SMART CARDS AS AN ELECTRONIC MEDIUM OF PAYMENT FOR BANKING SYSTEMS

Craig Lloyd Kent

Technikon Witwatersrand
Bachelors of Technology
Information Technology

ckent@absolutesys.com
(H) +27 11 705 – 3105
(W) +27 11 784 - 0078
(C) +27 83 – 225 – 4457
P.O Box 930
Fourways
2055
Johannesburg
South Africa

ABSTRACT
Smart cards are making a big impact on payment systems. The purpose of this paper is to excite the reader about the future of payment and banking technology in the domain of smart cards. This paper will introduce smart card banking technology to people who have no knowledge about smart cards and elaborate on existing knowledge of people who have an in-depth knowledge on smart card technology. Many South African companies do not understand the benefits of smart card payment. This paper is aimed at companies who want to learn about smart card banking and increase existing knowledge on smart banking, or information technology professionals who are interested on the future of smart card systems. The reader will be introduced into the world of smart cards. They will discover the advantages of smart cards for financial and non-financial purposes. They will see how smart banking is making an impact in security and e-commerce. The reader will be introduced to, and educated on EMV compliance for smart card transactions.

KEY WORDS
Smart card
POS (Point of Sale)
Smart card applications
Smart card payment
Smart card banking
Cryptography
Banking security
EMV (Europay, MasterCard and Visa)

SMART CARDS AS AN ELECTRONIC MEDIUM OF PAYMENT FOR BANKING SYSTEMS

1. INTRODUCTION

Imagine a cashless society, where you can use smart cards to do many interesting things. This is becoming a reality and smart cards are making people's lives much more easier. Smart cards are used for transportation systems, to store important medical information, and even to purchase items from vending machines like the examples mentioned in (Zoreda and Oton, 1994:139-163). Smart cards are even taking advantage of the Internet. A smart card reader can be plugging into the back of a personal computer (PC) and items can be purchased over the Internet making use of smart card security. Hyperion (1997) speaks about using smart cards over the Internet. This paper is going to investigate the new exiting field of smart banking.

The paper will start off by giving a small overview of smart cards, to give the reader a basic understanding on what a smart card is. The paper will then introduce a few examples where smart cards are used in non-financial applications. Then examples of financial applications will be presented. The paper will then investigate why smart cards are so popular. Before the paper wanders into smart banking, a basic overview of cryptography will be explored. The paper will then delve into banking with smart cards and have a look at e-commerce and secure payments. A standard for smart card banking called EMV will then be introduced. The paper will be concluded with an investigation of the use of smart cards in SA (South Africa).

2. BACKGROUND ON SMART CARDS

2.1 General information

Most people have come across smart card technology somewhere in their life. Zoreda and Oton (1994:5) refer to a smart card as a type of a chip card. A chip card contains one or several electronic circuits embedded in a plastic substrate. Dreifus with Monk (1998:17-22) mention two kinds of smart cards, memory cards and smart cards with microprocessors. A memory card is mostly used for storing information and is disposed of when the user has finished with the card (public telephone card). Smart cards with microprocessors (most commonly used at present) contain a microprocessor with an OS (Operating System) and receive their power to operate from the reader. Smart cards can also be contact less (reader communicates with smart card via radio frequencies) and are powered by the external source with an electromagnetic field as indicated in Zoreda and Oton (1994:51). Smart card application can be programmed using various programming languages (C, COBOL, Java) and downloaded onto the chip as shown in Dreifus with Monk (1998:15). The smart card readers will be able to invoke the application on the smart card for desired functionality.

2.2 Smart card readers

Smart card readers can be purchased and plugged into the back of a PC. Microsoft (2001) shows how Windows OS is making use of smart card functionality by integrating smart card technology into Windows. Smart card technology is taking advantage of Windows functionality and applications can be developed for Windows to process smart cards. A good example of this would be logging onto a PC using a smart card for identification and purchasing goods over the net, using a smart card as a debit/credit card. Smart cards can also be used with POS (Point of Sale) terminals, which are small devices that contain a modem, keypad, smart, magnetic reader, printer, and other

devices depending on what the terminal will be used for. POS terminals are normally placed at retailers for payment purposes. Ingenico range of terminals (leader in POS) can be viewed on the Ingenico (2003) website. Smart card readers are also placed within machinery (vending, telephone, gambling) to allow that machinery to make use of smart cards as will be seen in the examples.

