

Multi-Application Smart Cards:

The Next Property Boom?



About this Paper

Multi-Application Smart Cards: The Next Property Boom?

An inexorable shift in the world's card-payment business to 'smart' credit and debit cards is underway, spurred by their superiority to magnetic-stripe technology in combating fraud, and by a change in liability rules that is motivating banks to replace their cards by the end of 2005. Global smart card shipments are expected to increase substantially, from 1.7 billion to 4.1 billion units, with revenues up from US\$2.2bn to \$7.9bn between 2000 and 2006. Currently the Europe, Middle East and Africa (EMEA) region accounts for 50% of card shipments, but Asia-Pacific is catching up. North America is a late-starter in the smart card market due to the wider acceptance of magnetic-stripe technology.

The majority of smart cards today are in closed schemes providing single applications, e.g. SIM cards for mobile phones. However, adding more memory and processing power increases costs – between US\$4 and US\$9 per card is typical – but enables multiple applications. Among the most important of these will be access control – both physical and online – and authentication of messages by digital signature, etc. With e-commerce expected to exceed US\$1.4 trillion in sales by 2004, smart cards are proving the best technology for providing consumers with the online security, protection and portability they demand.

Who will exploit this powerful platform – the platform is the card, not the 'e-property' – and how? As smart card issuers explore which applications to provide, and with whom, issues of branding and customer relationship management loom large. In contrast to current credit cards, smart cards may well be owned by their holders, not by the banks. Defining a card proposition that will achieve the critical mass of users needed to secure commercial success promises big rewards, but the business model is far from obvious.

This paper is part of the global Financial Services practice's commitment to addressing the issues facing our industry, and aims to help financial services institutions transform.

Introduction

It's 2005, and Toni Teenager is checking her latest fashion accessory: her smart watch. This brings to five the number of smart cards she's wearing, but you can never have too many... in a few hours, she's got an appointment with her doctor at the local hospital for a check-up. She decides to stop by the gym first. She jumps into her boyfriend's car, using her smart card to unlock it. This automatically adjusts the seat's positioning and the radio's memory stations (which are different from her boyfriend's favourites). After driving a few miles, she stops to refuel the car. By inserting the smart card into the petrol pump, the payment is settled and value points are added to the card. She is excited to get the message that she only needs to collect a few more points to win a free trip to Disneyland!

At the gym now, Toni uses her smart card to record her weight and measurements. As Toni leaves the gym, she passes Dave Dynamic the gym owner who is pondering an interesting offer he has received from his bank manager. If Dave allows the bank to put its credit application onto his gym membership smart keyring, Dave will get a commission for every loan taken out by his members. Sounds like a good deal – but what's the catch? None apparently.

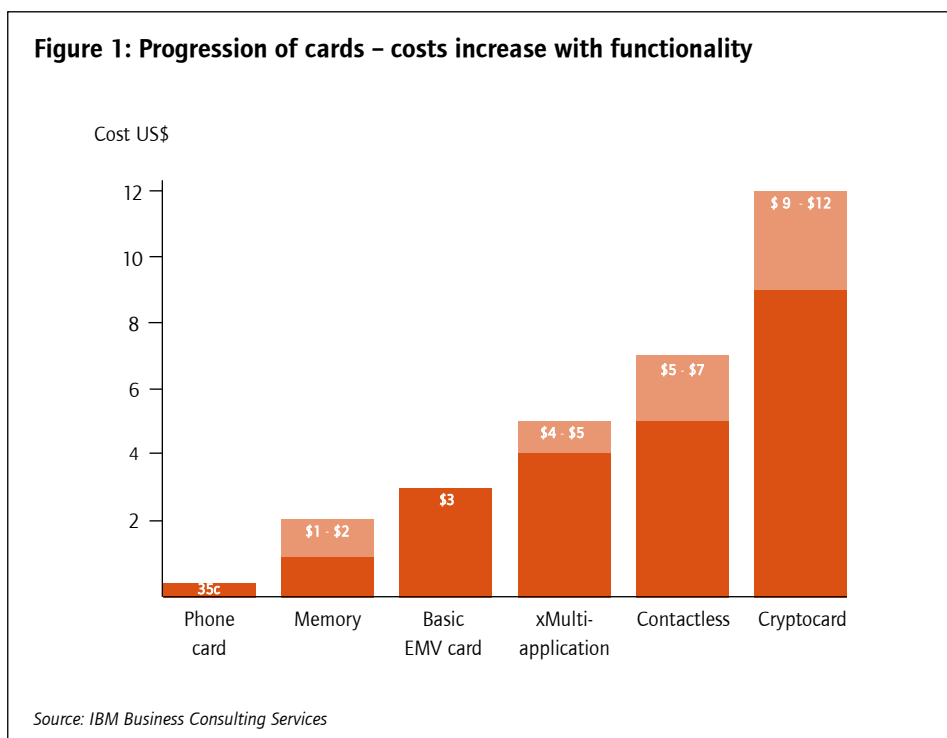
Toni has just arrived at the hospital and wants to make it a quick visit. The doctor uses Toni's smart card to check her medical history and he gives her a prescription that is stored on the smart card to take to the pharmacist. On the way to the pharmacy, Toni stops at a shopping mall to reload some money onto her electronic purse; she visits the pharmacy and uses the electronic purse to pay for the medicine. Finally done with everything, she looks at her watch and thinks "Gee, I'm running ahead of time!"

