Are we Smart about Security?

Keith Mayes, Konstantinos Markantonakis,
Smart card Centre,
Information Security Group,
Royal Holloway, University of London
Egham, Surrey, TW20 9NU

The introduction of new technologies and changes in behaviours has resulted in an erosion of personal contact and greater reliance on security systems and safeguards. The proliferation of independent security measures has generated an increasing amount of security information that must be stored and recalled by the consumer. Overall security can then be weakened as the consumer is inexpert at managing such data and really needs an integrated high security solution that is also easy to use. The Multi-application Smart Card offers a promising solution, however we may need to challenge some existing practices if we are to empower the Citizen in the on-line world.

1. Introduction

The world has never been a particularly secure or safe place and the early years of the 21st century appear to be no exception. As in previous centuries, many of the problems are inherent in the Human Race, however today we are also faced with insecurity caused by the introduction of new technologies and behaviours.

A lack of security can be combated by a security measure or control and as problems have arisen various ad-hoc countermeasures have been designed and deployed. However the increasingly complexity of the problems requires equally sophisticated solutions and we need to consider a more integrated end-to-end approach.

Many current examples of security measures have similarities and often relate to managing proven identities with associated sets of permissible activities. Each measure when considered in isolation may provide a robust means to increase security, however the fact that the problems are considered piecemeal, means that the proliferation of security measures and policies threatens to undermine their effectiveness.

A smart security approach is required, which would lay solid foundations for a whole range of integrated measures including personal, physical, national and information security.

2. Who can you trust?

The internet, mobile communications and advances in technology mean that our interaction with other people and organisations is changing. More and more businesses and official agencies are becoming “on-line” or accessible via automated telephone services. Whilst this change can certainly bring consumer benefits, it is usually associated with an erosion of personal contact. For example the trusted bank manager in the high street, may be replaced by an “on-line banking team” situated in some distant location.

When you click on the “buy” button for that new car, you can’t see if the salesman looks honest, you can’t be sure that the showroom web site isn’t hiding a crash repair business, you can’t even be sure that the car will be delivered once you pay your money.

With fears arising from reduced personal contact, the on-line consumer may look for well-known names and brands, however in the electronic age we have seen that brand presence is sometimes no more than an illusion created by a Fraudster with a cut and pasted logo bitmap.

As old-style judgement factors such as personal impressions, behavioural clues and trust are eroded, the consumer must have mechanisms to deal with entities that are not automatically regarded as trustworthy. It therefore becomes necessary to place increasing reliance on security systems and processes.

Most consumers would not be able to assess the quality of a security system so their participation in the on-line world is rather a gamble. It may be no more of a gamble than other day-to-day activities but because it is new, it is regarded with more caution and suspicion. When system security has proved itself to be normal, safe and as simple as presenting a passport or opening a door with a key, then it will become more widely accepted. Until that time we have two classes of consumer, those that shun the new technology and those that embrace it.

3. A Consumer for the Modern Age

Consider a modern day consumer that embraces the on-line mobile lifestyle. Such an individual may have equipped himself with the tools for the 21st century. These may include a laptop for business use, perhaps a desk top computer at home, a mobile phone, plus modems and ISP connections.

Figure 1 - A Consumer for the Modern Age

He can use these tools to access the growing range of on-line services that are meant to make his life more convenient and efficient. These services are certainly expected to be secure, but the emphasis is on ease of use which must extend to dealing with associated security procedures.

In short we should strive towards both ease-of-use and high security, two goals which in the past have contradicted each other.

3.1. Basic Equipment/Service Security

Before the consumer can do anything useful with his array of equipment he may have to navigate past a range of security precautions- each of which is basically trying to establish some confidence in the consumer's identity.

3.1.1. Boot Protection

Laptops which hold sensitive information often have encrypted file systems such that a secure code must be entered before the machine is allowed to boot-up. The consumer is proving his authority to access the information and the control employed is being allowed to use the computer hardware.

3.1.2. Operating System log-on

Having negotiated past the Boot Protection, the consumer is normally prompted for a password from the operating system e.g. to log on to Windows. The consumer is proving that he is allowed to use a system and may have some pre-established private account.

