SMART CARD NEWS

NOVEMBER 1996

Volume 5
Number 11

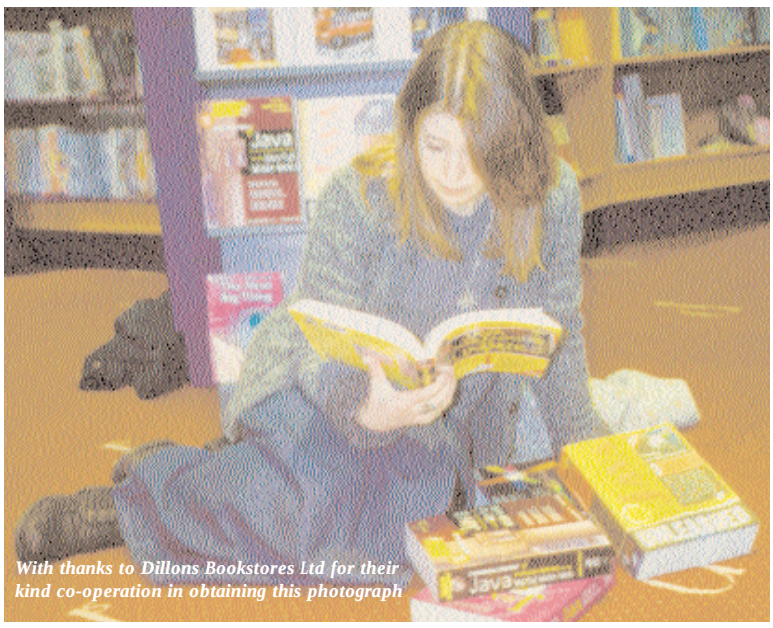
Sun Launches Java Card API for Smart Cards

Sun Microsystems' Java Card application programming interface (API) specification, announced to coincide with the opening of CarteS 96 in Paris last month, received an enthusiastic response from Smart Card industry leaders as enabling the first industry standard language and open API for Smart Card applications.

At the same show Schlumberger revealed their plans to introduce the first Java compatible Smart Card called Cyberflex. The card will have an SC49 Motorola 8K bytes EEPROM chip.

Java is a new software development platform and its significance to the Smart Card industry is its "Write Once - Run Everywhere" capability.

Continued on page 203



With thanks to Dillons Bookstores Ltd for their kind co-operation in obtaining this photograph

Smart Card News is published monthly by
Smart Card News Ltd
PO BOX 1383
Rottingdean
Brighton
East Sussex
BN2 8WX England
Telephone + 44 (0) 1273 626677 / 302503
Facsimile + 44 (0) 1273 624433 / 300991
email scn@pavilion.co.uk
ISSN 0967 196X

Patsy Everett
Managing Director
Jack Smith
Editor
Dr David B Everett
Technical advisor
Anna Ronay BA (Hons)
Editorial Assistant
Julie Barnes
Investigative Journalist
David Lavelle BA (Hons)
Graphic Designer

Editorial Consultants
Dr Donald W Davies CBE FRS
Independent Security Consultant
Peter Hawkes
Principle Executive
Electronics & Information
Technology Division
British Technology Group Ltd

Printed by Design and Print Ltd.
***Telephone* +44 (0) 1273 430430**

Visit Our Website!
http://www.smartcard.co.uk

Cards On the Cover
VisaCash / Taiwan *- Page 208*
Gemplus Public Key *- Page 206*
Pub Loyalty Card *- Page 212*
Schlumberger Smart Village Card *- Page 207*

Smart Card News - November 1996

Contents

Next Month:
Smart Card Tutorial
Integrated Circuit Card Standards
Specifications - Part 3

Sun Launches Java Card API

Continued from page 201

Applications created in Java can be deployed without modification to any computing platform from a Smart Card to a Personal Computer to a Mainframe computer. Applications, called applets, reside on the network in centralised servers and the network delivers the applet to your system when requested.

The size of a Java Applet varies, but typical size is around 1 - 2K bytes, including code and data. Given an 8K EEPROM on the first Java card this suggests that 4 - 6 applications will be immediately feasible.

Alan Baratz, President of JavaSoft, said Java was "leapfrogging the industry to take the concept of scaleability to a new level." He claimed: "Not only will Java Card applications run on any Smart Card, but Java programmers can use the same tools to develop applications for Smart Cards and pagers, note book and personal computers and fault-tolerant servers." He said that to date, Smart Card operators had written what were essentially proprietary applications that were not interoperable or portable.

The Java Card specification is available for download at http://java.sun.com/commerce.

Industry comment

Jean-Paul Bize, Vice President of Schlumberger Electronic Transactions, commented: "Java Card API is a breakthrough for the Smart Card industry because it opens the door for the development of new Smart Card applications from thousands of developers the world over. Applications will multiply, bringing the convenience and security of Smart Card transactions on a wide scale as the industry standardises on Java technology.

"Our research and engineering centre in Austin, Texas, worked closely with JavaSoft and others in the industry in the development of Java Card API, and we will introduce shortly Smart Cards that are Java-compatible."

"The Smart Card industry is clearly entering a new era with this announcement," declared Marc Lassus, CEO of Gemplus. "The increasing demand for open platforms on which to quickly develop Smart Card applications is proven. Gemplus has developed significant technology in the field of object-orienated card operating systems and is today totally supporting and endorsing the Java Card initiative. Combination of the hardware secure environment of the chip card and of Java's unmatched security features will rapidly improve being the ultimate solution to implement secure electronic commerce."

In Japan, Yukio Itakura, Senior Vice President, NTT Data Corporation, said the Java Card API offered exciting new potential that would lead to better solutions for their Smart Card customers. "We look forward to working together with Sun Microsystems to achieve optimal benefits for our Smart Card users," he said.

Mitsubishi Electric's Deputy General Manager, Koichi Maruno, commented: "It is clear that networked financial transactions will be a way of life for people in the near future, and there is no question that Java will be a key technology to make such systems really dynamic or interactive with proper security."

"Java Card API is a significant step forward in enabling fast application development without compromising embedded security," said George Maurel, Worldwide Smart Card Business Manager, Texas Instruments.

Peter B Gustafson, Executive Vice President of Visa International, said: "Java Card technology offers us and our member financial institutions new opportunities to reduce costs, improve time to market, and enhance application development productivity for chip cards with multiple applications."

Contact: Penny Bruce, *JavaSoft, USA -*
Tel: +1 408 343 1796.

France to Pilot an Electronic Purse

Groupement des Cartes Bancaires (CB), the French bank group which was responsible for changing all bank cards to Smart Cards at the end of 1992, making France the first country in the world to have a Smart Card banking system, is now turning its attention to an electronic purse.

A decision was taken last month to prepare a pilot scheme which will be largely transport-based but will include retail outlets in a town or city outside Paris.

The electronic purse card will be compatible with the EMV specifications. Hervé de Lacotte, a spokesman for CB said he could not yet say when or where the trial would be held.

Contact: Hervé de Lacotte, *Cartes Bancaires* - ***Tel: +33 (0)1 53 89 34 34.***

CarteS 96 Success in Paris

CarteS 96, held in Paris last month, finally threw off its reputation as a "French only" showcase for plastic card technologies and applications and, in this its eleventh year, became an international event with 48 per cent of the 120 exhibitors coming from outside France.

There was strong representation from Germany and the UK, and exhibitors from Austria, Belgium, Italy, Netherlands and Switzerland as well as from Israel, Korea, Japan, Singapore and the USA. The organisers claimed 130 new products, applications and systems on show, the most significant of the announcements perhaps being the Java Card Application Programming Interface (*see front page*).