Smart cards appear in many guises: microcomputer card, electronic purse, train ticket, SIM (subscriber information module) card for mobile phones and loyalty card, to name just a few. Increasingly, not only banks but many other kinds of organisations – from retailers and telephone companies to national governments – are issuing smart cards and considering the benefits of sharing the space on the card – the e-property – with other potential issuers of smart card applications.

Smart cards are mainly a European invention, momentum for which grew out of difficulties posed by the expensive telecommunications required for the much cheaper magnetic-stripe technology. Because anyone with access to the appropriate device can read, rewrite or delete the data on a magnetic-stripe card, such cards are unsuitable for storing sensitive data. As such,

they require extensive online, centralised, back-end infrastructures for verification and processing. Unlike the U.S., European countries had more problems establishing extensive, high-quality and cheap data networks, and sought an alternative which could operate securely offline. Beginning with concept definition in France in the early 1960s, and following patents in Germany in 1968, primarily European developers made a huge improvement over magnetic-stripe technology by introducing the integrated circuit card (ICC), also dubbed the 'smart card' or 'chip card'. As significant progress was made in cryptography during the 1960s, smart cards proved an ideal medium for safely storing cryptographic keys and algorithms of the type needed in bank cards.

A magnetic-stripe payment card costs approximately 20 cents; the simplest smart cards, such as those providing memory only – which are used widely around the world – cost upwards of 35 cents. Introduction of microprocessors and additional memory raises costs considerably. Depending on complexity, smart cards can cost US\$4 or more. Figure 1 gives an idea of how costs rise for increasingly sophisticated smart cards.



Multi-Application Smart Cards: The Next Property Boom?

More sophisticated smart cards provide a very effective vehicle for security functions. Encryption and decryption using public-key cryptography (employing two complementary keys: a private key – which is kept secret – and a public key) can now be supported on smart cards. Digital signatures using the RSA algorithm and verifications – even at the 1024-bit key length – typically take less than a second. Smart cards enable multiple personal identification numbers (PINs) and tamper-proofing facilities, supplemented in some cases by various methods of hardware security monitoring. Hence, access control, both physical and online, is expected to be among the most important uses of smart cards. Online access management mediated by smart cards, with authentication of messages by digital signature, could well become the key to secure and reliable electronic commerce.

