Smart cards in health

Dr Jim Briggs

Dr Roger Beresford

Healthcare Computing Group, University of Portsmouth, Portsmouth, PO1 3AE

Executive summary

This report considers the technical features of smart cards and how they affect the way in which smart cards might be used in the health sector. This is an important issue since the government has highlighted smart cards as a likely means of improving patients' access to the NHS. We seek to contribute to the debate by undertaking a review of the technology and predicting technical development of smart cards over the next ten years, and relating those developments to technologically based scenarios for the use of smart cards in healthcare.

Section 2 discusses briefly the technology of smart cards, drawing distinctions between memory and microprocessor cards and between contact and contactless methods of reading them. The development of new memory technologies is also touched upon. Section 3 discusses whether Moore's Law (that the complexity of silicon chips appears to double every 18 months) applies to smart cards.

Section 4 takes some particular aspects of the technology and addresses the implications of developments in these areas on the usefulness of smart cards. The aspects addressed are the memory capacity of a card, its speed of reading and writing, the range at which it can be read or written, the card's lifetime, and its resistance to unauthorised access. We also make an observation concerning the availability of cards.

Section 5 covers issues from an orthogonal viewpoint, discussing how smart cards might be used in the health sector and some of the issues arising from those uses. The scenarios addressed include holding medical records on a card, using the card as a patient identification token, issues specific to prescription management, smart tagging and patient monitoring.

Our conclusions are that smart cards provide a practical means of facilitating many of the information flows necessary for the maintenance of good health and the efficient delivery of care. The technology already exists to undertake many of the currently foreseen applications, though much work needs to be done on integration. Where the technology does not currently exist, Moore's Law allows anticipation that in the future it may do so.

Contents

1 Introduction

The NHS Plan[1], published in July 2000, sets the goal of using smart cards to provide easier access for patients to health records. According to the plan, they will be introduced "when the necessary infrastructure has been put in place and we have fully evaluated technical feasibility and effectiveness."

What does "provide easier access for patients to health records" mean? To what other uses in the health sector could smart cards be put? What other applications of smart technology are relevant?

In this report we aim to contribute to the answering of these questions by undertaking a review of the technology and predicting technical development of smart cards over the next ten years, and relating those developments to technologically based scenarios for the use of smart cards in healthcare.

2 The technology of smart cards

The role that smart cards can play in the healthcare sector is obviously constrained by the technical capabilities that are available at any point in time. In this part of the report, we first of all describe the basic features that distinguish the various types of smart card, before going on to consider how some of the capabilities of smart cards and other smart devices might be predicted based on lessons learned from the development of other, similar technologies.

2.1 Kinds of smart card

There are two kinds of smart card: memory cards and microprocessor cards.

Memory cards simply store data and can be thought of as a small floppy disk. Data can be written on the card over and over again, overwriting existing data.

A microprocessor card, on the other hand, can add, delete and manipulate information in its memory on the card. It can be thought of as a tiny computer and contains a processor with an operating system that supports input and output (read and write) facilities and memory. The thing that makes the card smart is the ability to load the processor with a program that supports the desired application or applications.

The size of the card (the conventional "credit card" size) is determined by international standard ISO 7810[2]. A separate standard (ISO 7816[3]) defines the physical characteristics of the plastic, including the temperature range and flexibility, position of the electrical contacts and how the microchip communicates with the outside world.

2.2 Reading the card

Smart cards fall into two categories according to how they can be read from and written to: contact cards and contactless cards[4].

Contact smart cards must be inserted into a smart card reader. They have a small gold plate about ½" in diameter on the front, instead of a magnetic strip on the back like a credit card. When the card is inserted into a smart card reader, it makes contact with electrical connectors that transfer data to and from the chip.

Contactless smart cards need to be passed near an antenna to carry out a transaction. They look just like plastic credit cards, except that they have an electronic microchip and an antenna embedded inside. These components allow the card to communicate with an antenna/coupler unit without any physical contact. Contactless cards are useful in situations

where transactions must be processed very quickly and there isn't time to bring the card into physical contact with a reader.

Contactless cards either carry their own battery power supply or derive their power from the radio signal from the reader. Of course, a contactless card has fewer restrictions on such things as size and shape than a contact card, since it does not have to fit on or plug in to anything. This means that other forms of contactless device can be used – one in particular being the RFID (radio frequency ID) tag that can be attached to an object in various ways.

2.3 Card memory technology

Most current smart cards use EEPROM (electronically erasable programmable read-only memory). EEPROM can be erased by exposing it to an electrical charge. Like other types of PROM, EEPROM retains its contents even when the power is turned off. However, like other types of ROM, accessing data in EEPROM is not as fast as RAM.

Flash memory is a special type of EEPROM that can be erased and reprogrammed in blocks instead of one byte at a time. The principal difference is that EEPROM requires data to be written or erased one byte at a time whereas flash memory allows data to be written or erased in blocks. This makes flash memory faster to access.

EEPROM and flash memory are both silicon-based technologies. An alternative is FRAM (sometimes written as FeRAM) – ferroelectric random-access memory. Despite their name, FRAMs do not contain any iron; rather they are ceramic crystals that take on a positive or negative polarity when set by an electrical charge. They have been around for a long time, but it is only in the last 20 years or so that the problem of early fatigue (losing data) has been solved[5]. Their advantage over EEPROM and flash memory is low power-usage and fast access times – comparable to conventional computer DRAM (dynamic random access memory) – while retaining data when the power is turned off (unlike DRAM).