3.1.3. Email/ISP Log-on

Access to the email system or ISP often requires a further username and password. Here the consumer is identifying himself to yet another system(s) where he has a pre-established identity/account

3.1.4. Remote Log-on

There are often special precautions for consumers that remotely dial into company IT systems requiring additional log-in names/password. This is similar to operating system log-on, however there are greater precautions due to a perceived higher security risk associated with weaker physical security or the use of non-secured bearers.

3.1.5. In summary

In the example scenario our consumer may have been challenged 4 times, simply to achieve a very basic level of access. If we assumed for example that all these measures were in use on a Laptop and say 2 each on a home and mobile device then we have amassed 8 security challenges. If each challenge required an 8 byte consumer name and 8 byte password, we have 128 bytes of security information to store and recall, before we even start to consider new on-line services.

3.2. On-Line Service Security

The modern consumer is encouraged to use his on-line connectivity to access a range of services. For example, On-Line banking is increasingly popular, along with booking travel and the management of utilities and communication services.

3.2.1. Banking

Increasingly banks are departing from the High Street and offering incentives for consumers to use on-line and telephone banking. Clearly there are cost reduction opportunities for the Banks but also consumer advantages from new services which give more visibility and control over finances.

It is not unusual for a consumer to have a debit card and a couple of credit cards from a variety of Issuers. One particular bank issues a 12 digit consumer ID for each card and requires for on-line access a further 5 digit pass code and an 8 character memorable phrase. Therefore each on-line card is associated with 25 bytes of security related information and a consumer may have say 75 bytes for his set of cards.

Not forgetting that each card must still be used in the “real-world” and will have its own number e.g. 16 digits plus a 4 digit PIN for ATM or EFTPOS transactions. There is also the 3 digit code on the reverse of the cards as further proof of identity, bringing us to a further 23 bytes per card.

It is therefore quite easy to amass almost 150 bytes for a small set of banking cards.

We should also remember that one side-effect of on-line access is that it is relatively simple for a consumer to have multiple on-line bank accounts and so the number of bytes could easily be increased.

3.2.2. Travel

Booking travel via the internet can be fast and cost effective with services offering discounts for on-line reservations.
Some sites offer consumer registration linked to loyalty schemes intended to retain consumers and simplify the booking procedure.
One airline site offers access via a 8 digit membership ID plus a 4 digit pass code. This information is then sufficient to book flights using stored loyalty points. The Electronic tickets that are issued allow check-in at the airport without presentation of a passport as this information is indirectly available, being bound to the membership ID in the airlines database.
If you use 2 such air-lines then you can have 24 bytes of security info to remember and you will have trusted your passport and other personal details to the unknown security and privacy policies of commercial databases

3.2.3. Access

Even physical security can add to our store of bytes. It is quite common for organisations to have electronic access control systems. A 4-6 byte pin-code challenge may be issued to an employee several times during the working day. Even card based systems can be complemented by PINs as many cards are lost.
Hidden behind the issue of an access enabler may be a whole host of employee information, including role number, location, grade, dept, length of service, security clearance level etc.

3.2.4. Communication/Utilities

Checking your home phone bill or configuring account functionality are useful on-line features. To do this a consumer may be challenged for an account number, plus a username and password. If we say 8 digits for each then we need 24 digits of information. Apply this to your mobile phone account and we may have another 24 digits. Add in your gas and electricity accounts and you are approaching 100 digits of information.

3.2.5. Citizenship Information

We must not forget that things of value, which include pins and passwords for service access, are often obtained only after presenting additional identification. This can be regarded as citizen information and may include your name, age, address, nationality, employer, national insurance number, signature, mothers maiden name, passport number, driving licence, bank address, current account number, fixed/mobile phone number sort code etc…
Interestingly if you search through this list you find only 2 fundamental pieces of identity information, or biometrics, which are the signature and passport photo. As neither of these is commonly used for on-line transactions our service providers are heavily reliant on a range of derived citizen information and therefore the organisations and processes that were used to produce it.