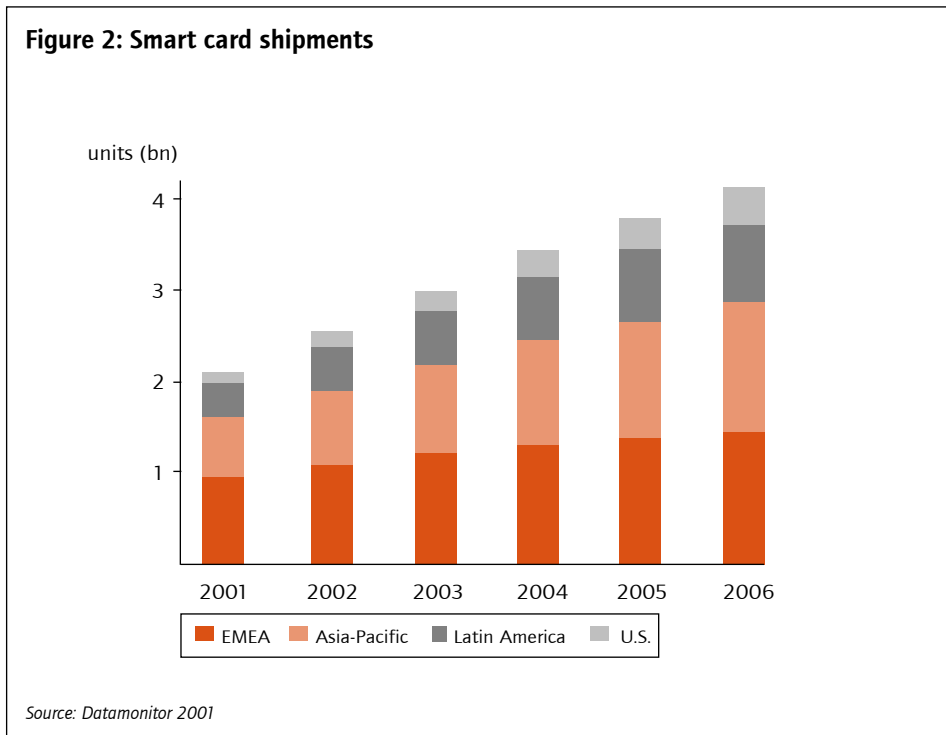
At present, smart cards are primarily deployed in closed schemes that provide single applications only. Thus, users must carry multiple cards for multiple applications. Furthermore, although sponsors such as telecommunications companies (telcos) can justify issuing cheap smart cards, e.g. for payphones, many potential sponsors have had difficulty building a suitable business case to introduce smart cards for their specific domains. The issue is not just the strength of the strategic business case, but uncertainty about take-up volume. Sponsors have struggled to define card propositions that will ensure the critical mass of users needed to make the scheme a success. Hence there is momentum for alliances providing multiple applications on the same card. The analogy of property is very apt: Who will be the owners? The freeholders? The renters? This translates as:

- Who will command the revenues from smart cards?
- Who will pay for the opportunity to deliver the services?
- Who will be prepared to take up the services?
- Who will actually gain the benefits?

These are all under active debate.

Size of Global Market

In shipment terms, the most mature smart card market is the Europe, Middle East and Africa (EMEA) region, accounting for over 50% of card shipments in 2000. However, EMEA's relative importance is expected to decrease as Asia-Pacific catches up.

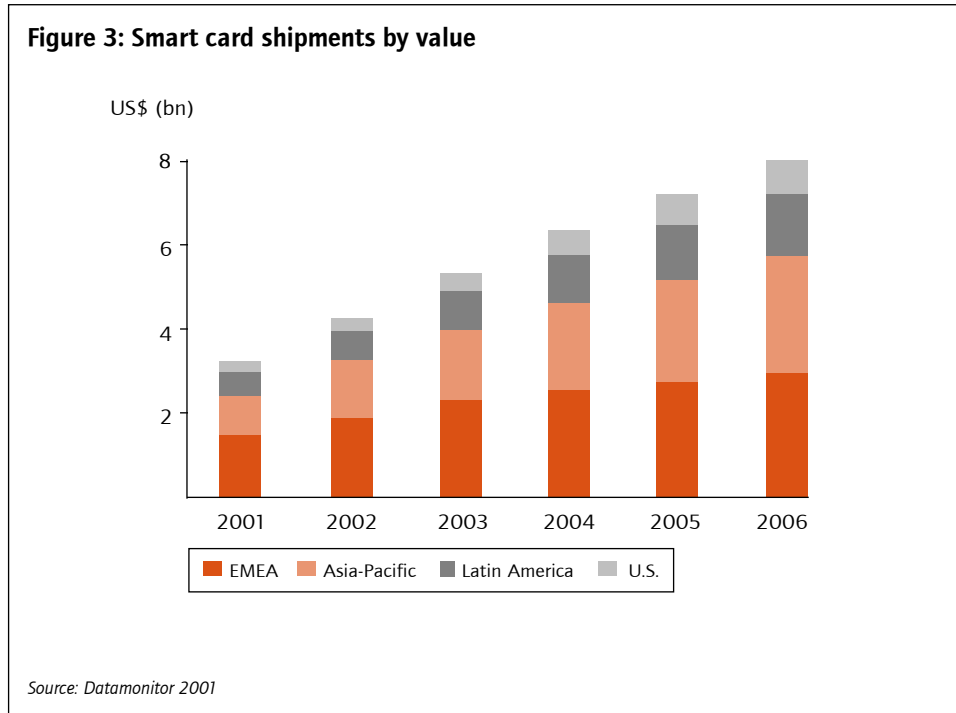


The vast majority of cards in issue at present are payphone cards, SIM cards for mobile phones and security/access cards for use in satellite and cable TV decoders.