2.3 OS on smart cards

Smart cards contain an OS, which handles the applications stored on the chip. Kingdon (1998) shows an OS called MULTOS (Multiple application OS) that can handle more than one application on a single smart card. A good example of this would be two applications, one used for transportation purposes and the other used for banking, on a single chip. This eliminates the need for another card, reducing the number of cards the person needs to lug around. An application can be loaded and deleted at an in-branch, an ATM, and even over the Internet. Each application on the smart card is protected by a firewall; so one application on the same card cannot affect the functionality of other applications.

3. NON-FINANCIAL APPLICATIONS

3.1 Biometrics and identification

Smart cards are drastically changing our lifestyles as will be seen in the following examples. The first set of examples that this paper will have a look at is non-financial smart card functionality. The first example will have a look at smart card biometrics. Smart cards can be used for storing biometric information (fingerprints, facial characteristics, and voice patterns). Gates (1997) illustrates an example of eye biometrics (Iris scanning). Data about the Iris is stored on smart card, and this can eliminate a pin number for banking transactions (every persons Iris is unique). The iris code can be used for conformation of identification. Another useful identification system for smart cards is identity cards. In the UK they are trying to implement smart ID's. Muir (2002) being very biased gives a negative perspective about smart ID's saying that it is invasion of people's privacy.

3.2 Medical applications

Smart cards are also making an impact in the medical industry. Kavanaugh (2001) shows a system in the USA, where medical information (demographic, insurance data, list of allergies, disease history, emergency contact information) is stored on a smart card. This information and patient data can be shared between health care providers. Ambulances contain laptops with smart card readers and pharmacies also have card readers attached to their PCs to read the information from these cards. This system can save a lot of people's lives by having important information within reach of medical personnel. Another good example of smart card usage in the medical field is security access in UK hospitals. The smart card becomes an information carrier; the smart card reader system only allows authorized personal into certain zones of the hospital. Hospital (2002) indicates how hospitals can become more safe and secure by limiting personal to specific locations at certain times. This hospital security system can even be implemented in the hospital's parking bay to help coordinate where certain vehicles can park.

3.3 Transportation

Transportation systems are also taking advantage of smart card technologies. The London Metro system is using smart cards to store credit as indicated Metro (2002). The smart card acts like a credit card and signals when the credit is running low. This system is also useful for collecting information, so that transport services can be improved. People traveling on the tube, mainline rail and bus transportation systems will make use of this smart card. Fare Collection News (2002)

illustrates a transportation system in San Francisco that is also making use of smart cards. Smart card readers are located at rail, bus, ferry and bridge operator terminals and the smart cards that are used store dollar values, rides and monthly passes. The passenger doesn't have to remove the card from their wallet; they just have to tag the card near a reader. Cards can also be reloaded in the future. Smart cards are also being used as locks in car. The 2001 Renault Laguna II illustrated in Gray (2002) uses a smart card identifier. The smart card sends out a radio frequency and the cars detection system looks for that card's frequency. When the driver opens the car door it will unlock and open if the smart card is in close range of the vehicles detection system. Locking the car is easy; the driver just has to walk away from the car (out of range). To start the car the driver inserts the smart card into the reader and pushes the start button.

