Smart Card Tutorial

First Published in April 1998

Smart Card Technology -
Where are we going?

Just a year ago searching the Internet for Smart Cards using a search engine such as Alta Vista would have produced a few tens of hits, today its over 28,000. The era of the Smart Card is truly upon us. The production of Smart Cards has not increased in the same ratio over the last year although no doubt many in the industry would wish it to be so, in fact just listening to some suppliers would convince you its already happened. In reality we are now in a major period of growth and it is time to stop and try and analyse what is happening.

Lets start by looking at the sales of Smart Cards by application sector for the second half of the decade. (TABLE 1) In all years the payphone represents the dominant sector. Why should this be? Do we really believe it will continue? At the end of the day it all comes down to the business case and for the payphone operators this is good business. Handling cash is a messy expensive operation, ask any retailer or bank, in the UK alone it is reckoned to cost £4.5Bn/year. Just the operation of collecting the cash and ensuring serviceability of the equipment is an operational nightmare. The technical function provided by a telephone card is relatively simple and involves a small memory with access control to ensure adequate security. Such chips are only a few square millimetres in size and can be manufactured for less than 25 cents (US). Add to this the revenue that can be produced by the advertising on the card and you can start to see the strength of the business case. The simplicity of a Smart Card reader/writer terminal compared with the relatively complex coin mechanism just adds to the benefits. We see no reason why payphones should die out even in the face of the success of cellular phones which with GSM is a Smart Card success in its own right. Curiously GSM and the payphone represent almost the two extremes of the Smart Card technology. The GSM industry has consistently taxed the available resources of the chip. Four years ago 8K bytes of EEPROM memory was the norm which in those days was a stretching requirement in the usage of the silicon real estate. Today the norm is towards 16K bytes of EEPROM memory.

The biggest difference between the GSM chips and chips for the financial industry relates to security. Financial operators place considerable reliance on the integrity and authentication of the data which forms the basis of a financial payment instrument. When we consider the electronic purse it is clear that the data stored in the chip represents the value of the owners assets. It goes without saying that both parties are concerned about the integrity of this data, an increase in value will upset the bank just as much as a decrease will upset the cardholder.

The business case for replacing the ubiquitous financial magnetic stripe card has been a quest not dissimilar to the search for the Holy Grail. For years many enthusiasts have tried to make the case on the grounds of improved security. Whilst the security of the Smart Card is several orders of magnitude better than its magnetic stripe counterpart, more on this later, the actual savings on preventing counterfeiting do not justify the additional cost. Losses due to lost and stolen cards totally bypass the technology involved.

So why do we believe that Smart Cards will have such an impact in the financial industry? There are two reasons, the first relates to the ability of creating a product that is not viable with magnetic stripe technology. The electronic purse is typical of such a product where it is clear that the highest security must be achieved. The integrity of such an instrument must be no less than that achieved with notes and coins and ideally somewhat better. Few would doubt that the technology of the integrated circuit chip achieves this aim and those in search of perfection should note that it is the security of the system overall that matters, it should not be economically viable to profit by abusing the system.

The greater future in the financial industry for the use of Smart Cards is the ability to have multi application cards. At least 3 are obvious, the credit/debit application, the electronic purse and the loyalty scheme. There is a fourth application which relates to identity and this may yet be shown to dominate. In our table we have

shown the ID card separately but really its just an application that could exist on a suitable multi application card. The need to carry a portable identity token is becoming an increasing commercial requirement and in the world where we are ever more interested in remote transactions it will become a necessity. Just look at the increasing number of companies that are working on such technology.