According to Datamonitor, smart card shipments will more than double from 1.7 billion units to 4.1 billion units between 2000 and 2006 (see Figure 2). Smart cards are still far from realising their full potential.

Multi-Application Smart Cards: The Next Property Boom?

Global smart card revenues are expected to increase substantially from US\$2.2bn to US\$7.9bn during the same period (see Figure 3).



Almost all smart cards issued today conform to a set of international standards in the ISO 7816 series, which defines the physical location of the chip on the card, the contact arrangements, and a wide range of internal memory and processing characteristics.

The main international suppliers of smart cards include:

- Geisecke & Devrient (G&D) in Germany and the U.S.
- Gemplus in France
- Keycorp in Australia
- Oberthur in France and the U.S.
- Orga in Germany
- Schlumberger-SEMA in France
- TTI-Cardtech in Japan and the UK

Most manufacturers write proprietary operating systems for each type of chip card they produce. However, in recent years, multi-application operating systems have been developed. These sit on top of the card's proprietary system and can host parallel applications separated by secure firewalls. To coordinate multi-application standards and development initiatives, Visa has brought together a number of manufacturers to create the 'Open Platform' group. This includes both the well-known operating system MULTOS (produced by the Maosco consortium involving MasterCard) and a development and operations toolset called JavaCard, whose sponsors include both Visa and American Express.

In contrast to smart cards, which all have very similar construction, smart card readers/terminals come in a variety of forms with differing mechanical and logistical sophistication. Electronically, all readers must conform to the ISO/IEC 7816-3 standard, but otherwise there are various options to consider, including whether insertion/ejection is carried out automatically or manually, whether sliding or landing contacts are employed, and how displays and keystroke entry are provided. There is now a move towards lower voltage cards and readers (3V instead of today's 5V) to allow longer battery life in mobile devices and higher clock speeds to give greater computational power.

Applications of Smart Cards

The three core functions of smart cards are:

- 1 Information storage and management
- 2 Identification of the cardholder
- 3 Calculation (especially for encryption/decryption)

These lead to a host of uses, of which the five most popular are described below.

Authentication

Smart cards offer a good means of identifying an individual. Usually this is based on a user name and a password or PIN. But other methods of authentication are available or are under test: biometrics, for example, in which a fingerprint or retina is scanned. Fingerprint scanning in conjunction with smart identity cards is now in routine use in, for example, Malaysia. Retinal scanning is widely used for military access control. The biometric parameters can be digitised, encrypted, and stored on the card and compared with the 'biometrics' measured directly from the individual when access is desired (e.g. for medical records, high-security areas, government and financial services).

Portable personality

In this case, smart cards are used to store a number of parameters which define the 'personality' of a normally much larger device. GSM phones are a good example: the smart card ('plug-in') that is inserted into the phone stores details such as account number and personal phone books. Plugging the smart card, or SIM, from phone A into phone B will transfer all of the stored account and contact details from the former to the latter.

The car industry is exploring smart cards that can set different characteristics – seat and mirror positions, for example – for different drivers of a given vehicle, so that they need not make multiple adjustments whenever they use the vehicle.

Portable data files

A smart card can currently store up to 100 times as much data as a conventional magnetic-stripe card. This is particularly useful in areas such as health services, for which a significant

amount of data storage is needed, that can be quickly accessed by those in need of the data. Special mechanisms (e.g. PINs and biometrics) for authenticating the person to whom the card relates are also offered by the smart card, so security and privacy are ensured. A pilot implementation of a health smart card carrying medical records, prescriptions and test results, for example, has been conducted in Australia.

Data held in this way can be kept in conjunction with a centralised or decentralised computer system, and the cardholders have control of their own personal records.