The event was supported by the Federation of Electronic Industries (FEI) in the UK, the British Embassy and the French-British Chamber of Commerce. In addition the FEI and the British Overseas Trade Services jointly sponsored a delegation of British business representatives to the exhibition, and the French-British Chamber of Commerce held a British luncheon to encourage exchanges between French and British business representatives. Nine UK companies exhibited at the show, but some key players were noticeably absent.

A highlight of the show was the first SESAMES awards (*see page 220*) for the best innovation and best application which attracted 34 entries from 13 countries around the world. SESAMES '96 was officially sponsored by Eurocard/MasterCard and supported by the UK Smart Card Club and the Smart Card Forum in Germany. The awards were presented at the gala evening held at the Paradis Latin where delegates and exhibitors were entertained to dinner and a cabaret show as only the French can stage.

The comprehensive conference programme ranged over Smart Cards, security, health, telecommunications, electronic payment, components, electronic commerce, PC cards, operating systems and a new section, Innovation '96 at which SESAMES' nominees presented their new products.

Advanced Chips on Show

Just how fast Smart Card technology is advancing was evident from the number of new products being announced for contact and contactless cards by the major chip manufacturers.
SGS-Thomson, for example, was showing two new devices aimed at contactless and very high security applications.

The ST16RF42 intended for use in high volume contactless and contact applications is a highly secure serial access microcontroller with 16K bytes of user ROM, 1.5K bytes of System ROM, 384 bytes of RAM and 2048 bytes of EEPROM. Both the user ROM and EEPROM can be configured into two sectors, with a user defined Memory Access Control Matrix governing memory accesses between different sectors.

Specifications for contactless applications include 3V operating voltage, 13.56MHz operation, 106kbits data transfer and direct connection to the external antenna via a built-in radio frequency (RF) interface circuit. Amplitude modulation is used for transfers from the reader to the card and load modulation for transfers from the card to the reader. In the contact mode, the ST16RF42 supports internal clock frequencies of up to 5MHz and operates over an extended supply range of 2.7V to 5.5V, as well as complying with ISO 7816 standards for contact assignment and serial access.

Another new product, the ST19CF68 is the first of a new family, ST19XYZ, built with 0.6 micron CMOS EEPROM technology that allows large memory sizes to be offered as well as very fast MAP co-processors and even custom logic blocks. Features to enhance security include a 64 byte block of protected One-Time Programmable memory and the ability to flash erase the entire contents of the RAM and EEPROM areas if there is an attempt at unauthorised access.

Contact: Jean-Paul Thomasson, *Smart Card Products Marketing Manager, SGS-Thomsom Microelectronics* - ***Tel: +33 (0)4 42 25 87 29.***

Atmel Corporation introduced the AT89SC series of secure microcontrollers for Smart Card applications. Compatible with the industry-standard MCS-51, these feature the ISO 7816-compliant Smart Card serial interface. All members of the family include on-chip RAM, Flash and EEPROM memory with a choice of capacities to suit all types of application. The reprogammable Flash memory gives flexibility in both design and production. On-chip security features include power-down protection, low and high frequency filters, unique serial number and transport code.

Christian Fleutelot, Atmel's Product Manager for Smart Card Microcontrollers, said: "The on-chip Flash program memory makes the AT89SC series unique on the market. These products respond to the need for advanced functionality, flexibility and high security in the emerging range of added-value Smart Card services."

Contact: Christian Fleutelot, *France -*
Tel: +33 (0)4 42 53 61 88.
Website at http://www.atmel.com

Motorola claimed it was the first major chip manufacturer to develop a "contactless" Smart Card microchip with security levels that match those of contact-based cards. In the new family will be the SC80 with 4K bytes ROM and 1K bytes EEPROM, the SC81 with 16K bytes ROM and 4K bytes EEPROM and the SC82 with 20K bytes ROM, 8K bytes of EEPROM plus Crypto.

Contactless memory cards offer significant benefits in a variety of areas, notably public transport, but have to date been restricted to applications with limited security requirements, said the company, and their new chip paved the way for higher security electronic purse applications, such as those being piloted by MasterCard and Mondex, which could now in theory be held on multi-function contactless Smart Cards.

Mike Inglis, Motorola's Worldwide Smart Cards Operations Manager, commented: "Using a card based on the new chip, a commuter will be able to load his Smart Card with money at an ATM or down a telephone line and use the same card as a contactless travel pass, giving huge savings in time and effort.

"The combination of contactless technology with the security features required by financial institutions is very powerful," he explained. "We have discussed the concept with transport authorities and card issuers around the world for some time, and they have expressed tremendous interest. Now we are making that concept a reality."

Motorola estimates there are approximately 20 billion commuter transactions per year worldwide, most of which could be handled by the new technology, which gives a market of "enormous potential" says Inglis.

"Industry analysts predict that contactless will be the fastest growing type of card in the global Smart Card market over the next five years," he said. "Motorola intends to be the leader tomorrow in contactless, as we are today in contact-based Smart Card microchips."

Motorola also unveiled two new chips which they believe to be the fastest encryption chips currently available. The "fast crypto" chips can perform complex encryption functions at speeds up to 200 times faster than conventional Smart Card devices.

The company says they have already been selected as the basis for an electronic payment system by Schlumberger for a new range of high-performance Cryptoflex Smart Cards performing RSA public key cryptography, and are currently being evaluated by Mondex.

Both chips incorporate the latest 1024-bit flexible modular encryption unit, which can perform complex cryptography algorithms in the shortest time currently published by any crypto-controller manufacturer, said Motorola.

The fast crypto chips are designed for electronic commerce and electronic purse applications and are named the M68HC05SC49A (SC49A) and the M68HC05SC50 (SC50).

The SC49A chip is an 8-bit microcontroller with 1024-bit modular arithmetic co-processor, 20K bytes ROM, 4K bytes EEPROM, 896 bytes of RAM and an operating voltage of 3-5V. The 1024-bit modular encryption unit can also efficiently handle 512 and 786 bit keys.

The SC50 chip uses the same configuration but incorporates 8K bytes of EEPROM which allows cards to undertake more than one application, for example, a single card could be used as a credit and debit card, electronic purse and loyalty card.

Contact: Kathleen Reid, *Motorola, Scotland -*
Tel: +44 (0)1355 565447

Siemens unveiled its new controller family, the SLE44C160S, with 16K bytes of EEPROM, 15K bytes of ROM and 256 bytes of RAM on a die size of 15mm².

Security functions include additional barriers against potential hackers, special protective functions for the EEPROM cells, encryption of the ROM addresses and measures to prevent simulation of the Smart Card IC. The range of non-volatile memories begins with 7K bytes of ROM and 1K byte of EEPROM; all the chips have 256 bytes of internal RAM.

Another chip, the SLE44CR80S crypto controller is equipped with a 540-bit co-processor for rapid processing of asymmetrical crypto algorithms. Siemens says this is the first time a crypto chip with 17K bytes of ROM, 8K bytes of EEPROM and 256 bytes of internal RAM as well as a coprocessor has been available on a chip area of 15mm². The crypto controller is designed for applications such as banking, electronic commerce via the Internet and high security applications.

Power consumption is typically 3 mA when operated at 3V. In "sleep mode" without an external clock applied the current drain is said to be reduced to as low as 35 A. The chip can be operated at 3V and 5V and frequencies of up to 5MHz (7.5MHz on request) without external clock dividers.

Siemens says the coprocessor offers an execution time of 220ms for an RSA 512-bit standard encryption or of 450ms for 1024-bit RSA employing the commonly used Chinese Remainder Theorem.

Contact: Edith Lalliard, *Siemens, France* ***- Tel: +33 (0)1 49 22 43 18.***

From chips to cards

Schlumberger announced it is using one of the new high-performance chips from Motorola in its new Cryptoflex card to provide 1024-bit key RSA cryptography to deliver high security for authorising transactions such as electronic commerce across networks, or confidential storage of personal data such as health records.