The on-line identity information can be considered as an expansion of the Citizen Information which is built up over a life-time, largely from the repeated presentation of the same biometrics i.e. your signature and facial appearance.

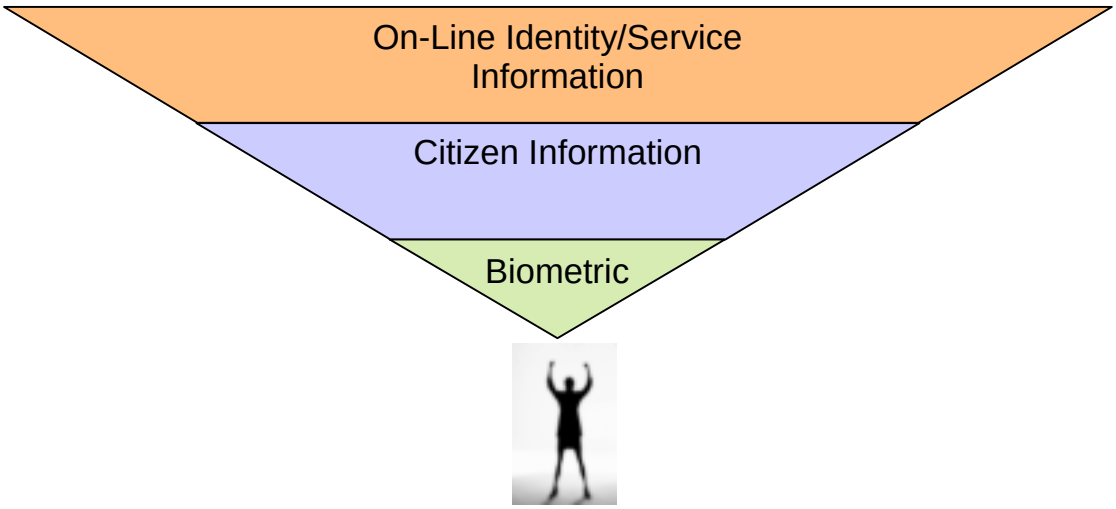

Figure 2 - The role of Citizen Information

3.3. Observation

The simple examples above serve only to illustrate that a relatively small set of useful and properly designed services can require the storage and recall of a significant amount (~400+ bytes) of security related information.
However we know from the mobile world that a major drain on Customer Care Services arises from consumers that have forgotten simple PIN codes. These codes are only 4 digits/bytes long, so how can consumers manage a hundred times this information?

4. Consumer Strategies for Handling Security Information

There may be individuals that can memorise large amounts of security data, however they are certainly not in the majority. So what strategies do consumers use to cope?

4.1. Re-use the same information

If all the systems and services used the same format for username and password then in theory you could set all services to use the same fields. Whilst there is some scope for this, largely it is either not possible or prevented. User names vary considerably. They can be parts of a real name, telephone numbers, email addresses, alphanumeric IDs and generally the consumer is unable to change them.

The Consumer may sometimes duplicate Passwords, but there are variations in character length, case sensitivity and permitted alphanumerics.

Attempts to re-use passwords are often frustrated by individual service security policies that cause them to expire at asynchronous times.

Furthermore the small print conditions for some services tell you not to use the same passwords or secrets for any other service

4.2. Use a Wallet

It is common practice for people to carry around a physical wallet or a purse. The wallet usually contains bank cards and hence some of the security information. The wallet affords a level of physical security that is under the owner's control.

Although discouraged, PIN codes are often written onto pieces of paper and despite all the sound advice to the contrary some of these papers will be found in the wallet alongside the cards.

Some providers of on-line services provide a card to remind you how to access their service. These are often the same dimension as a credit card and so it is natural that these end up in the wallet. We then have the temptation to add the log-in details into the wallet and perhaps just written on the card.

Now if the physical security breaks down and the wallet is lost or stolen then clearly there are big problems, however the wallet is usually regarded as a safe place by the consumer, as he only has to trust himself to manage it.

4.3. Store it on the PC

The on-line services are often accessed by the PC so you could store the security information on the computer. This could take the form of a simple readable file. The more cautious may try to protect it, at least with a password, which is only a little better providing of course that the password can be remembered. (Perhaps it ends up in the wallet again or on a slip of paper near the PC).