A further technology currently under development is MRAM (magnetic random-access memory). This is under development by IBM[6] and is scheduled for the mass market in 2003 or 2004. Its advantages are that it is even faster to access than DRAM and, like FRAM, retains its contents when the power is turned off. It is not possible at this stage to accurately assess its operational properties, such as its power supply requirements for reading and writing, nor its lifetime. We are not aware of any plans yet to construct a smart card using it, but it must be considered a likely application of the new technology.

The following table (Table 1) summarises the main technical features of the different sorts of memory:

	EEPROM	**Flash memory**	**FRAM**	**DRAM**	**MRAM**
Speed of access	Slow	Medium	Fast	Fast	Very fast
Volatility (what happens when power is switched off)	Retains data	Retains data	Retains data	Erases data	Retains data
Power needed to write	High	High	Low	High	Low(?)
Number of write operations before wearing out	Low ($\sim 10^5$)	Low	High ($\sim 10^{10}$)	High	High(?)

	EEPROM	Flash memory	FRAM	DRAM	MRAM
Density of memory capacity	Low	Low	High	High	Very high

Table 1 - Features of memory technologies

3 Moore's Law

3.1 Background

Moore's Law is named after Gordon E. Moore, one of the founders of Intel, the computer chip manufacturer. In 1965, when he was director of R&D for Fairchild Semiconductor, while preparing an article[7], he started to graph data about the growth in memory chip performance, and began to realise that there was a striking trend. Each new chip contained roughly twice as much capacity as its predecessor, and each chip was released within a year or two of the previous chip. If this trend continued, he reasoned, computing power would rise exponentially over relatively brief periods of time[8]. Remarkably, his prediction has proved to be reasonably accurate over the 36 intervening years.

Originally his prediction applied to the number of transistors per square inch on integrated circuits. One of his Intel colleagues generalised it from the complexity of the chips to the performance of computers[9]. Since then, other authors have used the term "Moore's Law" as a label for any computer-related development that improves at an exponential rate.

Moore's original prediction was that the doubling occurred every year, but in the mid-1970s he revised that to every two years. However, because you not only get a benefit from the doubling of density every two years but clock frequencies increase too, so computer performance could be said to double every 18 months. Doubling every 18 months is the generally accepted and quoted rate.

Many observers have expressed the view that Moore's Law cannot continue forever. Moore himself believes that it will only hold for the next 15-20 years. Limits arising from the fundamental size of atoms will come into play in that time frame, making it impossible to reduce the size of things further with existing technologies. However, other developments may well keep the pace of progress increasing.

Moore's Law is sometimes quoted in terms of cost in relation to performance. If, for example, one bought a processor with a certain speed of operation (expressed in instructions per second, say) for a certain price, 18 months later one would be able to buy one that performed twice as many instructions per second, for the same price. If one bought a memory with a certain capacity, 18 months later memories with twice the capacity would be available for the same price. An alternative expression of Moore's Law is to say that in 18 months, one would only need to spend half the amount of money to purchase a device with the capability of one that could be bought now.

Figure 1 below shows a graph of Moore's Law, illustrating how complexity rises over time (starting at 1).

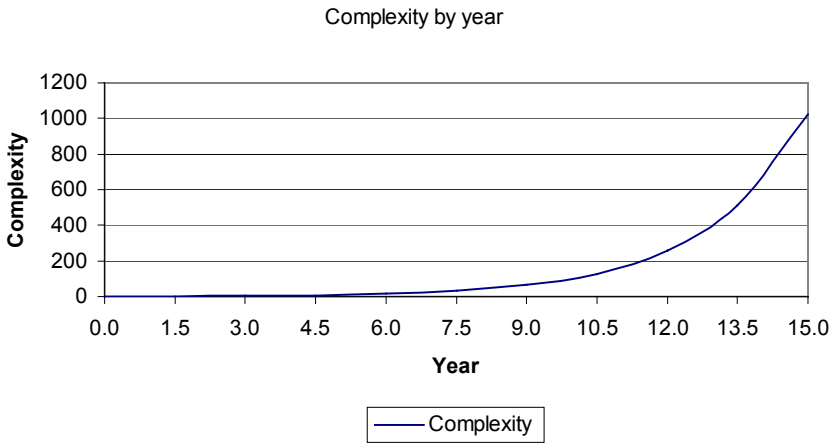

Figure 1 - Moore's Law: Rising Complexity

As can be seen from the graph, under Moore's Law a thousand-fold increase can be achieved in about 15 years.

Figure 2 is exactly the same, except that the complexity is plotted on logarithmic scale.

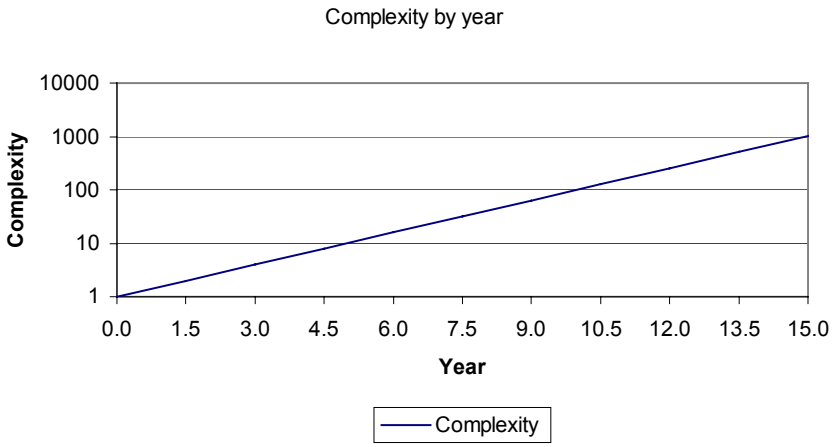

Figure 2 - Moore's Law: Rising Complexity (logarithmic scale)

Figure 3 is a third example of the same process, but this time expressed as falling cost rather than rising complexity.