"Cryptoflex cards give application developers the means of adding a unique digital signature to any electronic transaction," notes Eric Gaignet, Schlumberger's Marketing Manager.

"We see this capability as a catalyst for new generations of card applications, particularly for securing commercial transactions or communications across Internet or Intranets."

Contact: Isabelle Ferdane-Couderc, *Schlumberger Electronic Transactions* ***- Tel: +33 (0)1 47 46 66 98. Fax: +33 (0)1 47 46 68 66.***

Gemplus Public Key Cards

Gemplus was showing the first cards in its GPK (Gemplus Public Key) range with digital signature and verification capabilities for secure applications on the Internet, corporate MIS transactions, identity, healthcare etc.

The GPK2000-s has signature and verification capabilities and 2,000 bytes of free memory, while the GPK 2000-sp has additional "digital envelope" capabilities. This is a mechanism to implement data privacy in which the card internally generates a random key, encrypts the key with the other parties public key and sends it, and then is able to encrypt data with DES and this random key.

Further cards in the GPK family will be available next year - first the GPK4000 with 4K bytes of memory and 1,024 key length, followed by the GPK8000 which will be the same as the GPK 4000 but with 8K bytes of memory.

A GPK development kit with windows-based software, readers, cards and manual is available to help customers develop an application.

Features and performances:

	GPK2000	GPK4000 (Q2-97)	GPK8000 (Q4-97)
Application memory	2K bytes	4K bytes	8K bytes
Memory structure	according to ISO 7816-4		
Passwords	up to 8 passwords per directory		
Serial number	unique, 64 bits		
Comms protocol	T=0	T=0	T=1 optional
Speed of comms	up to 115 kbits/s		
RSA signature / 512b	150ms	85ms	85ms
Chinese Remainder Theorem	Yes		
RSA key length	512 & 768	1,024	1,024
DSA key length	512		
Hash functions	MD5, SHA1		
Secure messaging	DES and triple DES		

Contact: Flavie Gil, *Gemplus* **- *Tel: +33 (0)4 42 36 56 83. Fax: +33 (0)4 42 36 51 17.***

Philips Smart Cards & Systems revealed that its DX Smart Card - the first to feature an on-board RSA public key cryptographic algorithm - is to be the basis for a DX family. DX Plus, with 8K bytes EEPROM, is being developed with expanded cryptographic facilities, and Super DX is in preparation, on the same silicon platform.

Both cards will use the new Philips Semi Conductors 83C858 chip with an arithmetic co-processor. The DX ROM code is to be ported onto this component.

Philips says the improved performances achieved by DX Plus over DX are so impressive that in normal mode of operation, DX Plus reaches the speed achieved by DX only in Chinese Remainder Theorem mode. DX Plus will be available in the first quarter of 1997.

The French company also announced that certification had been received for the Smart banking card for the UK with an embedded debit-credit application developed according to the UKIS 2.0 specification issued by the UK Association for Payment Clearing Services (APACS). The card also complies with VIS 1.2 specification of Visa and EMV 2.0.

According to Philips, each transaction is electronically signed and the signature sent back to the issuer host. A risk management analysis is performed by the card before accepting to process the transaction off-line or after a host authorisation.

The card will be tested in field trials before the national roll-out planned for autumn 1997 when all 60 million UK bank payment cards will start to change from magnetic stripe to chip cards.

Philips says this first generation card is implemented on a "small" chip with 1K bytes of EEPROM, but a full range of cards is planned with memory sizes up to 8K bytes. One version will be based on a component allowing public key cryptography to support VISA Cash.

The card will be sold by DelPhic Card Systems, the joint venture between De La Rue Card Technology and Philips Smart Cards & Systems.

Contact: André Jacques Selezneff, *Philips Smart Cards & Systems* **- *Tel: +33 (0)1 53 62 51 54. Fax: +33 (0)1 53 62 51 03***

The Smart Village

Schlumberger came up with the imaginative concept of The Smart Village to present its activities and development strategy. As a turnkey solutions group, Schlumberger was able to use the concept not only to emphasise its expertise in Smart Card solutions but draw them together in a community infrastructure - a vision of the future!

Hubert Vigneron, Director of Marketing, explained: "Schlumberger is currently the only company in the industry that provides complete turnkey solutions for telecommunications, transport, banking and retail, healthcare and network access, as well as retail petroleum and parking systems. In that sense, the company has a key strategic position in the emergence of the Smart Village."

It is also a clever marketing platform. In the Smart Village scenario we see cardholders obtaining loyalty points, paying for goods at a point of service terminal, settling a restaurant bill at the table using the waiter's portable card reader, using an electronic purse at a snack vending machine, obtaining a parking ticket at a pay and display machine and buying a travel ticket at a ticket vending machine.

Communication is covered by cardholders using a pre-paid phonecard, a private site payphone, a GSM phone (which contains the Smart Card Subscriber Identity Module) and at a GSM public payphone. Other components are making a payment on the Internet from a home PC, using a healthcare card at the doctors and obtaining fuel at a filling station.

These activities are related not only to Schlumberger's Smart Cards but also to their Smart Card payphones, health management terminal, fuel dispenser, point of services and remote payment terminals, GSM payphones, ticket vending machines and pay & display machines.

Gemplus, of course, came up with the idea of a "Smart Card City" which it created in the French town of La Ciotat in 1994 to demonstrate applications in public transport, shops, cinemas, companies and homes. Schlumberger have taken their concept into the new dimension of strategic marketing, including a colour leaflet which can be mailed to potential customers.

Contact: Isabelle Ferdane-Couderc,
Schlumberger **- *Tel:+33 (0)1 47 46 66 98. Fax:+33 (0)1 47 46 68 66.***

VISA Cash in Taiwan

Visa has announced the launch of a VISA Cash pilot in Taiwan in partnership with eight Taiwanese banks, and says the pilot will mirror the recent VISA Cash launch in Hong Kong, eventually enabling the two schemes to join to create the first chip-based stored value card programme with cross-border compatibility.

The Taiwan pilot is being launched in partnership with ChinaTrust Commercial Bank, Chung Shing Bank, Citibank, Far Eastern International Bank, Grand Commercial Bank, International Commercial Bank of China, Standard Chartered Bank and Taishin International Bank. Each bank is to issue 200,000 disposable VISA Cash cards in values of NT$ 1,000 (US$ 36) or NT$ 500 (US$ 18) in the first phase.

Plans call for some 5,000 card acceptance devices to be installed at key retail outlets such as convenience stores, food courts in department stores, fast food chains and supermarkets. In subsequent phases, reloadable cards will be issued.

David Chan, Director of VISA Cash, Visa International Asia-Pacific, said: "While the programmes initially will evolve independently in Hong Kong and Taiwan, they will do so in parallel so that, three or four years from now, they can be merged to offer cross-border usage.

"Taiwan is an ideal market for of a VISA Cash pilot as the average Taiwan consumer spends NT$ 200,000 (US$ 7,143) annually on day-to-day necessities," said Chan. "With the numerous advantages of VISA Cash and the support of our member banks, we believe that the card will change consumer payment behaviour and become a popular alternative to cash transactions in the future."

Hong Kong success

He added that the Hong Kong pilot, launched in August, has already sold more than 100,000 VISA Cash cards and recorded more than HK$3 million (US$ 0.387 million) in transactions. "The VISA Cash programme there has surpassed all expectations to date," said Chan.

Contact: Colin Baptie, *Visa International, UK -* ***Tel: +44 (0)171 937 8111.***
Fax: +44 (0)171 937 0877.

Support in UK for Smart ID Cards

Identity cards are popular with the UK public according to a new survey which reveals that the vast majority would be happy to use a Smart Card as a driving licence, ID card, passport and social security benefit card. Also, three out of four people would be willing for the card to contain their fingerprint.