Some applications offer to memorise login information which means that your secret info is permanently stored on the machine and perhaps you do not need to respond to any further challenges for the computer to log on as you. This is a problem if your computer is not protected by physical security and also as the computer is on-line you are reliant on information security measures (if any) and it may be possible for others to read this information. Anyone who has installed a personal firewall on their PC will know that attempts at unauthorised access are a day-to-day reality.

4.4. Use a Personal Digital Assistant (PDA)

With 400+ bytes of security data we have an information management problem. Storage of significant amounts of useful personal data is often accomplished with a PDA. The security information will often be stored alongside and with no better protection, than phone numbers diaries, dictionaries and family birthdays.
PDAs accompany the Modern consumer in his mobile life, from place to place and computer to computer. Because of this they become an essential accessory acting like a sponge for important information and representing a snapshot of the consumers personal and business life. Anyone who has ever lost or damaged a PDA will appreciate the extent and true value of this stored information.
The PDA has physical security rather like the wallet and may have the option of a simple PIN code or login protection, although this is sometimes disabled by the consumer.

With all this valuable information stored on a PDA the consumer would be wise to carry out periodic back-ups. A consumer who would never dream of having a secrets file on his PC may well back-up his PDA onto the same machine. A consumer's life can then be laid bare with little more than a normal file viewer.

This could be overcome to some extent by backing up to a flash memory which can be locked away or alternatively to a secure off-line PC.

However PDAs are evolving and are increasingly becoming on-line devices either via GPRS modems or Bluetooth link to other wireless communicators. Or indeed the wireless communicator has become the PDA and is becoming an equivalent to the PC. As we move towards downloadable applications on communicators there is no reason why the device should not increasingly become a target for hacking attempts and viruses.

Perhaps one of the important features of the PDA has been lost, as it is no longer a standalone container for personal information. This is unfortunate as although it required some manual activity i.e. reading and typing, the PDA also helped the consumer negotiate through the various security challenges that were encountered.

5. So where is a safe place?

If the PDA is no longer a safe place for security information where can we put it? What we need is a container for say a few kilobytes of storage that will not give up its contents to unauthorised applications and systems regardless of whether it is connected to a communication system or standalone. The loss of the container should not allow unauthorised consumers to access its content even when deploying aggressive attack methods. Resistance to such attacks implies a hardware solution, which should be small and lightweight to support mobile use and inexpensive to encourage widespread deployment.
We also need some means to recover our security information if the container is lost or damaged.
Perhaps surprisingly our modern age consumer almost certainly has such a device and probably 3 or 4, but then perhaps that's the problem.

6. Smart Cards

Everyone that owns a GSM mobile phone has a Smart Card [2] and so we have over a billion around the world.
It is called a SIM which stands for Subscriber identity Module and whilst removable from the mobile telephone it is usually hidden away out of sight and largely forgotten. It was originally designed to ensure that only authorised subscribers could use the GSM network [1]. Because of cloning problems associated with earlier Analog networks, the SIM was necessary as a Hardware Security Module which would resist not only logical attacks but side channel and Physical attacks too[5].
The card has been very successful in this role. It is true that the COMP128-1 authentication was broken and such cards were at risk of cloning, but this was attributable to the inherent weakness of the algorithm and not to any failing of the Smart Card platform as a hardware security module.
The same can not be said for hardware security solutions attempted in the mobile phone, which in at least one case were circumvented by replacing a small integrated circuit.