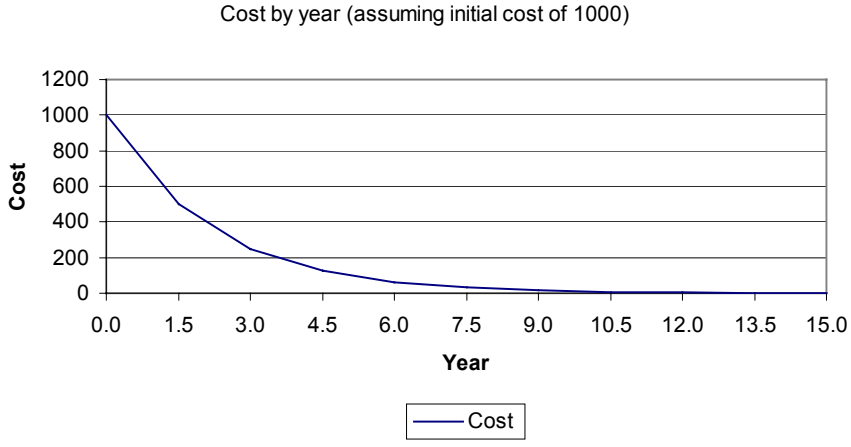

Figure 3 - Moore's Law: Falling Cost

3.2 Application to smart cards

Does Moore's Law apply to smart cards? As far as we know, no formal study has been carried out to test the hypothesis. However, tentative conclusions can be drawn from anecdotal evidence.

In 1990, the memory capacity of a state of the art smart card was 8Kbits. In 1995 it was 16Kbits. In 2000 it was 32Kbits. It is clearly unsafe to draw too much from only three data points, but these do suggest that Moore's Law does not apply, since under it we would expect an increase of somewhere between 64-fold and 128-fold in that time. An alternative hypothesis would be that there is exponential growth, but that the period to double performance is of the order of five years, rather than 18 months. This would suggest that 64Kbit cards will be available within the next 5 years and 128Kbit cards within 10 years.

However, the figures above relate only to EEPROM cards. The current capacity of an FRAM card is 4Mbits (512Kbytes) – a significant improvement. Using that figure as a data point, and assuming that growth has been exponential over a 10-year period, we can see a rate of growth approximately in line with Moore's Law. If that is the case, we can extrapolate to predict 32Mbit or perhaps 64Mbit FRAM cards in 5 years time, and 256Mbit or 512Mbit cards in about 10 years.

One may argue that comparing FRAM cards with EEPROM cards is like comparing chalk with cheese, and is inappropriate. But our response to that would be that the growth of computer capability was not restricted to one technology, and that periodic shifts in the technology used are an essential requirement in order to sustain growth over a long period.

4 Implications of smart card technology to healthcare

The discussion above has centred on memory capacity of a smart card, but this is not the only technical factor that is improving. In this section, we consider memory capacity and other technical factors, and discuss their relevance to the possible adoption of smart cards in healthcare.

4.1 Memory capacity

The capacity of a card is the major determining factor in limiting the information that can be stored on it. While it is possible to store less than the maximum capacity of the card, it is obviously never possible to store more.

A few kilobytes of capacity are generally accepted as being sufficient to store basic identification details (e.g. name of holder, identifying number(s)) and, in the healthcare context, domain-specific but generally applicable information such as details of allergies, medication and other emergency data.

Where the smart card is being used as a key to unlock an access control mechanism, encryption keys large enough to resist extensive brute force attempts to break them can also be stored.

Episode specific data could also be designed to fit into a few kilobytes. Examples of this might be details of one or a few prescriptions, information about appointments, etc.

However, the limits of capacity are rapidly reached when one talks about the sort of information that would constitute a patient's medical history over an extended period of time, or a shorter period of time with multiple or severe conditions. In particular, X-ray or similar medical images stored with sufficient resolution and colour depth to be useful, typically occupy at least 8-16Kbytes (64-128Kbits) of memory, even with suitable compression[10].

The space required to hold just one image exceeds the capacity of the latest EEPROM cards. FRAM cards could be considered for this purpose, but even then the number of images that could be stored is limited.

4.2 Read/write speed

The speed at which a card can be read from or written to is clearly important in some applications (though not necessarily so in all).

The read/write speed places a lower limit on the time within which the smart card must be in contact with or, for contactless cards, in the vicinity of the reading or writing device. This in turn limits the speed at which a smart card can pass a detector while in motion. Once the read/write time is down to some suitable insignificant (to a human) fraction of a second, further developments will normally be imperceptible.

Current contactless cards have a typical communication speed of up to 100Kbits/sec, which means an entire 32Kbit EEPROM card could be written in less than a second. We predict that communication speeds will increase in line with developments in other wireless technologies.

4.3 Read/write range

The range at which a contactless card can be read from or written to is also important. The range places an upper limit on the distance that the card can be from its terminal – the device that is reading from or writing to it.