4. FINANCIAL APPLICATIONS

4.1 Education

This paper is going to mainly focus on the financial aspects of smart cards. Smart card technology is playing a big role in banking and the financial sector. School kids in the UK are making use of smart cards to purchase meals from eating clubs and vending machines. Local (2002) shows this system where a smart card stores money and free school meal information. This allows parents to monitor what money is being spent, and money can be added on the card on a daily basis. Information about ordered meals is also stored on the card, so that pupils can be rewarded for healthy eating habits. These cards can also be presented at libraries for proof of age. Smart cards are also impacting on tertiary institutions. Didier (2000) takes a look at how smart ID cards are increasingly being used in universities in the USA and other parts of the world. These ID cards are used for secure identification (security access to certain parts of the campus) and for payments. These ID cards can be used over the Internet for uses like distant learning and student voting. Students can make phone calls using this ID card and the system will know which student account is to be billed for the phone call. These ID cards can also store electronic cash making it more secure for payments involving libraries, printers, telephones, vending machines, laundry facilities, dining facilities, bookstores and even merchants. The ID card can also be used as an ATM card for banking functionality, financial aid payments, and student refunds.

4.2 E-purse

Singapore is using a cash card which is a nation wide E-Purse (Electronic Purse). An E-Purse eliminates the need to carry wads of cash around, by just having a smart card for payment purposes. Cashless transactions can be done in Singapore using these cash cards as indicated by Ang (2000). These cash cards hold cash and can be used for multipurpose payments. They can be purchased at banks; post offices and cash card dispensers. Value can be added to the cash card at ATMs and top up devices. When the value is added, it is recorded on the card and the amount is credited to the consumer's bank float account. These cash cards can be used from department stores to payphones all the way across the country. The money value is stored in the consumer's float bank account and when purchasing an item using the cash card, the transaction details are uploaded and eventually the money gets debited from the consumer's float account. This system is also used to pay for toll roads using a contact-less smart card placed within the vehicle. The toll road payment points contain radio antennas, transmitters and cameras, used to exchange payment data over radio frequencies. These cash cards can also be used over the Internet to purchase items. In order to make use of electronic commerce the consumer needs to have a smart card reader and downloaded electronic wallet software.

4.3 Payphones

Yli-Untinen & Mononen (1998) describes a payphone smart card system that makes use of a SAM (Secure Application Module) chip. A SAM is similar to a smart card but only contains the small chip, which is used for security purposes so that the application can only run when the SAM is present. The SAM inside the payphone contains algorithms needed to authenticate payphone cards. There are two kinds of payphone smart card that can be used, disposable and reload-able. Disposable cards are disregarded after the money has been used up, while reload-able cards can be reloaded with more money. Reload-able cards are preferred because they are cost effective and have higher security.

4.4 Banking cards

Edwards (2000) indicates that banking with smart cards first started in France and is currently taking off in the UK. Visa cash electronic purse is one implementation that can contain credit and debit applications on a single card. This card can also have multiple applications like physical access to certain premises or remote banking over the Internet can be done with the same card. These banking cards can be used around most of Europe and hopefully soon around the world and can store biometric information for identification. This paper takes a deeper look at the protocols used for smart banking.

5. WHY SMART CARDS?

From the above examples it can be seen why there is so much interest in smart card technology. Zoreda and Oton (1994:20-21) indicate four methods (theft, counterfeit, buffering, and skimming) that are aimed mainly at magnetic card fraud. It also explains that anybody with a little technical knowledge can easily encode magnetic stripes. Edwards (2000) shows the advantages of smart cards in banking. It explains this by showing the security advantage of smart cards and how replacing the old magnetic cards with new smart cards have reduced fraud. The fraud rate has dropped in France when introducing smart banking cards and the same has happened in the UK. There is still nothing that can be done to address the problem of lost or stolen cards, but smart cards can offer more secure methods of holder verification. Another advantage of smart cards is the sharing of multiple applications on a single smart card (electronic purse). Smart cards can keep applications separate from each other and this eliminates a person's wallet from being crammed with individual cards for different purposes. Storing information is another big advantage of smart cards. Card verification methods can be improved by storing biometric information on the card. A good example of this would be storing a person's finger print information on the smart card for identification purposes.