The survey, commissioned by Smart Card chip manufacturer Motorola, was conducted by MORI, which interviewed 1,037 adults face-to-face and a further 100 top executives over the phone.

The findings show that 73 per cent would accept a Smart Card as a driving licence, 70 per cent as ID cards, 64 per cent as passports and 61 per cent as social security benefit cards. Fingerprint identification to ensure Smart Card security was approved by 76 per cent while 53 per cent said they would happily vote electronically - a higher proportion than currently vote in local elections.

Motorola says that the figures show that the British people are "more willing to use new technologies in their everyday lives than is currently believed."

Left behind

However, almost half of the population fear they are being left behind in terms of understanding new information technologies. Although 85 per cent have heard of the Internet, three quarters do not know how to connect to it. Only 9 per cent of the population use the Internet on a regular basis and 43 per cent do not use on a regular basis any main IT items currently available such as mobile phones, computers, electronic organisers or pagers.

"The British population is ready for the application of new technology to everyday life but this survey shows that we are still a nation of IT 'haves' and 'have-nots'," said Mike Alderson, Chairman of Motorola. "If the information society is to become a reality, we must make sure that we make IT work for everyone."

The survey, Prepared for the Future?: The British and Technology, is available from Motorola Corporate Communications Division - ***Tel: +44 (0)1753 575555*** *or visit the Motorola web site a****t http://www.mot.com***

Amex Enters Smart Card Arena

American Express is to enter the Smart Card arena in a venture with IBM to introduce ticketless travel on American Airlines.

Early next month the two companies will start testing an American Express Corporate Card using IBM Smart Card technology for use with the airlines' gate readers now installed in 21 US airports, which account for about 70 per cent of the airlines' passenger boardings.

Travellers will be able to proceed directly to the gate after showing identification at the airport. At the gate, the traveller inserts the Smart Card into the reader, receives confirmation of seat assignment and is ready to board the aircraft.

At the recent International Air Transport Association (IATA) Passenger Services Conference in Los Angeles, IBM demonstrated how Smart Cards can enhance the ticketless travel process - from reservation to boarding. The steps include:

* the passenger makes a reservation through the Internet or other on-line service or through a travel agency.

* the passenger then downloads the ticket confirmation number to a Smart Card via personal computer with Smart Card capabilities or at an airport self-service kiosk.

* The passenger then checks in, using the Smart Card at the airline desk or kiosk, and then proceeds to board, using the enhanced gate reader.

In the pilot, American Express will issue fully-functional Corporate Cards, featuring IBM's Multi-function Smart Card (MFC) technology, to a select group of employees of both companies.

The product represents the first commercial Smart Card application by American Express which says it will pursue multi-function applications that will speed travellers past check-in points at airports, hotels and car rental agencies.

Contact: Christine Levite, *American Express, USA* - ***Tel: +1 212 640 3382. Deborah Siegel,*** *IBM* - ***Tel: +1 914 642 5377.***

Smart Payphones for Private Sites

Schlumberger has announced its new Grafit Collection of purpose-designed Smart Card payphones for private sites.

Grafit phones are available with plastic or metal housings for light or heavy use, and in three functional variations, for use indoors such as in shops or restaurants and in semi-exposed sites such as stations or airport terminals.

Schlumberger says the flexible software architecture offers the ability to implement advanced real-time security checks and download new application programs over the networks. Extensive memory space has been left available for upgrades so that operators and site owners can take advantage of developments such as electronic cash as soon as they arrive. The phones can accept phonecards or any Smart or magnetic stripe bank card users have in their pockets.

Contacts: Nicolas Poirier, *Schlumberger Electronic Transactions, France* - ***Tel: +33 (0)1 47 46 59 34. Fax: +33 (0)1 4746 68 66. Sally Chew,*** *Schlumberger Measurement & Systems Asia, Singapore* - ***Tel: +65 740 0857. Fax: +65 742 6484.***

First UK Visa Cash Pilot

Visa International have announced that the City of Leeds will be the location for what may be the only UK trial of Visa Cash. The pilot is due to start late in 1997 when Leeds consumers will be able to use reloadable Visa Cash cards at a wide variety of retail outlets.

The six financial institutions working with Visa to impliment Visa Cash in the UK are as follows; Abbey National, Barclays Bank, The Co-operative Bank, Halifax Building Society, Lloyds TSB Group and The Royal Bank of Scotland. If the pilot is a success Visa Cash will be rolled out nationally.

Contact: Colin Baptie, *Visa International, UK* -
Tel: +44 (0) 171 937 8111.
Fax +44 (0) 171 937 0877.

Vice Chair for Mondex International

Ms Janet Hartung Crane has been appointed Vice Chair of Mondex International, the London-based international electronic cash card payment organisation.

Prevention is Better Than Cure

ODS R. Oldenbourg Datensysteme GmbH of Germany has developed a new medical chip card system based on the principle "prevention is better than cure." Named the BodyCare Health Card it is designed to enable easier communication between health care providers and patients.

The advantages for the patient are primarily the ability to keep track of diagnosis and medication. The card allows the patient's history to be quickly related to the doctor, leaving more time to discuss the current concerns. It can help to prevent over exposure to radiation from X-rays and unnecessary expensive double examinations. ODS suggest this function means "each individual can actively contribute to reducing health care costs."

Patients with conditions such as allergies, haemophilia or heart problems can feel comforted by the knowledge that the card means their needs will be more easily recognised. Therefore, should emergency treatment be necessary, the process is both simplified for the doctor and made safer for the patient.

Concern about the privacy and safety of medical records is addressed with an extensive security system including a secret PIN, data encryption and a photograph of the card owner.

The BodyCare system consists of two kinds of Smart Card. First, the BodyCare Card which belongs to the patient and contains their medical records. This information is held in several categories with different levels of access authorisation. Second, the authorisation cards which are held by doctors and pharmacists. These cards determine which information the holder is allowed to read. For example the pharmacist cannot read the diagnosis entered by the doctor.

The system is designed to be open, which allows further functions, both medical and other, to be added, for example, an area could be opened for diabetes or an application could be developed to use BodyCare with public transport. At present the system still has project status.

Contact: Eva Keil, *Marketing/Communication, ODS -* ***Tel: +49 8165 930 163. Fax: +49 8165 930 202***

AFC Demo Centre in London

AES ProData, which supplies Automatic Fare Collection (AFC) systems worldwide with Smart Cards as the re-usable fare media, has opened a demonstration centre in central London to display a range of their equipment.

The centre was originally planned as part of a bid for London Transports Prestige project. However a partner pulled out and the bid did not take place. The centre was then completed by AES Prodata as a means of demonstrating both their capabilities and the possibilities offered by Smart Card technology to the transport industry.

The first machine on display is the Excelsys which issues permits to travel. This system allows the traveller to use their contactless Smart Card as cash and to load value from a credit card at the point of sale. The Excelsys provides the customer with a paper ticket.

Mike Eastham, Senior Systems Engineer, explained that most people still like to see the physical manifestation of their purchase. The contactless system also allows the customer to obtain a statement of their last 10 transactions.

Stephen Bracegirdle, Managing Director of AES Prodata, described Excelsys as the "only add value contactless system" available. It is not currently in use, but AES Prodata revealed that interest has been expressed by various train companies who see the system as a possible "queue buster." Effectively the customer would only have to queue to buy or load up their Smart Card. However if the customer has a credit card then theoretically, once a card holder, they would never have to stand in the queue or deal with a human vendor again.

The next system on display is called the Validator or Platform Processor which is currently being used in Hong Kong. It is a contactless system and works in a similar way to the London Underground ticketing system.

However rather than putting your ticket into the machine and pushing through a gate you simply hold your card toward the reader and you are then 'validated' to travel. The card reader terminal tells you both the amount currently on the card and the amount that has been deducted for the journey.