Data transport

The utilities industry provides a good example of transporting data between computer systems and peripheral devices. Sophisticated gas meters and water meters store data that control tariffs and other service options. These parameters can be updated from a smart card containing a new set of data.

Central computer systems are used to collect meter readings in order to maintain an overall view of the domain. Smart cards are used in asynchronous communication between computer systems and meters. The central systems load new parameters onto the smart card and, when this is transferred to the meter, a reading is written back onto the card. In turn, the meter reading is passed back to the central system when the card is next charged.

Stored value

Telephone cards and electronic purses are widely used types of stored value cards. Stored value cards are available in either disposable or reloadable forms. The electronic purse, for example, can be reloaded from a bank account, over the counter, or by transferring value from another electronic purse. However, disposable prepaid cards, such as telephone cards, cannot be reloaded.

A different form of stored value is that associated with loyalty programmes. Here, the value stored and manipulated relates to the points-holding of the customer. Smart cards enable more sophisticated and flexible loyalty processing at point of sale. Tiered points allocation – for example, according to quantity and combinations of purchases, using applications downloaded to the card (so that the point of sale system does not have to handle them) – can be used to encourage purchases by the most profitable customer groups.

How the Changing Consumer Model Adds Impetus

Dramatic changes in the consumer model are driving the need for smart cards. By 2004, it is estimated that e-commerce will account for \$1.4 trillion annual worldwide sales, mobile commerce (m-commerce) will exceed \$175bn, and commerce conducted through digital TV (t-commerce) will surpass \$7bn in the U.S. alone (see datacard.com).

Case Study: Chipcard Migration Planning

IBM Business Consulting Services worked with major banks in Canada, Australia and Taiwan, to assess the business case for the mass introduction of payment smart cards. One of these countries, Taiwan, has a significant fraud problem. Canada and Australia believed there was an opportunity for added value from smart cards but did not initially feel that fraud would be a major driver. We conducted analysis of historical and projected fraud with and without chip cards, including projections of fraud migration from countries with a chip programme. We explored the benefits of PINs and developed a comprehensive financial model examining different fraud migration, liability, cardholder and merchant roll-out strategies. We investigated the potential benefits to be gained from multi-application smart cards and concluded that the most convincing benefit streams would arise from value-added applications, but that the threat of massive fraud was real and could be combated cost effectively by smart card deployment.

Authentication and non-repudiation

From a consumer marketer perspective, the emergence of e-, m- and t-commerce represents tremendous opportunities for growth and profit. But it also poses new challenges – primarily in terms of authentication and non-repudiation for the prevention of fraud.

Smart cards provide an effective solution for these challenges. Smart cards with public-key infrastructure (PKI) capabilities allow consumers to attach digital signatures to every online transaction they make. A variety of technologies – including cryptography – make it virtually impossible to forge or alter these signatures. This means that consumer marketers know precisely with whom they are conducting business. Moreover, merchants are protected from fraud because a cardholder cannot deny or repudiate a transaction verified by a digital signature. The technology helps clear the path to an entire new era of growth and prosperity driven by safe and easy online commerce.

Privacy and personalisation

Because e-, m- and t-commerce are relatively new, many consumers are concerned about privacy – especially as they conduct online transactions and provide valuable and highly personal data to people they will never meet.

Smart cards have proven to be the best technology for providing consumers with the online security, protection and portability they demand.

Consumers will be able to access privileges virtually anywhere with their smart cards. They will be able to insert their cards into computers, telephones, kiosks or terminals that are equipped with smart card readers, and instantly turn a generic device into a highly personalised one. Access to government services via online kiosks is an example – to renew vehicle registrations, for instance, or to change address on the electoral roll.

If these applications were stored on a computer, telephone or other device, they would not be nearly as portable. They would also be less secure. Applications stored on a standard PC, telephone or other network device could possibly be extracted and compromised. Applications and data stored on smart cards can be protected with advanced and highly secure on-chip operating systems, and held personally by the users.

Vendors are also developing systems that allow card issuers to replace lost or stolen cards very quickly – and the cards that are reissued will reflect the applications and the value that resided on the card when it was lost or stolen.

Who Will Win the Smart Card War?