6. BASIC OVERVIEW OF CRYPTOGRAPHY

Cryptography plays a big role in smart banking. Dreifus and Monk (1998:47-63) describes cryptography as a set of mathematical algorithms used to implement security functions and discusses four uses of cryptography namely data integrity, authentication, non-repudiation, and confidentiality. Data integrity makes sure that data doesn't get tampered with or corrupted during communications. Data integrity makes use of a hash value (check digit) and uses cryptography to check if this hash value is correct when receiving data. Authentication uses a digital signature (unique like a handwritten signature), which is transmitted to the desired receiving system. The received signature is decrypted to confirm the identity of the sender. Non-repudiation is used when other businesses (apart from the bank system) needs to process transactions. Confidentiality is used

to keep information confidential, so intruders cannot invade privacy. Confidentiality makes use of symmetric and asymmetric algorithms. Symmetric uses the same key at the sender (encrypt) as the key at the receiver (decrypt), which is referred to as a static key. Now asymmetric uses a private key (only one unique key) at the sender, which is different to the public keys (dynamic) at the receiver. Public keys can be distributed between a numbers of trusted receiving systems to encode the desired primary key. To really prevent fraud in banking systems, they use a session key, which makes use of triple encryption or superalgorithm. The information is encrypted three times making it impossible for intruders to crack.

Zoreda and Oton (1994:94-98) mentions that cryptographic keys are placed in the cards read protected memory, where only the microprocessor can have access to those keys. Access to those keys can only be made with permission from the microprocessor. There is a security standard ISO 7816/4, which controls card and message security. Card security is in charge of protecting the information on the card, while message security protects the information being sent and received from the card. Zoreda and Oton (1994:39-45) also mention two algorithms used for cryptography. DES, which is used for symmetric and RSA, which is used for asymmetric. Dreifus and Monk (1998:223) mention a new kind of public key, which will replace RSA called EEC (Elliptic Curve Cryptosystem). EEC provides greater strength, faster speeds and smaller keys.

7. SMART CARDS USED FOR SECURE BANKING

7.1 Smart banking systems from the past

As an introduction to smart banking, this paper will first have a look at two old smart banking systems, Mondex and Visa Cash. Wayner (1997:209-215) speaks about smart cards acting like cash. Money can be transferred between smart cards or merchant computer systems. If a card is misplaced, it can be cancelled (similar to canceling a traveler's cheque) because each card has a unique PIN number. A big advantage is that money can be transferred, without getting permission from a central bank, but there will be a problem if someone manages to produce rogue cards (counterfeit cards). With the Mondex system there are cards that keep an audit trail of all the money that has been accepted and dispensed. There is also a wallet, which is a smart card containing LCD, keyboard, and port. The wallets function is to transfer funds between other smart cards (soon a wallet will be integrated into cell phones). In order to eliminate fraud, two different protocols are loaded onto the chip at a time. The transfer of money is done using different protocols. The protocols are continuously updated on the cards, to avoid the cards becoming invalid immediately. The Mondex system is broken up into different levels (cards don't have equal status). On the primary level the card only maintains a balance and there is a limit on the amount the card can hold. On the next level is the wallet, which is allowed to transfer funds and can have different amount limits. The following level will be the merchant terminal, which keep a longer record of transactions and correspond frequently with the central bank. The final level will be 'Mint money' which is controlled at the central bank that actually generates the money. With the Visa Cash system smart cards and readers are dispensed all around the city. This system was tested at the 1996 Olympics held in Atlanta Georgia.

7.2 E-commerce

E-commerce is playing a big part in smart banking. As previously discussed, a smart card reader can be plugged into the back of a PC opening a whole new world of shopping. Kendrick (1997) explains the benefits that smart cards can add to e-commerce. Smart cards have the advantage of being able to store lots of information and being able to contain multiple applications on a single

chip. Using smart cards together with the Internet can solve authentication and security problems involving trading over the web. With old ATM cards, data had to be stored inside a single computer, but now with smart cards, data can be stored on the card. This makes payment with smart cards more transferable. Money can be downloaded from a bank account and loaded onto the smart card using the Internet, Kendrick (1997) likens it to having a coin box plugged into the back of your PC. Money can be channeled more securely through the Internet with smart cards acting as a catalyst. A problem with using magnetic type credit cards is that most customers don't have them and most merchants (especially small scale) don't accept them. Smart cards are becoming more accepted and because of their tighter security advantage, customers and merchants will accept them with greater enthusiasm. Smart cards could bridge the link between physical and virtual worlds. At the time the Kendrick (1997) was published VeriFone had plans to introduce the Personal ATM (P-ATM), which is a palm sized smart card reader which connects to the telephone line. Cash can be downloaded onto a smart card from a bank account using the P-ATM.