The sorts of distances that might be involved can be categorised according to their order of magnitude as follows:

touching – within a millimetre
very close contact – within a centimetre
fairly close contact – within 10 centimetres
same room – within a metre or two
same building – within 10 metres or so
same neighbourhood – within 100 metres or so
same district – within 1 kilometre
same city – within 10 kilometres
same region – within 100 kilometres
same country – within 1000 kilometres
same continent – within 10,000 kilometres
and so on

Smart cards already exist that can operate at the scale of fairly close contact or same room. The issue with expanding the range is that of introducing unwanted effects. There is a story (possibly apocryphal) of a smart card used as a bus fare token. Not only did the reader on board the bus deduct the fare from the cards carried by passengers who boarded, but also from those who were left standing at the stop because the bus was full! This illustrates that small range has its advantages since it requires the user to make the conscious effort to bring the card into the proximity of the reader.

Devices that can operate within a district or city are already available – they are called mobile phones. There are trade offs to be made in the development of smart cards between the size of the card (especially insofar as it affects the length of aerial and capacity of power supply that it can carry) and the range it can operate over, but we believe these are not make or break considerations in most envisaged applications.

4.4 Lifetime

There are three factors that together contribute to measuring the lifetime of a card. This section addresses these in turn.

4.4.1 Number of read and write operations

The lifetime of a card relates mainly to the number of read and write operations that can be applied to it before it wears out and is incapable of holding or releasing data any longer.

Current EEPROM and flash memory cards are capable of the order of 100,000 operations. This is increasing steadily but not spectacularly. Spectacular improvements can be achieved by switching to FRAM where the lifetime is 10,000 times longer.

The following graph (Figure 4) shows the lifetime of both types of card (in years) according to the number of operations per day performed on it:

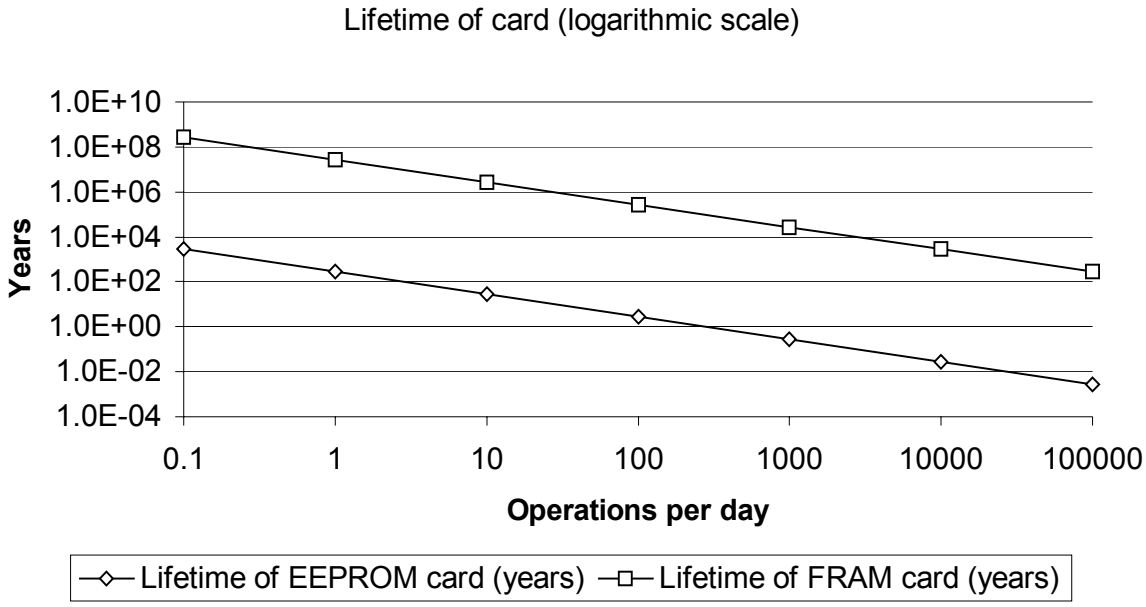

Figure 4 - Lifetime of a card

Current credit cards are expected are expected by their issuers to have an operational lifetime of a few years[1]. This is consistent with the EEPROM line above, if one expects a customer to use the card on the order of once per day. That an FRAM card used with similar frequency will last several million years probably means that adequate capability is already available for similar applications. Alternatively, a lifetime of over 100 years can be achieved even with 100,000 operations per day (more than one per second).

4.4.2 Data retention

Without performing any operations, how long will a card hold its information? Data retention in both EEPROM and FRAM is a function of temperature – the warmer the card the shorter the period of time it will hold its information. Current cards have a non-volatile data retention lifetime of the order of 10 years at 85°C. However, cooler temperatures provide much longer lifetimes. One FRAM manufacturer's figures show that keeping the card at room temperature may give a retention period of more than 5000 years![11]

[1] This is one of the reasons why they have an expiry date and are re-issued to customers.

However, data retention in an FRAM memory has an additional supportive feature. When the system performs a read operation on a FRAM, the internal memory array actually performs a read and restore. Therefore, a read is effectively a write. In conventional terms, data retention is measured from the last write operation. Therefore, each read operation restarts the retention interval. Since the retention intervals are measured in years, it is possible to achieve virtually any required data retention simply by periodically reading the entire memory.