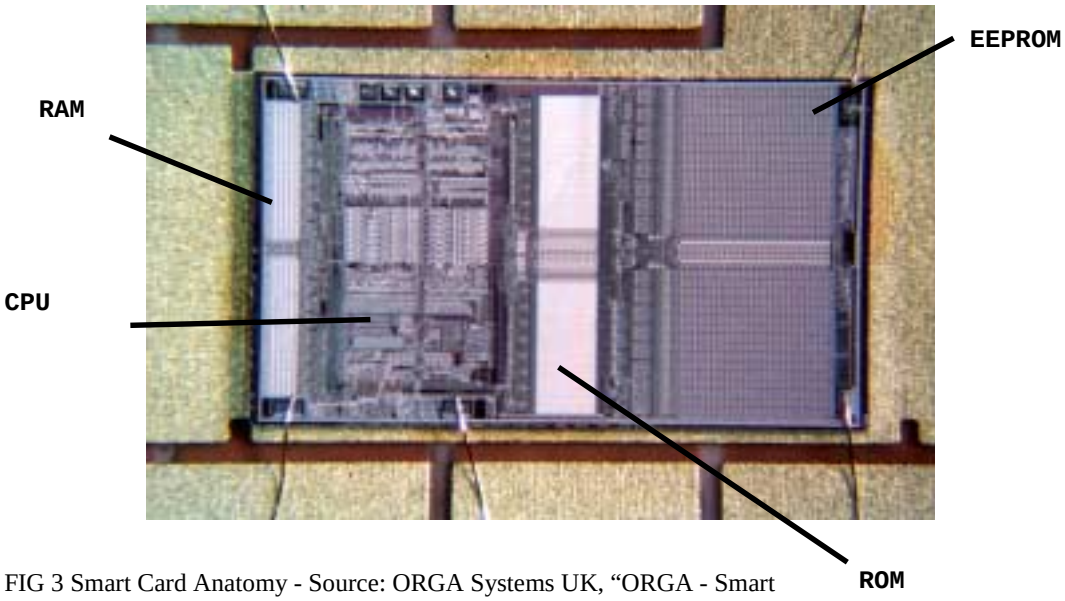

FIG 3 Smart Card Anatomy - Source: ORGA Systems UK, “ORGA - Smart Cards Basics”

The essential components of the Smart Card chip are shown in Fig 3 above. To store security information we need to make use of the non-volatile but re-writable EEROM memory. Typical cards today have 32kbytes of EEROM which should be quite sufficient for GSM as well as some added application or security information. More application packed cards can use 64k products and 512k cards are quite possible with today’s technologies.

The card is logically robust and communicates via well defined and standardised interfaces [3, 4]. File access and permissions are also well defined along with PINs and management procedures that prevent trial and error attempts to discover the values.

Furthermore the ICs are expertly designed to resist sophisticated attacks such as power analysis and physical probing.

These features are certainly not restricted to the SIM and you will probably find some more Smart Cards in your wallet. The gold coloured contacts on your credit and debit cards tell you there should be a smart card chip inside. These cards need be no less powerful than their SIM relations and may be designed to higher standards of security. The primary advantage of the SIM is that it comes in a device with a user interface, in-built card reader and communications capability. Whilst there have been some attempts to incorporate a second card reader into mobile terminals these have had limited support, largely one suspects because the network operators wish to defend their control of the value chain.

Aside from mobile network operators and banks, the impressive credentials of Smart Cards are also well known to the government and a forum has been established to promote exploitation of this technology [7]. Given this level of interest and support, we might wonder why Smart Cards aren't already used to underpin a much wider range of security solutions.

7. The Problem with Cards

There is a fundamental difference between a PDA and a Smart Card. It is not the obvious physical features such as MMI, memory or processing power but rather the question of ownership.
The PDA is “Personal” and it tends to be bought and owned by the consumer (or perhaps his company). If it is helpful for the consumer to use it for shopping lists, games and contact lists as well as passwords, then that is his choice.
The Smart Card is generally not bought or owned by the consumer. It is given, or more precisely, loaned to the consumer by an organisation such as a Network Operator or Bank.
The Issuing organisation has made an investment to provide the card and does so for commercial advantage.

7.1. Card proliferation

The issuing organisation chooses the type of card and the applications and data that are issued with it. Furthermore cards can be managed in the field with file updates and application downloads being possible. The management needs of course to be secure and relies on keys that are known to the card and the Issuer.
The management key is very important, as without co-operation of the holder it is impossible to modify the card.
Bearing in mind that the most common function of the card is to establish identity then there is significant synergy between applications, however card ownership, management, branding, standards and business competition issues hinder the full use of a card which supports multiple organisations. Therefore we have a proliferation of cards and a bulging wallet in which to keep them.