7.3 Smart security

Secure payments are the biggest advantage of smart banking. Hochfield et al. (1997) gives a deeper explanation of smart payment security. Confidential data (payment details like PIN codes) needs to be sent over open systems like the Internet. Intruders can tap into this information and use it for fraudulent purposes. These systems require a method to determine if the sender is a genuine sender and an intruder has not tampered with the message. The solution to this is a digital signature (an electronic version of a hand written signature) for authentication of messages. These signatures are encrypted with an encryption key and sent along with other message data, the signature is then decrypted with an encryption key on the receiving side. This encryption key would have to be sent out to everyone who needs to be communicated with. Each smart card would have a unique secret key. This gives each user with a unique card identity and no other communication system will know this unique ID, preventing fraudulent activity. If a system needs to authenticate a message, that system would have to get hold of that particular key. Hochfield et al. (1997) also shows how contact less smart card can be used for payment purposes. Financial applications (e-purse, loyalty schemes, credit/debit card) can be loaded onto a card. Electronic Airline Ticketing system is a good example of an application that can be loaded onto a contact less card. This card can be inserted into a smart card reader connected to a telephone line. A ticket can then be purchased online and the ticket details will be stored on the card. When arriving at the airport, the passenger can go directly to departures because there will be a contact less reader which gather ticket information and allow the passenger to board. Another example is the Automatic Fare Collection. A reader plugged into a telephone slot can renew a transport ticket. The ticket will be paid for by credit/debit card functionality and transportation credits will be loaded online to the card.

7.4 Cellular transactions

Smart cards and WAP (Wireless Application Protocol) are creating a big impact in wireless communications. WAP is a protocol that enables hand held devices (cell phones and PDA – Personal Data Assistant) to make use of the Internet. Nicholson (2001) indicates that smart cards play a role in encrypting data and a role in using digital signatures for authorizing transactions. Smart cards allow for safe transactions to take place within WAP. E-commerce normally makes use of public key structures. WIM (WAP Identity Module) makes use of smart cards for security over wireless networks. WIM makes use of cryptographic algorithms (RSA, elliptic curves, dynamic session keys), which are stored within the chip of the smart card. Private keys are used for client identification. A signature can be used with other identification data (PIN or biometrics). WIM can be implemented in three ways. The fist is the SWIM package, which allows the additional banking

services to be added to a cell phone SIM (only in WAP enabled cell phones). The next is a dedicated WIM card that can be used when making secured transactions. The last option is packaging WIM on a separate card that can only be used with duel-slot mobile phones.

8. EMV STANDARD

8.1 Introduction

EMV (Europay, MasterCard and Visa) is a standard specification given for smart banking. Three global card franchises (Europay, MasterCard and Visa) came together to produce the EMV standard for smart banking as indicated in Dreifus and Monk (1998:4). EMV specification provides technical infrastructure for smart cards and smart readers process credit and debit transactions. Dreifus and Monk (1998:41-44) continue to show that EMV can be divided into three levels. The first level gives a standard for the card and chip environment. The second level describes the terminal environment and how the terminal handles data and applications. The third level gives a standard on how the terminal and smart card identify each other. This level gives a standard on how the terminal can identify the correct application on the card. This level also gives a standard on the communications protocol between the terminal and the backend software, on how best to implement security standards. EMV is the most dominant standard in the financial world. EMV provides a common understanding on smart banking between merchants. Old OS on smart cards made use of a hierarchical structure, where data and programs are stored in a hierarchy. Dreifus and Monk (1998:119-123) explains the disadvantage hierarchical OS and how extremely limited they are. New smart card OS are making use of objects. Information is stored on the card in object form. This makes it easier to identify and manipulate data elements on the card. Larger and more complex programs can be developed using objects. EMV specifies that card OS must object orientated. This is an advantage for security, making use of encapsulation (confidential data and keys can be hidden). Dreifus and Monk (1998:166-171) also show that terminal software and hardware that process smart banking transaction must also be EMV compliant. Terminal and smart card applications must communicate synchronously. In multiplication environments it must be determined which application on the terminal must speak to which application on the card.