4.4.3 Physical durability

The other factor affecting the lifetime of a card is its physical durability. This means the amount of wear and tear the card physically suffers as a result of being carried and used normally, and its resistance to damage through being bent, crushed or exposed to extremes of temperature.

The current international standard for card durability is ISO 10373[12]. It specifies that cards must be able to withstand 250 bending cycles per side and 500 torsion cycles, as well as being resistant to alcohol, fuel and sweat, and to operate within a range of temperatures from -20°C to +50°C. It would seem a reasonable expectation that future cards will have higher standards of durability. Perhaps the telling factor here will be the development of new plastic materials to surround the "smart" part of the card. However, even the most indestructible of materials is still prone to being lost down the back of a cushion or falling through a grating.

4.5 Resistance to unauthorised access

It is obviously desirable that smart cards are resistant to having their data or programming erased or modified by unauthorised persons or equipment. This is normally achieved by locks implemented by password control – terminals are only granted the desired access if they provide the correct read or write password (and these can be different).

Passwords (and associated rights) are usually identified for the manufacturer, fabricator (the organisation that incorporates the smart device into the plastic card, say), issuer and user of a card. A first stage threat is for new cards to be stolen from the manufacturer before the issuer initialises them. The stolen card can then be made into a pirate card by a variety of means. The manufacturer therefore programs in a password that is specific to the fabricator. After fabrication and testing, the fabricator replaces the manufacturer password with one specific to the issuer. The issuer can then use this to unlock the card and set passwords to its own requirements, including, normally:

- an application key that is specific to the use to which the card is put, and which is the information that needs to be known by all authorised terminal devices; and
- an issuer key that allows the issuer to override various settings

As long as the passwords or PIN numbers associated with a card are kept safe and not revealed, this level of security is usually enough. The state of the art involves the implementation in the card of what is known as an attack counter. This is used to count the number of unsuccessful attempts to gain access and is reset to zero when the correct password is provided. If the counter reaches a predetermined limit (suggesting that someone is trying to guess the password), the card is locked and all access is denied. Where appropriate this can either lock the card forever, or until the appropriate issuer key is used to reset the attack counter and unlock the card. In many respects, the resistance of a smart card to unauthorised access is similar to the tamper proofing of a car's engine immobiliser. Lessons learned by the motor industry might usefully be applied to card security.

However, smart cards have a vulnerability that is not shared by many other crypto-systems. Because it is relatively easy for a card to be stolen, a thief or hacker can have the benefit of

privacy to make their attempts to break into it. Thus the security of a card in this regard is not the same as, for example, an ATM machine that is solidly encased in the wall of a building, or even an immobilised car, which are difficult to transport or conceal. The ability to test the card in private opens it up to brute force attacks (where every possible permutation of code is attempted), but this is relatively easy to defend against using attack counters. However, it also opens it up to so-called "physical side-channel" attacks, where observations of the power consumption and time taken to do cryptographic operations are used to uncover their details[13].

Because so many of the potential uses of smart cards are concerned with secure information, it is tempting to forget that the security of the card itself is only part of the whole picture. One needs to remember that there are threats to the security of data contained on a card if a card reader terminal is itself tampered with, so appropriate security measures must be taken to defend these. The security of any system in which a smart card is a part is dependent on the security of all parts of the system.

4.6 Availability

A significant but much overlooked factor in considering smart cards is their availability. The demand for cards by the mobile phone industry over the past few years has been phenomenal and manufacturers are struggling to meet that demand. One undesirable corollary to Moore's Law is Rock's Law[14] – the cost of building production facilities for high-tech products doubles every four years.

We have heard that it is the case that anyone ordering a large number of cards for a new smart card application should not be surprised to have to wait two years before receiving their stock.

5 Healthcare scenarios

In this section, we look at some of the possible applications to which smart cards could be put in the healthcare sector, and discuss some of the technical and other implications of each.

5.1 Emergency medical data recording

5.1.1 Background

In many circumstances, patients are admitted to hospitals in a condition unfit to communicate vital medical details. Emergency medical data on a smart card could be used to speed treatment, especially in paramedic situations where full data access to a hospital system is less likely. A photo on the card provides a double check for identification purposes.

Some small trials have been undertaken, such as the EMR Medicard trial in Gloucestershire[15], but abandoned due to poor take-up. The benefits to the individual have not been perceived as sufficiently great to prompt people to use the smart card and the benefits to the NHS have not been sufficiently compelling to prompt the NHS to pursue it.

5.1.2 Benefits to the individual

What benefits might there be to the card carrier? Health benefits to an individual are tied to the availability of the resources to read and use the smart card data in whatever location the individual chances into an unplanned interaction with the medical emergency services. As with any of the eCash experiments (e.g. the Mondex trials at the University of Aston or the town of Swindon[16]), ubiquity of reading equipment is a requirement.

Empowerment of the general public is only going to be relevant if the data held is "sensible" to the holder, both in terms of the language used and the means of presentation, as well as in terms of any personal use the individual could make of the data.

Summaries of medical history may, for example, be helpful in dealing with insurance companies, who for cost reasons try to avoid formal contact with the GP unless the data reported by the individual raises questions. This is clearly not a major requirement, but possibly illustrative of usefulness. Vaccinations are another area where patients might appreciate access to their medical data – foreign travel has widened the range of specific immunisations that are deemed desirable and few people can accurately remember what jabs or similar they have had.