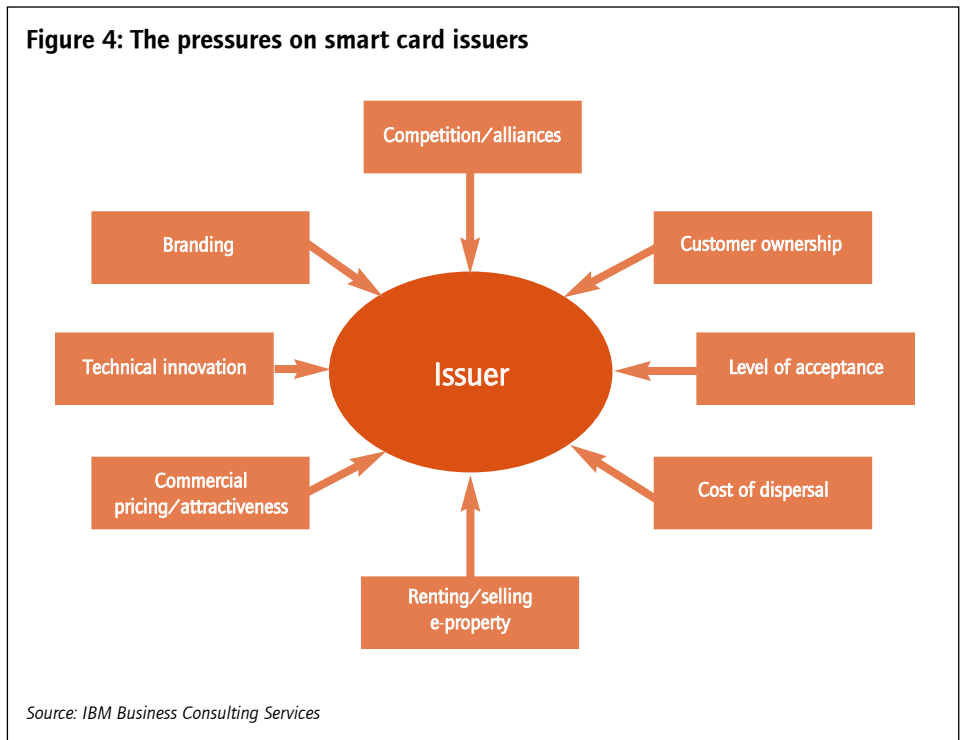
Will payment systems move to smart cards, and smart cards expand to multiple applications?

Europay, MasterCard and Visa have introduced a global standard for financial institutions (the EMV Standard) on a non-competitive basis for all financial transactions that use smart card technology. Mandatory dates have been set by Visa for all acquiring banks to comply with the EMV standard. Essentially, in the European Union (EU), all new terminals from October 2002 must be EMV-compliant. For the rest of Europe, the Middle East and Africa, the deadline is one year later. However, at the end of 2005 liability for fraud falls wholly on the issuer for non-EMV cards, so there is strong incentive for all terminals and cards to be EMV-compliant. Additionally there is an opportunity to expand electronic funds transfer at point of sale (EFTPOS) to high-volume, lower-value transactions using off-line authorisation, as well as to develop new revenue streams from multiple applications hosted by EMV cards.

In North America, the situation is more complex. Because of cheaper telecommunications and extensively outsourced networks, magnetic-stripe technology is not yet regarded as a problem that needs to be fixed. However, there is particular concern that, even in countries with online debit card EFTPOS systems, pre-status fraud (fraud that occurs before the loss of the card is reported) and counterfeiting will continue to grow rapidly, and that fraud will migrate to hit non-EMV issuers.

Financial institutions are already using smart card technology, card personalisation and smart card management systems for smart card applications and schemes. Some of these will now have to integrate with EMV payment functions. However, the real question for banks is whether they own their customers in this area, or – given that they have lagged in technology – will these customers be poached by other suppliers with multiple-application smart cards, which offer payment facilities as an adjunct? Clearly there are regulatory limitations on this; nevertheless, bank branding may suffer as non-bank institutions push their products on the card, leaving the payment function as a lesser element.

Figure 4: The pressures on smart card issuers



Outlook

In the short-to-medium term, there are certain smart card markets in which single-product smart cards will continue to present a strong proposition, including their use as simple phone cards to support GSM-based mobile telephony and certain high-specificity payment and security products.

In the medium-to-long term (three to five years), the strong financial proposition – both in terms of cost sharing and greater cardholder utility – is likely to drive the vast majority of issuers toward smart cards able to support multiple cross-industry products simultaneously.

