many reasons why multifunction smartcards are a bad idea, except in limited applications such as GSM SIM cards where the lack of an alternative forces them to be considered, and where user control of the terminal removes many of the technical threats. (Even here the commercial success of the concept has been notable by its absence.)

If multifunction tokens lie in our future, then the lack of a user interface alone means that the smartcard is not the right choice for the job. We already have two functioning multifunction tokens - the mobile phone and the PC – soon to be joined by the TV set-top box. Some of these devices may have smartcards in them. However, focussing on the smartcard is the wrong level of abstraction. Firstly, the real driver is the Internet, not a particular component technology; and secondly, the next user token might be the palm pilot, or the e-book, and might not have a card at all. In the medium term, tamper-resistance might come to be provided by the Intel main processor line, or by an embedded microcontroller (as in Firewire), or by software. This is the sort of thing government can't control and is foolish to try to anticipate.

Indeed, the government's track record in 'picking winners' among the plethora of available information technologies and standards lends support to the contarian view. The proposed endorsement of the multifunction smartcard may be taken by the digerati as welcome and timely proof that it has finally breathed its last.

Note

Finally, we wish to register a strong complaint about the procedural aspects of this consultation. We were made aware of this exercise by CCTA on the 12th November, the business day preceding the 15th November which is the deadline for submissions, and even this notification was the result of a chance meeting. It is said that the consultation has been open since the 1st November. In any case, for consultation to be limited to two weeks (even when well advertised) contravenes Cabinet Office guidelines. Furthermore, the web site allegedly containing the definitive version of the document was defective on the 12th November when the consultation was brought to our notice.

Reference

'Framework for Smart Card Use in Government', Alan Collier, CCTA, 1/11/99;
`http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/cardnonsense.txt`