A smart card might be a convenient means of carrying this kind of personally accessible medical data, but presupposes that the patient would have the means of reading the card's contents. There are two major issues to address under this scenario: the security of the card's data and the availability of suitable readers. The security issues are well covered in relation to the various eCash experiments (Mondex et al), but access to a suitable reader poses a more difficult issue. The eCash experiments have relied on the provision of ATM-like card charging points and investment in card readers by retailers. Where the economic incentive to provide a range of medical smart card readers lies is difficult to see. The value to retail organisations like Sainsbury's of installing smart card readers for public access in their stores is tied to their value in gathering marketing intelligence – feedback to the general public is a minor additional fixed cost that saves on staff time. Unless ubiquitous smart card readers become sufficiently generic to offer a range of functions in such circumstances, or perhaps be tied through sponsorship to specific retailers card schemes (c.f. the Boots Advantage card and the organ donor scheme), then the direct public empowerment benefit is difficult to generate.

5.1.3 Benefits to healthcare professionals

Emergency medical data vital to staff might include the patient's HIV or Hepatitis status. Being able to extract this kind of information from otherwise unknown patients admitted to hospital might help protect medical staff. Protection of this potentially "difficult" information as encrypted smart card data may be more acceptable to the public than a more open coding scheme based on eye-readable medical data.

Patient history may need to include information on the "completion rate" of previous courses of treatment. How this data might be collected is of course a different and difficult question, but it would inform the staff, particularly for a mobile patient base not calling at the same clinic for many consecutive sessions.

5.1.4 Added value from multifunction cards

The volume of data to be stored on a card is not really a critical issue, as only summaries of current status, drug regime, allergic responses, etc. might be required. If the smart card can have other purposes that encourage or require it to be carried, then the health benefits are an bonus and not the raison d'être and thus more likely to be widely adopted. Multifunction smart cards would be required in this context, with the "other" application offering the inducement value to the user. Protection of the medical data from corruption or access by the other application can be assured by the smart card operating system, e.g. MULTOS which has an ITSEC E6 High security certification[17].

It may well be that the smart card could be part of a mobile phone, thus confering a number of other more obvious benefits. The use of the phone itself as part of an identity token has not yet been widly considered, though they are now being used to enable a value exchange, e.g to

buy a coke from a vending machine! The advantage of the phone in this context is that it has a user interface, i.e. the keypad and screen. Thus applications that are added to the smart card embedded in the phone (currently for identification and payment) can be rendered visible to the user. A conventional smart card cannot of itself communicate with the user, requiring insertion into a terminal (for a contact card) or into the vicinity of one (for a contactless card). The use of the phone as the reading device makes access by the general public a possibility without the need for widespread introduction of reading stations.

5.1.5 Full medical records/history

The need for a full portable medical record on a long term development of a smart card seems significantly at variance with much of the current development work in a wide variety of non-medical environments. It would seem likely that the pace of development of network technologies and associate data distribution systems would for the foreseeable future keep ahead of the data density possible in a portable smart card.

The use of a smart card as an access token and protected crypto engine to networked data seems more viable. This does of course assume that there is agreement as to data model standards for the different levels of an individual's interaction with healthcare services and that there is agreement as to what data a patient and their professionals should have access to.

There would seem to be very little benefit to the individual in carrying about a copy of the full medical record, when in the majority of instances the network infrastructure could deliver it to the relevant medical staff over a network. The assumption that the full record would be assembled into a single location, even given a fully implemented network environment is not certain. In circumstances where network access is difficult due to infrastructure problems, the facilities to read and make use of a full medical record on a smart card are also likely to be absent. The probability of loss/damage of card at a critical point would further militate against this scenario.

5.2 Patient identification services

5.2.1 Relationship to a national identity card

Smart cards need to have a justification and benefit evident to the individual, otherwise the negative connotations of a mandatory national identity card will present political difficulties. The introduction of smart cards for tracking "customer loyalty" is paid for in discounts, air miles, etc. The benefits to the card issuers are usually not made public and masked by a marketing play on the potential monetary gain to the individual. In the context of a health service smart card, the benefits to the individual are not as easily identified. In fact, there may seem to be little that could be offered as an inducement in a health service context other than the rather nebulous potential improvement in the system as a whole.

Another factor of import is the management process for issue to patients. In current practice, this might be the responsibility of the individual's health authority, or could just as possible be part of the process of registering with a GP. An alternative would be to issue cards from some national agency (as is currently done with driving licences). In each of these cases, the provision of a secure mechanism for loading the relevant applications and data on to the card would need to be established. One possible implementation of this is to employ a cascade of different stations: the first level installs the healthcare and any other application software; subsequently the more individual functions and data relevant to the eventual end user of the card are added. Provision for this process to be undertaken in stages is implicit in the current design of money bearing smart cards, where the physical and data security of the partly set-up

cards is managed via the distribution channel from manufacturer through fabricator to issuer and user.

5.2.2 Secure key into networked data

The use of a smart card as a repository of encryption keys and access tokens is perhaps the most likely in the near future. This means that the smart card does not itself contain the important data, rather it holds the keys and access tokens necessary to read or write encrypted data that is itself retrieved or transmitted over a network (e.g. the Internet).

The technical limitations with such a system lie in the speed of any crypto processing that needs to be done by the (relatively slow) processor on the card itself. This problem will undoubtedly diminish as card processors get faster (in line with Moore's Law?). In the meantime, it can be avoided if the key is read into a more powerful computer for it to do the encryption/decryption, but this may introduce its own security hazards if that machine is not itself secure. Some computer workstations are now available with a smart card reader built in to them or as an attached peripheral[18,19], and we envisage their availability and use will increase.