Multi-Application Smart Cards: The Next Property Boom?

With several applications residing on one card, the necessary investment in hardware can be spread across those applications. Just as a PC becomes a viable purchase because it can perform varied functions (Internet access, spreadsheets, e-mail, word processing, etc) so smart cards become economical to issue if they have many uses – each with a revenue stream attached. Also, because smart cards can carry rewriteable memory, applications can be dynamically loaded and deleted from cards after they have been issued.

The result is that the card's lifespan is increased – old applications can be removed and new ones added, and there is no need to issue a new card (as is the case with single-application smart cards or magnetic-stripe technology). The longer a card is usable, the longer it has to make money for its issuer.

There are already a number of products on the market which enable a card issuer to manage the dynamic loading and unloading of applications onto a multi-application card. These include:

- Affina by Platform Seven (part of Datacard in the UK)
- Smart Chip Manager from ACI (one of the main card-transaction switch suppliers, based in the U.S.)
- 4Most from Oberthur in Germany
- Arterium from Cards Etc in Sydney, Australia

Challenges

Of the many challenges facing issuers of smart cards, we highlight three below.

Data storage and protection

The smart card has the capability to integrate applications to form a multiple-application card by utilising its embedded microprocessor and memory-storage spaces. However, this kind of integration is always limited by external logical elements rather than by technical issues. For instance, in a single-application card system, data stored on the card – and even the card itself – always belongs to the card issuer. This may become impractical with more than one application residing in a single card.

Moreover, the method of partitioning the memory spaces for different applications, and management of the rights and privileges of data access, must be considered. This also relates to data directory configuration and security between each application. Furthermore, the ability for applications to communicate and share data is another important concern that may affect the whole design of the system and its operability.

Branding

Some of the biggest commercial issues concern branding. The current situation is to have one brand logo per application on the card. This works well as long as the applications on the card are few, and remain static. But with the growth in available erasable programmable read-only memory (EPROM), allowing more and more applications to be loaded onto the card, the number of logos required to show all the different applications on a card will proliferate. Eventually the time will come when it will not be possible to fit all logos legibly on one card face.

Furthermore, with the ability for applications to be added and deleted, if there is one logo per application the card will no longer show all the services it can provide, or may even show ones that it no longer carries. New technology solutions may provide an answer to the problem of adding and deleting brands from a card's face during its lifetime.

Banks are concerned that, even if they provide an application on a multi-purpose card, the branding power of the card for the financial institution will be eroded.

Multi-Application Smart Cards: The Next Property Boom?

An innovative solution to the branding problem is to create one brand which covers a number of applications that companies provide as an issuer/group of issuers. An intriguing example of this is the 'I-Life' umbrella:

Case Study: The Multi-purpose, multi-issuer smart card

The 'I-Life' Multos card in Hong Kong has been issued as a joint venture between HSBC Bank and Hong Kong Telecom/Cable & Wireless. The card contains financial applications such as MasterCard's M-Chip Credit payment application and the Mondex e-Cash application, together with the HKT/C&W International Calling Card application. In addition, there is a digital signature application allowing secure access to Web-based services offered by the two organisations, including secure shopping on the Internet. The services offered are branded under the 'I-Life' umbrella.

Wherever the cardholders see the brand logo, they will know an application on their 'I-Life' card is supported by the retailer. If new applications are added to the 'I-Life' card later, HSBC and HKT/C&W can advertise the fact via a marketing campaign, by, for instance, direct mailing the cardholder to keep them informed of the new applications use. Or the cardholder can be presented with a menu of applications on their card at the point of interaction, e.g. an ATM, or Internet browser screen.

Cards and tokens

We are concentrating our attention at present on cards, but there may be more convenient tokens in which intelligent chips can be embedded, such as rings and watches. Chips may even be embedded within the body.

Already, SIM cards are only a small segment of a credit card-sized piece of plastic. However, the investment necessary in both tokens/cards and terminals capable of reading different kinds of tokens is large and it is likely that the humble plastic card will be with us for a while yet.

In thinking through future design, however, issuers need to be imaginative if they want to invent a category-killer product.