7.2. Space to Rent?

Leaving aside the proliferation of cards perhaps it would be possible to just build our mini PDA into one of the existing cards. You could choose any card but most of them need a reader. The reader for the bank cards is usually an ATM or EFTPOS terminal and it is not that common for a consumer to have a card reader attached to his PC. The obvious choice is the SIM card as it always sits within a reader that is equipped with display and keyboard i.e. the mobile phone.
The functionality to store and recall security information is not overly complex and a simple SIM Toolkit solution could be readily implemented. So why is this not widespread?
One important reason relates to storage, as any function on the card uses memory. The memory on the card is limited and it relates to its cost. The spare memory is therefore precious to the Issuer who would want to use it for commercial advantage e.g. a new service that generates revenues. Now a mini PDA may be great for the consumer but where is the benefit for the Issuer? The information stored may have nothing to do with the Issuer and may even be safeguarding competitor details. The Issuer might get a more tangible benefit by buying smaller cards so there is no spare memory.

7.3. Consumer Control

Perhaps the first big step towards a more open approach, is for the consumer to own a Smart Card. That way the contents will be present for the consumer's advantage and not for the commercial benefit of an Issuing organisation. Unfortunately, this adds to the proliferation of Smart Cards but you could argue that this may ultimately be the primary card on which bank or communication applications are hosted.

In the first instance it is likely that this would be a standalone card and so would need a reader and as we have observed there are not many consumers that have card readers.

7.4. Form Factors

When the consumer buys a standalone Smart Card it challenges a lot of pre-conceived ideas. Firstly do we really mean a physical card? Certainly we need the Smart Card functionality and attributes but it doesn't have to be the same as the Cards we have today. Banking cards conform to standards that mean they fit into ATM and EFTPOS machines. For SIM cards the plug-in is important so that it can fit into phones.

So the consumer should look for a form factor that is convenient, which could be a card, or perhaps a USB key or even a Bluetooth token.

8. Multi-Application Citizen Card

The foregoing observations and arguments can lead towards a vision of a personalised security solution. It is based on Smart Card functionality put may be flexible in terms of form factor. A key point is that it is a Citizen Card i.e. it is owned by a Citizen and contains as a minimum some Citizen information of the type that is used to prove identity and permit access in the “real-world”. This information is available for on-line use but represents a small part of the Cards capability. The second key attribute is that the card is Multi-Application and can be used to host a range of independent services. The Citizen Card can be a passport, driving licence but also a credit card, a transport ticket as well as an access key for a wide range of system and physical access solutions.

The Issuing process for such Citizen cards may be different to banking and SIM cards and will require confidence in the identity and integrity of the manufactured device and the mechanisms ensuring its secure linkage to the consumer. One possible scheme [6] considers the use of device certificates that are created during card manufacture. The certificates can be used to authenticate and manage the device prior to the eventual association with a registered consumer.

9. Eggs, Baskets and Redundancy

Having proposed an integrated, Citizen and card centric solution we should not leave the subject without giving some thought to effects on redundancy and resilience.
If all your security information is held in one device and you reduce the number of authentication methods, then you may be accused of “putting all your eggs in one basket”. It might be argued that the proliferation of systems, challenges and security information gives the benefit of added redundancy. Whilst this may be partly true, the redundancy offered may be regarded as almost accidental and not designed/optimised to combat a particular problem.
Consider the analogy of transmitting an image over a radio channel. A digitized image contains a great deal of redundancy and to transmit this over a radio bearer would normally not be desirable due to the time/radio resources required. Fortunately an image may be greatly compressed prior to transmission. As the image is transmitted it is “attacked” by the fading radio environment which will cause errors. Not surprisingly the compressed image is unlikely to arrive successfully; however neither is the raw image. This is because the inherent redundancy is not appropriate to combat the “attack”. The optimal approach is to reduce the source information and then add in the necessary minimum redundancy to cope with the channel.