The public are experienced with the use of security tokens to access bank ATMs, albeit with only minimal data held on a magnetic stripe. The extension of this type of identity key to include qualified access to individual medical records presupposes a perceived benefit to the individual in such access.

5.3 Prescription management

Drug prescribing is an area where a smart card could offer potential benefits to the holder (patient or patient's guardian) in the form of better care and reduced administration. These include:

- If the smart card contains details of all the prescriptions issued to a patient, then possible drug interaction effects might be more easily spotted. At present this is difficult to do if a patient goes to a different pharmacy for each prescription. The implementation of this is dependent on the memory capacity of the card being sufficient for the necessary information.
- A smart card might provide a secure means of carrying an electronic prescription from the doctor to the pharmacy. This would be an advantage over systems where the patient has to designate the pharmacy to which the prescription is to be sent at the time the prescription is written.
- A smart card might provide a secure and reliable means of identifying patients who are entitled to free prescriptions.
- Another area where the security features of the smart card could be advantageous would be in the management of drug addicts. A secure record of the drug substitutes prescribed could be of considerable value. The mobile nature of this group of patients would again be perhaps well served by a personally carried smart card. The benefit to the patient being the assured supply from a variety of locations without the delays that might be required for checking through normal channels.

5.4 Smart tagging

5.4.1 Smart labels for pathology test samples

A machine-readable label for pathology test samples is already fairly well established, using bar codes and other optically read equivalents. The current systems have the benefits of economy and simplicity, but offer only limited identity tagging.

Replacing the barcode or handwritten label with a smart tag would permit more data to be included in the order, and provides the potential for an automatic system to add the results of the test directly to the tag. The benefit of a smart tag is its physical attachment to the sample it relates to; whether the data needs to be included on the tag, or merely used to identify the sample with the data being captured and carried via a network, in which case the value of it diminishes. This presupposes that a network is not a more likely solution within a hospital environment.

The possibility of the smart tag playing an active part in the process does pose some interesting questions. The time the sample was taken is often a critical feature in many of the laboratory investigative processes. The potential for this to be bound into the results may well be helpful. One could also envisage, using current technology, a smart tag raising an alert via a nearby sensor if its test was urgent or overdue, or if the sample was tampered with.

5.4.2 Inventory tagging

Much inventory is manually recorded, with larger organisations using bar codes to identify resources. The combination of eye-readable numeric identity codes and machine-readable equivalents is a cost effective and reasonably reliable inventory control system.

A contactless smart tag with inventory details encoded might be a valuable aid in identifying equipment that is moved on a regular basis. Benefits here could include logging usage with a view to managed maintenance, logging where and when and by whom it was used, and theft detection if it was removed from its intended usage zone. This presupposes a potentially wide scale implementation of sensors/reading stations at all entry and exit points. With the development of mobile data-aware devices, the provision of this infrastructure might not be as expensive or special purpose as it would be at the current time.

5.4.3 Building entry control

A smart card used to identify patients and staff could be used as part of either building security, or for access to controlled resources, anything from special diet kitchens to automatic drug dispensing systems. The use of contactless smart card badges has been trialed for the purpose of staff tracking in Cambridge University research labs.

5.5 Patient monitoring

5.5.1 Mobile lifestyle monitoring

With wide scale adoption of smart cards, their use in collecting and securing many sensor readings could be relevant. There are currently many portable recording media, Audio Mini Discs being a current example. Whether a refined smart card would be preferable depends amongst other reasons on the ubiquity of the medium.

Music distribution is currently largely via compact discs, with Internet distribution being fought over in the courts. If the music industry can migrate to an Internet distribution model where portable MP3 players can be "charged" from a periodic Internet link, then the habit may well be exploitable in the context of portable smart card based data capture devices

being used to upload data via the Internet. There would be a range of alternative structures that might be employed in place of the smart card format, yet retain the equivalent functionality for this purpose.

The value of smart cards for collecting this data could be said to reside in the security potential and resistance to tampering. There are a range of other devices that might be able to record the data, for example the memory cards now used in digital cameras commonly have capacities in excess of 16 MB (with 256MB now possible), in a package comparable to a smart card, but with no security features.

Another feature currently not present in smart cards is that of a visible user interface. The user has to take on trust that the smart card is performing as expected and has not been compromised (in terms of its security features) and is only performing its intended medical function. The binding of the smart card into an equally tamperproof management device with a user interface might alleviate this problem. A mobile phone is perhaps the most common example, with significant development of user interface functionality expected. The value of a user interface for confirming the encryption features explicitly has been set out in a commercial context[20]. The balance between a networked future and the collection of long term personal data on removable cards remains a moot point.

5.5.2 Hospital monitoring

The use of smart cards within a hospital environment, whist technically feasible, is less likely in view of the likely ease of internal networked access. This may be wireless in the future, but will probably mean conventional wired networks for at least the next few years, due to the potential for interference effects with the wide range of electronic medical equipment.

As discussed above, it is likely that any mobile monitoring of patients may well be enhanced by capture to a smart card, but the range of options available in a fixed and managed hospital environment remain significant. The use of Bluetooth enabled devices, now that the standard is reasonably stable and real devices are obtainable, may be significant so long as the possibility of any interaction between the Bluetooth devices and other medical electronics can be eliminated. However, potential problems have been highlighted by a number of sources[21,22].