The contactless card also works from within a wallet or pocket, clearly saving the traveller the hassle of searching for their ticket and juggling luggage through electronic gates.

Hong Kong project

In Hong Kong the card reader deducts the maximum fare and then reimburses the traveller on exit according to their actual journey. SCN asked what would happen if the card holder had insufficient value on their card to travel. Stephen Bracegirdle explained that a direct debit agreement is one option. Should the customer's card value reach a certain pre-agreed level value can be automatically added to the card, debited from the customers bank account. Stephen told SCN that each card reader can allow sixty people though per minute.

Currently, in Hong Kong there are 5,000 card reader terminals in use on buses, ferries, light and heavy rail. An estimated three and half million cards will be issued by the end of 1997.

The demonstration centre also displays systems designed for use on buses which provide an equally speedy service. The driver punches in the desired destination, the traveller then holds their contactless card toward the reader. The terminal is able to read the card in under 200 milli-seconds and a paper ticket is immediately issued. This system is currently on trial in Kent, where the second

phase of cards has recently been issued.
Stephen Bracegirdle explained the systems advantage for bus drivers. A Wireless LAN (Local Area Network) operates in the depot and, as the driver enters the depot, data is automatically "downloaded" from the bus. This allows the driver more time behind the wheel, bypassing the signing on and off process.

The TP 4000 also on display separates the bus console, card reader and ticket issuer. It was specifically designed for London's requirements and includes a portable card reader for inspectors.

The final system on display is the EPOS Mark 2 Positron terminal, 1,900 of which are currently in use in London's information centres, news and travel agents. The terminals are designed to issue tickets and use a contact Smart Card as security. All data is stored on the Smart Card, therefore even if the terminal is damaged the data is safe. Stephen Bracegirdle described the machine as "the bridge between Smart Cards as ticket and payment means".

The terminal can issue traditional tickets or use the Smart Card as a ticket which in effect allows the gradual implementation of Smart Card technology.

Asked about the future of Smart Cards in transport, Stephen suggested that we will probably see the transport function embedded within individual Smart Transport Cards and multi-application cards. The choice, he predicted, will be the travellers.

The demonstration centre will remain in London until December and will then be moved to an, as yet, unrevealed new location.

Contact: Janet Taylor**, AES Prodata - **Tel: +44 (0)1204 371372. Fax: +44 (0)1204 370567. E-mail aes@provider.co.uk.

Pub Loyalty Card

The Samuel Platts pub (part of Greenall Brewery), near the Old Trafford sports ground in Manchester, UK is using a Smart Card system from Smart Card International to help on match days.

The Smart Card is issued to regular drinkers. On busy football match days the system can allow only card holders into the pub. The card is loyalty based and holders are awarded a point for visiting the pub. The card is inserted into a card reader which shows the card holders name and number of points accumulated. At the bar the card gives the customer a discount on purchases and can also be used as an electronic purse. The cards, readers and chips, (2 Kbyte memory) are all supplied by Gemplus.

The scheme was introduced in August 1996 and has been judged a success with approx. 1,000 cards issued to date. The scheme is set to continue with a new card being introduced each season. Bob Cuthbertson of Smart Card International told SCN that there are plans to extend the system to include the pub's car parks. The card would be used to operate the barrier, thereby controlling use of the parking space.

The system is beneficial in a number of ways. It allows the landlord/lady to keep track of their regular customers and to target them with promotions or special nights. It helps to control access on match days which have a reputation for becoming troublesome. Additionally the system reduces the need to carry money and controls cash shrinkage.

SCN asked Bob Cuthbertson if any other pubs or breweries had shown an interest in the system. The answer was a clear yes. One example of interest is the systems recent sale to a leisure group based in Preston who have seventy pubs. There are also a number of similar schemes running in the South of England.

Contact: Bob Cuthbertson, John Gallagher *Smart Card International, UK* - ***Tel: +44 (0) 1482 650999. Fax: +44 (0) 1482 652271***

Smart Cards in Mexico

Schlumberger Electronic Transactions has acquired an 80 per cent interest in a company to be created with its partner, Printer, Mexico's leading magnetic stripe card manufacturer and a key supplier to Mexico's banks and telecommunications companies.

Eric Claudel, Director General of the joint venture, Schlumberger-Printer, based in Mexico City, said: "Adding chip technology to our manufacturing capability will accelerate our growth substantially, tripling card output (currently at 20 million cards a year) within two years and enabling us to address the extensive deployment of Smart Card technology planned by Mexico's government, banks and telcos."

Mexican banks have adopted the VISA Cash specifications for their next generation Smart Card-based payment cards and Schlumberger-Printer says it will supply Smart Cards to Banco Bilbao de Viscaya for field trials of the new stored value payment cards next year, and to major pilot projects to follow.

Schlumberger-Printer is involved in major Smart Card projects for the Mexican government including the Pase programme involving the issue of millions of Smart Cards for health, social security and welfare purposes to most of Mexico's 100 million inhabitants. The government also plans to introduce a vote card as part of a campaign to eliminate election fraud.

Schlumberger-Printer SA de CV, is based at Trigo 129, Col Granjas Esmeralda, CP 09810 Mexico D.F.

Contact: Eric Claudel - Tel: +52 5 582 1540. Fax: +52 5 670 8563.

Mondex in New Zealand

Westpac and Trust Bank started in-house trials of the Mondex electronic cash payment system in staff cafeterias in Christchurch and Wellington last month.

Harry Price, Chief Executive of Westpac and Trust Bank, said the cafeteria in Christchurch could handle four Mondex transactions a minute, much faster than an EFTPOS system. Over 90 per cent of eligible staff are using the card and the cafeteria is already receiving around the same number of payments from the cards as in

traditional cash. Staff use the special Mondex-capable telephone in the cafeteria up to 30 times a day to download cash from their bank accounts to their card. About NZ$8 (US$5) is downloaded each time. The trial in Wellington head office involves over 300 staff.

Last July, New Zealand's six major banks purchased the New Zealand Mondex franchise and expect to introduce a public trail within 18 months.

Hitachi Data Systems provided key technology, including the Mondex chip, balance readers, electronic wallets and systems management for the trials, and Michael Keegan, Chief Executive of Mondex International, said the trial had set a record for the speed with which a bank had moved from accepting the Mondex concept to introducing the electronic cash.

Contact; Takako Yamakura, *Shandwick USA* - ***Tel: +1 212 420 8100.***

Smart Card Plant in Brazil

Solaic, the Smart Card manufacturing subsidiary of French Groupe Sligos, and Daruma, a leader in the payphone market, have formed a joint venture in Brazil to manufacture memory and microprocessor cards at a local plant starting in 1997.

The new company, called Solaic do Brazil, is owned 51 per cent by Daruma and 49 per cent by Solaic. Based in the state of São Paulo, the plant is to be equipped with technology to make microprocessor cards for GSM and bank card applications as well as with Solaic's proprietary MOSAIC technology for the production of phonecards.

Contact: Boris Eloy, *Solaic-*
Tel:+33 (0)1 49 00 9633

Movie Gold Card

A Smart Card system for movie theatres has been developed by CardLogix, the Costa Mesa, California-based provider of chip transaction cards. Called the Movie Gold Card, it can be used to purchase tickets, refreshments and related products and services either at an individual or chain of theatres.

The card has a preset value, for example US$ 65, and users simply insert the card into a self-serve card reader/kiosk and using a touch screen within the kiosk can specify the number of tickets they wish to deduct from the card as well as the desired film and show time. The reader then approves the purchase, deducts the value from the card and prints out ticket(s) for admission at the requested time.

CardLogix has also developed Movie Magic software for use with the touch screen and reader/kiosk allowing the customer to preview current and future attractions, buy merchandise and purchase additional cards.