Conclusion

There are a broad range of approaches to, and applications of, smart cards. Designing multi-application products and roll-out strategies that will attract the required degree of take-up for commercial success is certainly a challenge. It remains to be seen whether the banks will be able to maintain ownership of customer card bases when other types of issuers (telcos, government, retailers or even fashion houses) could also offer smart card products capable of supporting payment-card applications. Smart card branding and customer relationship management open a new arena for competition and cooperation.

The case for smart cards is compelling:

- Smart cards enable the consumer marketers to know precisely with whom they are conducting business and to implement valuable loyalty programmes.
- Smart cards have proven to be the best technology for providing consumers with the online security, protection and portability they demand.
- Smart cards can provide three core functions: information storage and management, identification of the cardholder, and calculation (especially for encryption/decryption) which allows uses such as authentication, portable personality, portable data files, data transport and stored value.
- Europay, MasterCard and Visa are promoting the implementation of the EMV Standard and there is a general acceptance that EMV smart cards will form the basis of future card payment services.

Call for action

Moving to smart cards is not optional; the EMV Standard timetable is in place and those who don't adopt smart card technology will pay the price in increased fraud – and fraud prevention is a must. Given the significant investment implicit in replacing existing magnetic-stripe cards with more expensive smart cards, and upgrading IT (eg replacing terminals), etc, how can the returns be maximised from this powerful technology – before the competition? The timetable creates a finite period to benefit from being a pioneer or fast follower entering the smart card market; the entry cost raises the stakes for getting the strategy right from the beginning. At a minimum, organisations need to ask themselves:

- What unique opportunities can we pursue on our own?
- What alliances should we be pursuing with other industries for multiple applications?
- How do we market smart cards effectively to our customer base?
- How will smart cards support banking through multiple channels (e.g. online) in the future?

The strong financial proposition – both in terms of cost sharing and greater cardholder utility – is that smart cards are able to support multiple cross-industry products simultaneously. The vast majority of smart card issuers will head in that direction – so don't be left behind. Better yet, be proactive and move nimbly towards a creative customer proposition!

Glossary

EFTPOS: Electronic Funds Transfer at Point of Sale

EMV Standard: Europay, MasterCard and Visa international standard for smart card technology

EMV '96 ICC Specifications for Payment Systems: Europay, MasterCard and Visa joint specifications for smart payment cards – setting in place the components of the framework for a worldwide payment system based on the use of smart cards. This has been augmented by EMV 2000.

EMV 2000: This is intended to provide the basis for implementation of EMV '96 and extends the standards for smart cards, related technology and the next generation of cards.

EPROM: Erasable Programmable Read-Only Memory

GSM: Global System for Mobiles – digital mobile phone standard

ICC: Integrated Circuit Card (also known as the 'smart card' or 'chip card')

ISO 7816: This standard is separated into multiple sections, the first three defining the physical characteristics of the integrated circuit card, the dimensions of the card and position of contacts, and the electronic signals and transmission protocols.

ISO/IEC 7816-3: 1997 standard from the International Organisation for Standardisation and International Electrotechnical Commission, surrounding electronic signals and transmission protocols for integrated circuit cards with contacts.

PIN: Personal Identification Number

PKI: Public-key Infrastructure

RSA algorithm: Public-key cryptosystem (originally developed to help ensure Internet security) – invented in 1977-78 by MIT professors Ron Rivest, Adi Shamir and Leonard Adleman

SIM: Subscriber Information (or Identity) Module. A mobile phone consists of two main components: the mobile transceiver and the identification module – or SIM card. Different identification modules can be used with the same transceiver and vice versa.

Acknowledgements

Thanks to the following for their contribution in the creation of this white paper:
Dr. Gordon Clarke, Kate Daniels, Richard Kernick, Christos Tsialtas, Andrea Lowe.

About IBM Business Consulting Services

IBM Business Consulting Services (ibm.com/services) is one of the world's leading providers of management consulting and technology services to many of the largest and most successful organizations, across a wide range of industries. With offices in 160 countries, IBM Business Consulting Services helps clients solve their business issues, exploiting world-class technology for improved business performance.

www.ibm.com/services



©Copyright IBM Corporation 2002

IBM Corporation

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
All Rights Reserved

IBM logo is a registered trademark of
International Business Machines Corporation
in the United States, other countries, or both.

Other company, product and service
names may be trademarks or service
marks of others.

References in this publication to IBM
products and services do not imply
that IBM intends to make them available
in all countries in which IBM operates.

GW510-9139-00