5.5.3 Embedded monitoring

Contactless smart card technology, or a more specialised derivative, may well permit the embedding of the monitor and sensors in the patient. To what extent a smart card component would be required, useful or even possible is currently an open question. Were smart cards to achieve a significant role in the provision of healthcare, then this additional element may be worth developing. The use of Bluetooth chips may well be used to pass the monitoring data to an external device, which may of course also involve a smart card for security or data-retention services[23]. However, embedded monitoring would seem unlikely to be the first application area in healthcare for smart cards.

5.5.4 Episode recording

Here the presumption is that patients would be given a smart card for the duration of a particular episode of care. There may be health benefits by involving the patient actively in both the gathering of data and the management of the care involved.

The integration of the resulting dataset into the hospital maintained electronic patient record would be a separate process not involving the patient.

6 Conclusions

The current state of smart card technology, combined with the new developments in memory technology that are on the horizon, allow us to conclude that smart cards are a practical means of providing many of the services that are required in the health sector. In many respects, such as the speed of transferring data to and from the card, the technology is already sufficient for currently proposed applications. In others, such as memory capacity, new technological developments, modelled by Moore's Law, promise to deliver improved performance in the foreseeable future.

Smart cards can be used both as a means of information storage and for information flow from one place to another. At least in the short term, the small capacity of cards compared to the rapid speed of networks suggests that most data will be stored centrally. Instead the smart card will be used to facilitate its retrieval and security by providing a physical token that can be used as part of an access mechanism.

References

[1] Department of Health. The NHS Plan: a plan for investment; a plan for reform. 2000; Cm 4818-I.

[2] International Standards Organisation. ISO/IEC 7810:1995 Identification cards - Physical characteristics. 1995.

[3] International Standards Organisation. ISO/IEC 7816 Identification cards - Integrated circuit(s) cards with contacts. 1994-2000.

[4] Gemplus SA. All about smart cards [Web Page]. 10 October 2000; Available at http://www.gemplus.com/basics/what.htm.

[5] Neil Weinberg. A computer in every shirt collar? Forbes Magazine, 8 March 1999.

[6] IBM, Infineon Technologies AG. IBM, Infineon to Advance Revolutionary Memory Technology [Web Page]. 7 December 2000; Available at http://www.ibm.com/Press/prnews.nsf/jan/1F2DF62A9462BF13852569AE00577748.

[7] Gordon E. Moore. Cramming more components onto integrated circuits. Electronics, 19 April 1965; 38(8).

[8] What is Moore's Law? [Web Page]. Available at http://www.intel.com/intel/museum/25anniv/hof/moore.htm. (Accessed 12 March 2001).

[9] Dori Jones Yang. On Moore's Law and fishing [Web Page]. 17 October 2000; Available at http://www.usnews.com/usnews/transcripts/moore.htm.

[10] Alan Lock. The Determination of an Optimal Technical Standard for Minor Injuries Telemedicine. Proc. 3rd Annual Conference of the Southern Institute for Health Informatics. Available at http://www.dis.port.ac.uk/hcc/sihi/sihi2000/proceedings/Lock/index.htm.

[11] Ramtron International Corp. Data Retention Characterization [Web Page]. 12 May 2000; Available at http://www.ramtron.com/products/appnotes/data%20retention%205-00.pdf.

[12] International Standards Organisation. ISO/IEC 10373:1993 Identification cards - Test methods. 1993.

[13] Nigel Smart. Physical side-channel attacks on cryptographic systems. Software Focus, December 2000; 1(2).

[14] Interviews with visionaries: Arthur Rock [Web Page]. Available at http://www.intel.com/intel/museum/25anniv/int/rock.htm. (Accessed 9 April 2001).

[15] Smartcard for high risk patients [Web Page]. 12 December 1999; Available at http://news.bbc.co.uk/hi/english/health/newsid_558000/558438.stm.

[16] Liz Amos, Tony Bell. The Smart Campus Newsletter [Web Page]. October 1999; Available at http://www.aston.ac.uk/smartcard/newsletter/9-newlet.htm.

[17] John Elliott. Free-commerce and MULTOS [Web Page]. 31 March 2000; Available at http://www.consult.hyperion.co.uk/pub/PDFLibrary/Y2000/CFI_CTSTarticle.pdf.

[18] Security Information Management Online Network. Veridicom PC Peripheral To Integrate Smartcard Reader & Fingerprint Sensor Aimed At eBusiness Markets [Web Page]. 12 September 2000; Available at http://www.simon-net.com/pressRelease.asp?ID=3184.

[19] Litronic Inc. Argus 300 Smart Card Reader [Web Page]. 6 December 2000; Available at http://www.litronic.com/solutions/readers/300.html.

[20] D. Balfanz, E.W. Felten. Hand-held Computers can be Better Smart Cards. Proceedings of the 8th USENIX Security Symposium. 1999

[21] C. Akass. Wireless Networking: How we broke the Wi-Fi link. Personal Computer World, April 2001; p. 19.

[22] Roger Howorth, Paul Grant. Early Bluetooth lacks bite [Web Page]. 8 January 2001; Available at http://www.zdnet.co.uk/news/2001/1/ns-20070.html.

[23] Byron Kaye. Bluetooth arrests heart problems [Web Page]. 24 January 2001; Available at http://www.zdnet.co.uk/news/2001/3/ns-20458.html.