8.2 EMV implementation in Italy

Associazione (2001) explains how smart banking is being implemented in Italian banks with the EMV standard. Another advantage of the EMV standard is that banks used to have to process all their transactions online for security reasons, but with smart banking transactions can now be done offline with the same level of security. Italian banks can now introduce more services (e-commerce, loyalty, digital identity) with EMV compatible smart banking. Edwards (2000) shows that France was the first country to introduce smart banking, but they did not implement a standard. The UK started to take an interest in smart banking and was the first country to implement the EMV standard. The UK has taken the advantage of this standard and now is the world leader in smart banking. When Edwards (2000) was written, it was a vision to see EMV standard implemented around Europe and finally the world (international standard). This standard will be implemented over time in a few steps. VISA encourages this implantation by hoping to make all their smart card programs EMV compliant. There is an urgency to make all system and networks capable of carrying EMV information. Systems that are not EMV compliant will stand greater danger fraud. EMV will be able to be used with multiple application cards, which means that the same card can have smart banking functionality while also having other functionality like e-purse.

8.3 Authentication and verification

Heyns (1997) speaks about EMV96, an old implementation of EMV but illustrates some important information on EMV. EMV contains CAM (Card Authentication Method) functionality, which is used to determine if the card is genuine, or not. As previously shown smart cards can store security algorithms and digital signatures to aid in CAM functionality. EMV also contains CVM (Card Verification Method) functionality, which can be used to verify if the correct owner is using the chip. PIN codes can be stored in a secret zone of the chip and can be used for verification securely. This enables offline transactions to be possible because the PIN doesn't need to be obtained from the host system.

9. SMART CARDS IN SA

There are big opportunities in SA for new technology. Old legacy systems are being replaced by new advanced technology. With this influx of new technology, it makes it advantageous for smart card technology to be implemented. There is a shortage of technical skills in SA to maintain this new technology, but the focus on education should eliminate this problem. Morris (2000) illustrates a few areas where smart card technology can be implemented in SA. In SA there is a demand for cellular technology. Cellular technology makes a large usage of smart card technology, therefore creating more opportunities for smart cards. There is a difficulty in maintaining identity information of a person in SA (administration difficulties). Monitoring pension payments can be a nightmare. Smart ID's can be very beneficial in solving these problems. SA has a high percentage of poor/disadvantaged people, which unfortunately leads to high crime rate. Smart cards can eliminate the need for a person to carry large amounts of money. Smart banking offers high levels of security thereby preventing fraud. As can be seen from the above, there is a good market for smart card technology in SA.

10. CONCLUSION

From this paper it can be observed that there is a lot of opportunity for business implementing smart card technology. The examples illustrate how smart cards are making humans' lives easier. SA has enormous potential for the smart card industry. Opportunity is waiting for SA companies with the right infrastructure to handle smart technology. Smart card technology will be able to reduce fraud as well as help eliminate poverty (create more infrastructure) in SA. This paper also shows that computer hardware and OS (like Microsoft) are adapting to smart card technology. It is not too far into the future when smart cards will be used for banking instead of magnetic cards all around the word. The next question is: "Is the world heading to a single global currency?"

11. REFERENCES

- Ang J. (2000) Cashcard-Singapore National E-Purse (Cashcard Alternative to Cash), Smart Card Technology International (The Global Journal of Advanced Card Technology). Applications Section, 81-84.
- Associazione Bancaria Italiana (2001) National EMV Implementation, Smart Card Technology International (The Global Journal of Advanced Card Technology). Contents Section, 84-86.
- Didier JW. (2000) New Card on Campus (Impact of Campus Cards in Higher Education), Smart Card Technology International (The Global Journal of Advanced Card Technology). Applications Section, 64-68.