Emil Nastri, Vice President of CardLogix, said: "The card adds convenience and a sense of personal treatment for each moviegoer and builds loyalty and business for the theatre." He added that the system can track the type of movie most often viewed by a customer and issues a credit for similar-subject video rentals at a co-operating merchant.

"This is a powerful marketing tool that theatres as well as their business partners can use to profile the market and increase business in a targeted way that customers will appreciate," he said.

The company is issuing development kits to customers with Movie Magic software for use with the card so that they can customise their system kiosks to fit their individual market needs.

CardLogix says that kiosk manufacturer RTC and reader manufacturer American Magnetics are prepared to support the system and make kiosks and card readers available.

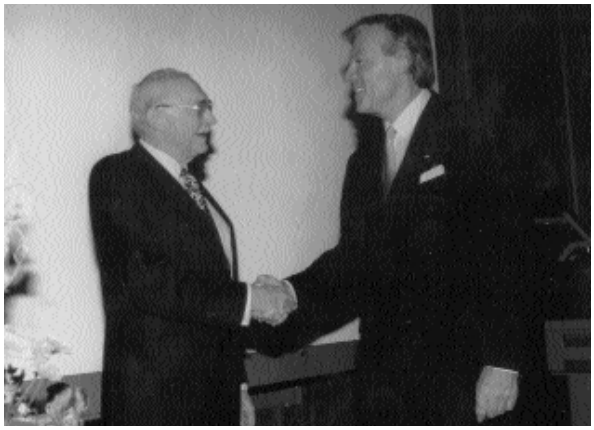
CardLogix was founded in 1995 to develop advanced chip card solutions, including Smart Cards and their patented VaultCard products.

Contact: Emil Nastri or Art Krause, *CardLogix* - ***Tel: +1 714 437 0587*** *or at* ***www.cardlogix.com***

Banksys Sells Proton World License to American Express

Under terms of the agreement, American Express gains the right to implement multiple pilots in the next year using Banksys' Smart Card technology, including Proton, its internationally renowned electronic purse that is now rolling out on a national level in Belgium.

Smart Card Pioneers Honoured



Two pioneers of Smart Card technology have been honoured with the award of the Eduard Rhein Foundation 1996 technology prize worth DM 200,000.

Jürgen Dethloff and Roland Moreno received the award from Hans Zehetmaier, Bavaria's Deputy Chief Minister and Minister for Education, Culture, Science and the Arts at a ceremony attended by 250 scientists from all over Europe in the Hall of Honour at the Deutsches Museum in Munich last month. The award was "in recognition of the lifetime achievement of two men whose contribution has been decisive to the success of this new medium."

Mass Production of IC Card Readers

Nam Tai Electronics, Inc has announced that it has shipped the first mass production of integrated circuit (IC) card balance readers to a European bank under order from a large Japanese OEM customer.

This year Nam Tai expects to ship between half a million and one million IC card readers to a number of banks and credit card companies, with a substantial increase in orders expected in 1997.

Contact: Wendy Wiseman, *Nam Tai Electronics* ***- Tel: +1 604 669 7800. Fax: +1 604 669 7816.***

Smart Cards to Defeat Hackers

Siemens has launched a Smart Card-based security system to prevent hackers from accessing private telephone networks and running up large bills by making long-distance calls, communicating over the Internet or selling access numbers to third parties who then sell on the illegal time.
Recent research shows that illegal access to an organisation's telephone system is costing British business millions of pounds of a year.

The solution from Siemens is called SecureCall, a voice processing application which prompts employees to enter an ID followed by a PIN number and a unique real-time passcode (which changes once every minute) displayed on a small LCD window on their Smart Card. Security servers throughout the network then validate the passcode to either allow or deny access. If access is approved, the application then asks the caller to enter the destination telephone number they wish to call. Once confirmed, the application initiates the call and releases the caller to ringing.

Barry Hannam, Managing Director, Siemens Business Communication Systems, explained that with growing concern over telephone hacking, many organisations have been cautious about giving remote users access to the corporate telephone network. But, with SecureCall, organisations can control who has access to their telephone systems and private networks. Travelling employees or staff working at home can dial into the voice processing server and use the features of the telephone system, including making long distance calls.

"With many organisations using private and virtual private networks, remote users will now be able to access them and so reduce the cost of long distance telephone calls," he said. "SecureCall ensures that the caller never gains access to the dial tone and as a result, the problems inherent with most telephone security devices are overcome."

Further security options include Call Barring, Call Back and Call Logging. Call Barring means that the system can be configured to prevent authorisation to certain call users and particular destinations, such as cellular and international calls.

Call Back makes it possible to control costs to a higher degree. When a user has accessed the network, Call Back requires the user to enter the number they are calling from as well as the number they wish to dial. Once the application connects the call, it will call back the original caller. Call Logging provides the ability to log call details enabling calls to be charged back to cost centres.

Research findings

Telephone hacking is costing British business millions of pounds a year, according to research conducted by Benchmark Research and sponsored by Siemens.

The report, based on 300 interviews with senior representatives from Times Top 500 organisa-

tions, found that the majority of UK organisation are unaware of the problem of telephone hacking, have no idea how much they would lose through fraudulent calls or system misuse, yet all believed the crime would increase over the next year.

"Despite numerous security alerts from the telecoms industry, few companies have heeded the warning and most remain oblivious to the problem and unprepared to deal with it, said Hannam.

Corporate Security: An Investigation into Telephone Fraud in the UK, is available priced £35 from Siemens on telephone number 0500 500712.

Contact: Mike Sylvester, *Siemens Business Communication Systems, UK* ***- Tel: +44 (0)1908 855000.***

CADiX 70 Card Accepting Device

A new card accepting device for multiple card payment applications, the CADiX 70, from Landis & Gyr Communications is to be incorporated in several large electronic purse field trials currently underway in The Netherlands and Germany to support new applications, says the company.

Based on an integrated platform, the device can be used for all card-based applications, including vending, ticketing, parking and multimedia kiosks and is designed to evolve with operators' changing needs by supporting new applications and accepting new or modified card schemes.

Contact: Adolf Deyhle, *L&G, Switzerland* - ***Tel: +4122 749 3355 Fax: +4122 749 3539.***

New Fare Collection Alliance

Three US companies have announced the formation of a new strategic alliance to provide what they describe as "a dramatically new approach to public transit fare collection in the North American market."

The alliance, under the name of the Tran$cash Consortium, brings together GFI-GENFARE, a leading supplier of automatic fare collection systems; Racom Systems, manufacturer of contactless Smart Cards, and systems integrator Perot Systems Corporation.

GFI-GENFARE, based in Elk Grove Village, Illinois, is a unit of the Connecticut headquartered General Signal Corporation and has been a leading supplier of bus-related fare collection systems in North America, recently broadening its equipment offerings to include rail-based transit systems, and various types of fare vending machines. Dallas, Texas-based Perot Systems Corporation is a major player in the integration of information systems worldwide.

As the card technology provider to the Tran$cash Consortium, Racom Systems, of Denver, Colorado, plans to utilise its new High Frequency (HF) contact/contactless, or dual interface Smart Card platform. It will apply the technology in contactless mode for the high throughput, high reliability requirements of transit, using its contact capability to serve the high security, multi-purse applications needed by the financial sector.

The consortium says that in this way, banks, card associations and other financial institutions can issue cards which will be compatible with a transit system's needs and thus assist in fare media distribution, an otherwise difficult and expensive task for the transit operator.

New Racom Card

The new HF Smart Card Series recently announced by Racom is a multi-application ISO-standard Smart Card which unifies contact and contactless operations using a single microprocessor.