Year	**1996**	**1997**	**1998**	**1999**	**2000**
Payphones	450	585	60	900	1125
GSM	17	40	60	100	150
Health	75	102	138	185	250
Banking	50	85	146	225	380
ID	6	16	44	140	350
Transport	5	12	30	88	220
TV	22	32	47	60	85
Gaming	5	14	39	140	385
Metering	6	10	18	30	50
Vending	14	27	52	100	200
Total	650	906	1304	1908	3095

Table 1: By Application Sector (Millions of Cards)

No of Cards Issued, in Millions	**Name of Project**	**Application**	**Issuer**	**Country**
78+	German Health Insurance Card	Health	German Health Insurance Companies	Germany
40	GSM	Mobile Telecommunications	Over 208 operators in 105 countries	Worldwide
30 Entire population will receive card by 2000	Sesam / Vitale Card	Health	Ministry of Social Affaires	France
40-50	Geld Carte	Electronic Purse	ZKA (Zentraler Kredit Ausschuss)	Germany
8	Advantage Card	Loyalty	Boots the Chemist	United Kingdom
5 10 by end of 1998	Giropas	Electronic Purse	Postbank	Netherlands
4+	SMART	Loyalty	Shell UK and a Consortium of retailers	United Kingdom
4	Automatic fare Collection- Seoul Bus Card Project	Transport	Seoul Bus Union	South Korea
4	QUICK	Electronic Purse	Europay	Austria
3.7 2 ordered	Hong Kong Mass Transit Project (Octopus)	Transport	Creative Star Ltd	Hong Kong

Table 2: SCN Smart Card Top Ten (March 1998)

The long sought quest of government is likely to be solved by commercial pressure. The interesting thing about an ID card is the underwriting of risk. If such cards are being used to effect value transactions who picks up the pieces when it all goes wrong? This rather fundamental point seems to have escaped the notice of many industry players.

The use of Smart Card for accessing satellite TV programs is well established and apart from GSM and the Boots Advantage card is the only major use of Smart Cards in the U.K. The security of such cards is at a premium since they attract considerable attention from the technology hackers. The psychology seems to suggest that it is fair game to break such systems, a concept which fortunately does not seem to extend in the same way to other walks of life. How much easier it would be to defeat magnetic stripe cards but then they don't offer the same intellectual challenge.

Mass transit is a major development area for contactless Smart Cards. Clearly the volumes could be significant and the relatively low cost of such cards allows them to offer the necessary business case. Perhaps of greater surprise is the move in Japan to promote the use of contactless cards for payphone use, this will certainly concentrate the minds of the producers who will no doubt be severely challenged on the pricing of such cards.

Vending is another significant application class but you might consider it to be nothing more than an application for the electronic purse. Interoperability is the name of the game and one suspects that customers really do not want to carry around large numbers of cards. One might conjecture that a small number of electronic purses will dominate the market for which Visa and Mastercard must be the dominant players.

Gaming is the last of the major application areas identified in the table. There are so many possibilities here ranging from straight gambling to computer type games applications. The depth of imagination is boundless but of one thing we are sure gambling and gaming are basic human characteristics where the portability and security of the Smart Card has a lot to offer. Of course in all such matters it is often something totally new that becomes the dominant factor, that killer application, is it already hidden in these application types or are we all going to be surprised?

Next month: Technology trends continued
David B Everett

Smart Card Tutorial

First Published in May 1998

Smart Card Technology –
Where are we going? Part 2

Last month we looked at what has been happening in the Smart Card world and now we are going to look at what is happening today and our expectations for the future. Included with this article is the latest version of the Smart Card top 10.

We can start by looking at the chips and the moves being made by the major semiconductor manufacturers. Traditionally Smart Card chips have been viewed as a small part of the semiconductor manufacturers revenue and as such they have tended to use the older and cheaper manufacturing technology. We usually discuss the process technically in terms of its minimum features size. The smaller the feature size the more components that can be packed into the same square area of silicon. At the front end of the technology wave manufacturers are working with a feature size of 0.18 microns. Whilst typical Smart Card chips today are 0.8 microns. The newer technologies are applied to the more complex chips such as the Pentium (i.e the PC main processor) or in memory chips where it is desirable to pack as much memory as possible into a single chip. The smaller the chip area the higher the yield that can be obtained in the manufacturing process and although there is no limit on the size of the Smart Card chip due to any popular standard or specification it is generally agreed that on reliability grounds at least that the chip should be less than 25mm2. Many articles on Smart Cards refer to a maximum size of 25mm2 as an ISO impediment, the only consideration relates to the contact plate and the position of the contacts which would limit the size (and aspect ratio) if the chip is placed directly on the back of the connector plate. But of course you do not have to put the chip there and in the case of a contactless card it may be anywhere within the card's natural volume. If for the moment we assume the commonly available 0.8 micron process technology then we would expect to find a typical specification as follows:

- 8 bit CPU
- 24K Bytes ROM
- 8K Bytes E2
- 512 Bytes RAM
- + A cryptographic coprocessor

It is a totally commercial decision as to how semiconductor manufacturers employ their various fabrication lines and what is interesting is the major change in emphasis that has been happening over the last year. Whilst traditionally the Smart Card chips trailed the process line top end by about 2 years they now seem to have taken more of a pole position and we are aware of a number of major manufacturers looking at 0.5 microns and even 0.35 microns for the next generation of Smart Card chips. This of course has a large effect on the possible resources that can be provided on a reasonable size chip (10-20 mm2). So looking on the horizon we might expect to see:

- 32 bit CPU (RISC)
- 64 K Bytes ROM
- 32 K Bytes E2
- 2 K Bytes RAM
- + A Cryptographic Accelerator

We may also expect to see 0.18 micron process technology introduced early in the next decade with yet a further increase in available on chip resources.

Now we might ask ourselves what is behind all this? We can be sure that it is all to do with the business case which optimises the return on investment where the manufacturing fabrication plants costs several billion dollars, to put in place. Two simple factors come into play, volumes and added value per chip. The basic

volume game is dangerous and is subject to the vagaries of the market place. Several manufacturers caught a cold with the DRAM (Dynamic RAM as used in PCs) when the market dropped severely 2 years ago. The added value per chip is far more interesting and this largely accounts for the financial success of Intel who are able to charge 100s of dollars for their new generation chips. So one of the interesting questions here is whether the market can withstand more expensive Smart Card chips. In the finance market it has been traditionally assumed that you are competing with the magnetic stripe card that can be provided for a few cents whilst the GSM market has been able to hide the cost of the SIM (Subscriber identity Module) card as part of the phone handset. If we can justify the business case for the Smart Card on the basis of a small portable multi application computer then the more powerful chips will come to the fore. The enormous interest in the Javacard and Multos multi application cards suggest that many people view this as a major growth area.

We may note with interest that the smaller process technology brings with it lower voltages for which the existing Smart Card infrastructure is ill prepared. Whilst it has been suggested that such chips will need to include a voltage regulator to operate in the current 5V terminals it should be understood that there is a price to pay and one would like to see ISO apply a somewhat greater degree of urgency to such problems.

The other big move on the chip front relates to security. In broad terms this may be broken down into two categories:

- Logical security
- Physical security

The logical security offered by the chip relates to the ability to protect data whilst stored, processed and transmitted. The use of cryptography is fundamental to achieving the desired level of assurance. Physical security relates to the basic chip hardware and its resistance to attack.

Traditionally we hear a lot about cryptography, the various algorithms and their key lengths. Early Smart Card chips predominatly operated with symmetric algorithms such as DES (Data Encryption Standard) but the greater interest today is in the public key algorithm such as RSA (Rivest, Shamir and Adleman) and ECC (Elliptical Curve Cryptosystems). The RSA algorithm is not a practical proposition for an 8 bit CPU running at low clock speeds as used in the Smart Card world. This has resulted in a number of chips being developed that contain a cryptographic co-processor. Five years ago 512 bits were the norm for RSA but today 768 bits and even 1024 bits has become the expected value. It is the move to such long key lengths that has brought about an interest in ECC as the preferred cryptography for Smart Cards. Key sizes of 160 bits in ECC are believed to offer the same cryptographic strength as 1024 bits in RSA. Although bit for bit the ECC algorithm exerts more processing effort there is a significant gain to be achieved if 160 bits is deemed to be an acceptable value. The RSA foothold is however so strong that it seems unlikely that ECC will have any major impact in this decade. Although it is possible at low performance to implement ECC in Smart Cards without an arithmetic co-processor it seems unlikely that this would become common place with the smaller 8 bit processors. The use of 32 bit RISC processors with higher clock speeds may however lead to these principles being challenged.