For the Citizen Card solution we should therefore design the common integrated solution that meets our requirements and then consciously add in the appropriate redundancy and support systems to cope with perceived risks and problems.

10. Concluding Remarks

We have observed how new technologies and behaviours have resulted in an erosion of personal contact and greater reliance on security systems and safeguards. The proliferation of independent security measures has resulted in a growing amount of security information that must be stored and recalled by the consumer. Overall security can then be weakened as the consumer is not expert at managing this data and really needs an integrated high security solution that is also easy to use.

The basic technology to support a more integrated, optimised security framework exists today and is even ubiquitous in the form of SIM and Banking Smart Cards. However, diverse issues around card ownership and the form factor of cards and tokens have hindered the arrival of the Multi-Application solution.
A Citizen Centric approach is a potential solution that should be researched further. The idea being to expand the role of a Citizen Card or Token as a consumer owned secure platform for access to a wide range of services

[The Multi-Application Citizen Card is being considered as a research topic within the Smart Card Centre of the Royal Holloway University of London and contacts are invited from interested parties within government and industry]

11. References

[1] GSM & UMTS – The Creation of Global Mobile Communication – Wiley 2002
[2] W. Rankl and W. Effing – Smart card handbook 2nd edition John Wiley 1997
[3] ISO 7816-x Integrated circuit cards with contacts. ISO Geneva Switzerland.
[4] ETSI TS 100 977 (GSM 11.11) ETSI Sophia Antipolis France
[5] Advances in Smartcard Security - Mark Witterman - Information Security Bulletin July 2002
[6] UK patent application GB 2365264 Mayes, Bone & Walker published 13.02.2002
[7] Smart Government Forum www.smartgovforum.com

Keith Mayes (B.Sc. (Bath) Ph.D. (Bath) CEng MIEE) received his BSc (Hons) in Electronic Engineering in 1983 from the University of Bath, and his PhD degree in Digital Image Processing in 1987. During his first degree he was employed by Pye TVT (Philips) which designed and produced TV broadcast and studio equipment. His PhD was sponsored by Honeywell Aerospace and Defence and on completion he accepted their offer of a job. In 1988 he started work for Racal Research where he worked on a wide range of research and advanced development products and was accepted as a Chartered Engineer. In 1995 he joined Racal Messenger to continue work on a Vehicle Licence plate recognition system (Talon) and an early packet radio system (Widanet/Paknet). In 1996 Keith joined Vodafone as a Senior Manager working within the Communication Security and Advanced Development group, under Professor Michael Walker. Early work concerned advanced radio relaying systems and involved participation in international standardisation. Later he led the Maths & Modelling team and eventually took charge of the Fraud & Security group. During this time he was training in intellectual property and licensing, culminating in membership of the Licensing Executives Society and the added responsibility for patent issues in Vodafone UK. In 2000, following some work on m-commerce and an increasing interest in Smart Cards he joined the Vodafone International organisation as the Vodafone Global SIM Card Manager, responsible for SIM card harmonisation and strategy for the Vodafone Group. In 2002, Keith left Vodafone to set up his own Telecoms Consulting Company (Crisp Telecom) and in November 2002 he also started as the Director of the Smart Card Centre at RHUL.

Konstantinos Markantonakis (B.Sc. (Lancaster University), M.Sc., Ph.D. (London)) received his BSc (Hons) in Computer Science from Lancaster University in 1995, his MSc in Information Security in 1996 and his PhD in 2000 both from Royal Holloway, University of London. His main areas of interest are smart card security and smart card applications along with security protocol design. Since completing his PhD, he has worked as an independent consultant in a number of information security and smart card related projects . He has worked as a Multi-application smart card Manager in Visa International EU, responsible for multi-application smart card technology for southern Europe. More recently, he was working as a Senior Consultant in Steer Davies Gleave (a transport consultancy company) responsible for advising transport operators and financial institutions on the use of smart card technology. He is also a member of the IFIP Working Group 8.8 on Smart Cards. He is currently a member of the Information Security Group, as a Lecturer in the Smart card Centre. He continues to act as a consultant on a

variety of topics around smart card security, smart card migration program planning/project management for financial institutions and transport operators.