HF Series cards can be read both in HF Series contactless readers as well as in ISO-standard 7816 contact readers. When used with HF Series contactless readers, the reader and card conduct secure, authenticated transactions using radio-frequency signals that permit complete transactions in under 100 ms, meeting a major speed requirement for public transit. HF cards also support contact operations in ISO-standard 7816 contact card reading devices, enabling the use of the same card in traditional contact-based Smart Card systems such as pay telephones and automatic teller machines.

Ferroelectric random access memory (FRAM) delivers up to 10,000 times the speed, consumes less than one millionth the power, and lasts up to 10,000 times longer than EEPROM memory used in conventional Smart Cards, says Racom, adding that it reduces fraud and counterfeiting risks by storing data using a polarization mechanism which cannot be electrically sensed or read externally.

The HF Series cards use custom ferroelectric integrated circuits produced for Racom by Rohm Co.,

of Kyoto, Japan, based on the FRAM technology licensed from Ramtron International Corporation.

Contacts: Bill Jacobs,** Racom Systems - **Tel: +1 303 771 2077. Fax: +1 303 771 4708. Kim Green,** GFI-GENFARE - **Tel: +1 847 593 8855. Fax: +1 847 593 1824. Kevin Wilson,** Perot Systems Corporation - **Tel: +1 303 804 5000. Fax: +1 303 779 1346.

Michael Love Joins First Union

First Union Corporation has appointed Michael G Love as Vice President of Smart Card Technologies to serve as project manager heading the team implementing the bank's Smart Card efforts.

Payment/Loyalty Card Partnership

Two French companies, Schlumberger Electronic Transactions and High Co Technologies, have entered into a partnership to develop Smart next-generation multi-function payment/loyalty cards and expect to ship them in 1997.

Jacques Cosnefroy, General Manager of Schlumberger's Cards Division, said: "The challenge for today's retailer is to turn new customers into loyal, regular patrons. Now, by integrating loyalty and electronic cash functions onto the same card, such schemes offer global potential."

Aneace Haddad, President of High Co Technologies, added: "The market for customer loyalty programmes is doubling every year."

Schlumberger's Payflex operating system software and dedicated chip will provide the foundation for the new cards. The chip's easily partitioned memory array allows several applications to co-exist securely on one card, with no possibility of switching between applications without additional checks. Each application has its own security mechanism to ensure flexibility, enabling multi-function cards to support multiple loyalty schemes alongside electronic cash facilities.

High Co Technologies is a software company specialising in Smart Cards and terminals. It has developed a library of loyalty card software applications, running under its open operating system, XLS, which optimises the resources used by the card's added-value services: loyalty points, electronic coupons, special purpose pre-paid electronic cash schemes, and any personal information such as school, health, family benefits and vehicle maintenance data.

Contacts: Nicolas Suraqui,** Schlumberger Smart Cards & Systems - **Tel: +33 (0)1 47 46 55 44. Fax: +33 (0)1 47 46 68 26. Aneace Haddad,** High Co Technologies - **Tel: +33 (0)4 42 24 58 24. Fax: +33 (0)4 42 24 58 25.

Ecash for Australia

Advance Bank will be the first bank in the Asia-Pacific region to issue electronic cash on the Internet in a pilot of the Digicash ecash system with Advance Bank and BankSA customers and merchants.

Andreas Furche, Managing Director of Digicash Pty, said: "This is good news for companies wanting to sell digital goods such as information, software or database access. They can set up shops that automatically provide services and collect money."

Contact: Andreas Furche - Tel: +61 2 375 2316. Fax: +61 2 375 2121.

Intellect Wins Dutch Orders

Intellect Europe has won orders in The Netherlands, through its local partners, to the value of US $32 million for upload units and payment terminals as Dutch banks and retailers gear up to handle the Chipknip and Chipper purse card schemes.

The company has also announced that a large Dutch retailer has selected Intellect products to equip all of its supermarkets with multi-functional terminals capable of handling both electronic purse card systems and customer loyalty programs.

Contact: Marleen Raskin,** Intellect-Prodata, Belgium - **Tel: +32 2 722 8711. Fax: +32 2 725 0628.

Alliance to Market Production Lines

Dutch company GPT AXXICON, which dominates the market in mould-making and injection moulding technology, has formed a strategic alliance with Meinen, Ziegel & Co., of Germany, a leading manufacturer of contact and contactless Smart Card production equipment.
The two companies will now be able to offer card manufacturers the manufacturing line concept from Meinen, Ziegel & Co with fully automatic card body manufacturing from GPT prior to chip implantation and personalisation.

Contacts: Eric de Bruijn,** GPT AXXICON - **Tel: +31 492 598854. Tomas Meinen,** Meinen, Ziegel & Co - **Tel: +49 89 614481-0.

Smart Card Threat: From Bellcore

The October issue of *Smart Card News* led with the story of attacks on Smart Cards, publicised by Bellcore (Bell Communications Research). Since then, new ideas have been stimulated by Bellcore's work. Because any new material about smart card security has to be studied carefully, it is worth looking again at what is being suggested and I would also like to comment on the manner in which the announcement was publicised by the Company.

The idea of the attacks is to bring a new factor into cryptanalysis (the breaking of ciphers) by deliberately inducing errors into the performance of the cipher algorithm and observing the effect. The effect of some totally unknown error is unpredictable so, if it is to aid cryptanalysis, there must be some assumptions about the error pattern. It is these assumptions about the way errors will behave that make the likelihood of success controversial.

Attacking Smart Cards by inducing errors is nothing new, in fact it is a threat which designers have considered for a long time. To give an example, Smart Cards have software which has been used in their initial testing, immediately after manufacture, and could be misused, in principle, to read out any part of their memory. This test routine is cut off from use before the card is issued, by a variety of means. Perhaps the normal, working program could be made to jump into the test routine by an induced error? This is just one of the possibilities that designers and programmers have to consider. The stress which induces the error could be a blip on the power line or a hiccup on the clock or raised temperature. The newer chips for Smart Cards have a selection of detectors for such stresses. But whatever precautions are built in, there will possibly be some trick or combination of tricks that can make the chip misbehave, so we have to take the threat of induced errors very seriously.

Jumping into the wrong bit of program is precisely what the Bellcore-style attackers don't want to do; they want the error to be in the *result* of an apparently good calculation. These data errors can be divided into two categories - either the result will be uncontrolled rubbish or perhaps just one bit will change in a certain register, just once in the crypto calculation. The former is much more probable but at first sight seems unlikely to give much help to the attacker. The most interesting observation made by the Bellcore authors is that at some stages in an algorithm a totally wrong result can help the attacker.

They describe attacks on six applications of cryptography which might be found in Smart Cards. The first two are attacks on RSA and a variant of RSA due to Rabin, which can be tried if a method of calculation using the "Chinese remainder theorem" (CRT) is used, as often it will be. This attack works if a certain part of the calculation has *any* kind of error, so its probability must be rated highly. The other four examples, and an error inducing attack on DES proposed by Biham and Shamir, depend on inducing sparse errors in a register once during the calculation. I have written "sparse" because sometimes these methods can be extended to errors of more than one bit, for example two bits in a register or conceivably three, but it gets much harder for multiple bit errors. These attacks can be rated as much less likely to succeed, but cannot be ruled out.

So the attacks can be divided into two categories, the attacks which essentially target the Chinese Remainder process and seem plausible and the much more problematic "sparse register errors" which seem to need a moderate or large number of trials with the same data, and the correct result for comparison. In the case of a smart card used for authentication, the crook who is able to make a large number of trials might be better employed using the card for fraud, instead of a cryptography exercise.