- Dreifus H. with Monk JT. (1998) Smart Cards (A guide to building and managing smart card applications), Canada, John Wiley & Sons, Ltd.
- Edwards A. (2000) Smart Cards You Can Bank On (A Look at the Migration to Smart Bank Cards in the UK), Smart Card Technology International (The Global Journal of Advanced Card Technology). Applications Section, 26-29.
- Heyns G. (1997) The Issues Facing Issuers and Acquirers Beyond EMV, Smart Card Technology International (The Global Journal of Advanced Card Technology). Chapter 2, 123-126.
- Hochfield B., Mitchell R. & Reid K. (1997) Revolutionary Payment Systems, Smart Card Technology International (The Global Journal of Advanced Card Technology). Chapter 2, 127-131.
- Hospital Bulletin Hull (2002) 'Smart Move' Smart Cuttings for September 2002, Cambridge, Smart Card Club.
- Hyperion DB. (1997) Smart Cards and the Internet (Smart Cards are the Link Between the Real and Virtual Worlds), Smart Card Technology International (The Global Journal of Advanced Card Technology). Chapter 2, 92-95.
- Ingenico (2003) The world leader in secured transaction systems [online] (cited on 15 May 2003) Available from <www.ingenico.com>
- Kavanaugh C. (2001) The Southern Oklahoma Physical Hospital Organisation (SOPHO) Smart Card System, Smart Card Technology International (The Global Journal of Advanced Card Technology). Contents Section, 119-120.
- Kendrick K. (1997) Electronic Commerce (The Role for Smart Cards), Smart Card Technology International (The Global Journal of Advanced Card Technology). Chapter 1, 60-64.
- Kingdon H. (1998) The Future of Smart Cards is with Multiple Application on a Card, Smart Card Technology International (The Global Journal of Advanced Card Technology). Chapter 2, 86-89.
- Fare Collection News (2002) 'San Francisco Bay Area Expands Six-Month TransLink Smart Card Trial' Smart Cuttings for September 2002, Cambridge, Smart Card Club.
- Gates KL. (1997) Use of the Eyes as a Biometric: Definitive Automated Identification Through Iris Recognition Technology, Smart Card Technology International (The Global Journal of Advanced Card Technology). Chapter 1, 38-40.
- Gray T. (2002) 'The Car That Locks Itself' Smart Cuttings for July 2002, Cambridge, Smart Card Club.
- Local Government IT In Use (2002) 'Smart Lunch' Smart Cuttings for July 2002, Cambridge, Smart Card Club.
- McMurtrie M. (2000) Tomorrows Transaction Terminals, Smart Card Technology International (The Official Publication of the Online Smart Card Exhibition), Technology Section, 106-107.
- Metro Travel (2002) 'At your service' Smart Cuttings for September 2002, Cambridge, Smart Card Club.
- Microsoft (2001) The Impact of Windows for Smart Cards on the Future of Business, Smart Card Technology International (The Global Journal of Advanced Card Technology). Contents Section, 109-111.
- Morris BS. (2000) Smart Card Developments In Southern Africa, Smart Card Technology International (The Official Publication of the Online Smart Card Exhibition), Applications Section, 55-57.

- Muir R. (2002) Identity Crisis? Smart Cuttings for September 2002, Cambridge, Smart Card Club.
- Nicholson B. (2001) Universal Mobile Commerce Starts To Get Real, Smart Card Technology International (The Global Journal of Advanced Card Technology). Contents Section, 57-61.
- Wayner P. (1997) Digital Cash: Commerce on the net (2nd edition), London, Academic Press Limited.
- Yli-Untinen J. & Mononen T. (1998) A Secure Key Management System for Payphone Cards with a Migration Path to an Electronic Purse System, Smart Card Technology International (The Global Journal of Advanced Card Technology). Chapter 2, 138-141.
- Zoreda, JL. With Oton, JM. (1994) Smart Cards, London, Artech House.