The physical security of the chips has been presented as a new world of adventure. Rarely do new concepts with no previous basis occur and it is clear that the Smart Card chip can be referenced against a long field of study relating to Tamper Resistant Modules (TRMs). In the first instance we may note the use of tamper resistance, the thoughts of tamper proof can only be a dream. It is the task of the designer to ensure that the work function presented by the chip is fit for purpose. In general we can say that it should not be economically viable to break the chip. We can see immediately that the chip should be considered as part of an overall system and it is the breaking of the system that must be made sufficiently difficult and costly.

Lots of claims have been made about the breaking of Smart Card chips. In reality in those cases where it can be shown that the chip has been made to reveal its security we can show that this was a fault of the system not the particular chip component. Many of the attacks referred to on the Internet and else where refer to chips that are not normally used in Smart Cards and which provide very primitive security features.

Even the current generation of Smart Card chips invokes a number of security features that require high skill levels with sophisticated technology to defeat. The newer breed of chips emerging in the marketplace allows very secure systems to be put in place. As an example we might note that the idea of physically probing the internal bus of 0.18 micron or even 0.35 micron process technology is really impractical. Equally as the memory cells become smaller the number of electrons decreases to the point that is difficult to imagine how any beam imaging technology could succeed.

Assuming a well designed system and that includes the interaction of hardware and software, then we may feel confident that the Smart Card will act as the security kernel of such systems whether for financial applications or other equally important business areas.

The move towards multi application operating systems has become the current in subject. The press is littered with discussions of Java and Multos.

You can determine every concept that these systems compete to the position that they are converging to a common specification. In truth they are different, Javacard relates to a virtual machine very much a subset of the widely used Java architecture. Multos is both a virtual machine designed specifically for the small resources made available by Smart Card chips and an underlying operating system also designed for a Smart Card chip environment. Multos provides a specification for the total life cycle of the card including its initialisation and the loading and deletion of application in a secure fashion.

No of Cards Issued, in Millions	**Name of Project**	**Application**	**Issuer**	**Country**
82 100 by September 1998	GSM	Mobile Telecommunications	Over 208 operators in 105 countries	Worldwide
80+	German Health Insurance Card	Health	German Health Insurance Companies	Germany
40-50	Geld Carte	Electronic Purse	ZKA (Zentraler Kredit Ausschuss)	Germany
15 by Nov 98 36 by May 99	Sesam / Vitale Card	Health	Ministry of Social Affairs	France
10+ 13 - 15 before 1999	ChipKnip	Electronic Purse	PTT Telecom and Postbank	Netherlands
6	Advantage Card	Loyalty	Boots the Chemist	United Kingdom
5* *1997 figure	Giropas	Electronic Purse	Postbank	Netherlands
4.6	Automatic Fare Collection- Seoul Bus Card Project	Transport	Seoul Bus Union	South Korea
4.3 7.5 by 1999	Proton Card	Electronic Purse	Banksys	Belgium
4+	SMART	Loyalty	Shell UK and a Consortium of retailers	United Kingdom

Table 1: SCN Smart Card Top Ten (May 1998)

Common to both systems is the need for adequate security segregation and the availability of sufficient chip resources. At the current time we have Mastercard supporting the Multos platform through Mondex International and Visa supporting the Javacard platform. It is technically possible to build a chip supporting both Javacard and Multos applications although this would potentially be inefficient. What is clear is that the move towards more sophisticated chips such as those with a 32 bit architecture enables Javacard to become a more practical proposition.

Gently emerging from the scenes is a bigger move towards contactless Smart Cards. There can be no doubt that in some application areas the contact card is not really practical. In particular mass transit is based on the ability to move people efficiently through some gate structure. The act of putting the card into a reader

can never match the passing of a contactless card over the surface of the reader. The performance of the application in the card is not dependent on the type of card; it is just as easy for a contact card to process a transaction in 150mS as it is for a contactless card. The perceived difference in performance is entirely due to the difference in the processing task. Most modern contact cards are working with public key cryptography compared with the much simpler symmetric processing used in contactless cards. The availability of the Combi card which provides both a contact and contactless interface is likely to become more commonplace and allows the complexity of the security functions to vary between applications using the two forms of the interface.

David B Everett