The attack on RSA operations in their CRT form is very interesting and much the best of the ideas presented. The RSA calculation is to take a message M and, using the secret exponent d, to form the exponential M^d modulo pq, where p and q are secret primes and only their product pq is made public. The CRT method is to find M^d twice, using each of the two moduli p and q separately and from these two results get the answer, modulo pq. If just *one* of the two intermediate results (either modulo p or modulo q) is wrong, the error this produces in the final result enables p and q to be found and the security is broken. Getting just one of the two calculations to be wrong may not be too difficult because they take some time to perform and the blip or hiccup can be timed to hit one of them.

As Bellcore described it, this CRT attack requires two results with the same initial data, one with an error and another for comparison, usually the correct value (though an error on the same side will do). Many systems will not allow this. Arjen Lenstra has improved the attack to use only one erroneous result. If there is an error on the modulo q side, we get a result R which is congruent to Md modulo p (but not modulo pq) and then the attacker calculates M* = Re modulo pq, which

would correctly be *equal* to M, but actually is *congruent* to M modulo p, so that the greatest common denominator of M-M* and pq gives p, and the security is broken.

When the M^d calculation is used to form a signature, checking the result before releasing it is a good countermeasure. The Bellcore paper says that checking the signature process involves repeating it, which may be too much extra calculation. But a small exponent e can be used, making the checking a trivial matter. Given that the attack on RSA-CRT is a plausible one, it would be a sensible precaution to check the result before releasing it. On the other hand, if the M^d calculation is a decipherment, some redundancy in the plaintext must be checked. I do not know any example without redundancy in the real world. When RSA is used for key management, this checking before using the plaintext has always been present, in my experience. In any case, the plaintext includes a secret key which is never revealed to the user. Real systems are quite different from those imagined by cryptographers.

The really significant new idea is the attack on the CRT method for RSA calculations, because it gets its results from an unspecified error in one part of the process. This is not to say that the attack is easy or even that it will be possible, but it is certainly plausible. Checking the signature (or decipherment) using a small exponent e is a countermeasure, though unfortunately some RSA co-processors are not efficient with small exponents. The differential attacks using "register faults" are much less plausible; only experiment will show if they can succeed, assuming that the system allows them.

Bellcore issued a "Media Advisory" entitled "Now, Smart Cards Can Leak Secrets" with a subheading "A new breed of crypto attack on tamper-proof tokens cracks even the strongest RSA code" and in the following text: "It diminishes confidence in Smart Cards that are used for stored value, such as some forms of electronic money."

In another "Media Advisory" we read that "Even if all the products currently using RSA authentication were upgraded to 1024 bit moduli we could still break the code."

These statements, with no qualifications, are wrong and misleading. Nowhere in the press releases is there any hint that there are limitations to the attack on RSA. "In the case of RSA implementations our algorithm efficiently factors the RSA modulus" hardly leaves room for doubt if you trust the organisation making the statement.

Large projects using RSA and Smart Cards can depend for their progress on the support of people who have no expertise in either technology and have to believe what they are told by experts. When a company with the prestige of Bellcore makes these wild statements, these people, reading only the press summaries, take some notice. At the least there will a few difficult days for the project, while the echoes reverberate in the media and there may be some permanent loss of confidence, which is not justified by the facts. After all, Bellcore say it "diminishes confidence in Smart Cards", without qualification.

This is not to diminish the value of the Bellcore work or to deny that we should look again at systems which employ the CRT method. Since these are relatively new results and there will be further developments, it would be foolhardy to come to final conclusions. My own reaction is that there is now a plausible and significant attack on the CRT method, which calls for a simple countermeasure and there are interesting questions about "register errors" which only experiment will answer.

D.W.Davies, CBE, FRS. 1st November, 1996

Mondex / MasterCard Rumour Continues

As SCN goes to press the rumour is that MasterCard is set to acquire Mondex and an announcement will be made within a day or so.

Officials still refuse to confirm or deny such suggestions. Martin Jones of Band and Brown Communication did say that MasterCard and Mondex are in discussion, but added "Mondex is in discussion with a number of financial institutions around the world. As yet no deal has been struck".

If, however, MasterCard does acquire Mondex tension with their closest rival Visa will surely increase, heating up attempts to agree an industry standard for Smart Cards.

Visa has already trialed Visa Cash in a number of countries including America, Spain, Australia and Argentina. Their most recent pilot has just been announced, the location will be Leeds in the UK (see page 209).

To confuse the picture further MasterCard recently said they would pilot their own Smart Card in New York, March 1997.

Smart Card Diary

International Smart Card Applications in Transport, The Kenilworth Hotel London WC1, 25th November 1996.

This conference will explore the latest opportunities offered through Smart Card applications within international transport systems. Tel: +44 (0) 171 436 5735. Fax: +44 (0) 171 435 5741.

Smart Card Europe: Developing and Managing Smart Card Applications, The Royal Lancaster Hotel, London, 11/12 December.

Conference focusing on the efficient deployment of Smart Card applications and how best these schemes can be managed. Pre-conference workshop, Introduction to Smart Cards, at same hotel, 10 December; and post-conference workshop on Smart Card Security, The Marble Arch Marriott Hotel, 13 December. IBC Technical Services - Tel: +44 (0)171 637 4383. Fax: +44 (0)171 636 1976.

Preventing Plastic Card and On-Line Fraud, Forte Posthouse Regents Park, London, 23-24th January 1997.

Includes contributions from card companies, the police, banks and retailers.

Ruth Chambers - Tel: +44 (0) 171 915 5141. Fax: +44 (0) 171 915 5001.

Optimising on the Potential of the Electronic Purse, The Kensington Hilton, London, 30 - 31st January 1997.

This event will demonstrate how to develop and impliment an efficient electronic purse scheme. It will also provide disscussion on current issues.
Kathy Gardner, Tel: +44 (0) 171 252 2222.

Smart Cards and Electronic Ticketing within the Air Industry, Central London, 17-18th February 1997.

This conference will cover key issues relating to Smart Cards and electronic ticketing including technical applications, IATA's regulatory requirements, marketing of new services, partnership development and usage within airports.
Barbara McManus, Tel: +44 (0) 171 453 1904. Fax: +44 (0) 171 580 2071.

SESAMES Awards

Banksys, the Belgian network for electronic payment Bancontact / Mister Cash, won the Best Application Award for its development and operation of the Belgian electronic purse system, PROTON. Not only has Banksys made PROTON a national success, it has exported the technology to Interpay in The Netherlands for the Dutch national electronic purse scheme Chipknip; Telekurs in Switzerland which will market its card under the name Cash; ERG for the QUICKLINK consortium for applications in Australia, Hong Kong and New Zealand; MITEL in Brazil where Banco do Brasil has started several pilots. Two Swiss banks, Sparbanken and Nordbanken are to jointly launch a PROTON test site.

SCN understands that negotiations are currently taking place between Banksys and other parties interested in the PROTON technology and the first of several announcements can be expected soon.

The Best Innovation Award was presented to Motorola and Gemplus for the development of SmartVue, a standalone portable Smart Card reader with a totally new virtual display concept - VirtuoVue - developed by Motorola. SmartVue is the first pocket-portable Smart Card reader that can display photographs or graphics for advanced as well as security applications. It was one of the big talking points of the show.

Technical specification:

* weight 150 grams, size 125 x 75 x 27mm
* personal and confidential viewing
* full screen size viewing (comparable to looking at an 18" monitor 1.5 meters away)
* compatible with ISO 7816-1-2-3(T=0, T=1)
* 240 columns x 144 rows of amber pixels
* 14 rows x 40 characters of text
* 16 shades of gray allowing the display of pictures, icons or graphical characters

Marc Lassus, CEO of Gemplus, said: "Smart Cards without SmartVue are like a PC without a screen. From now on, cardholders will be able to view the information stored in their cards which will build consumer confidence for future Smart Card applications such as identification, security and credit/debit card applications."

Bertran Cambou, Senior Vice President of Motorola Semiconductor Products Sector, said: "The virtual displays provide unique opportunities for people on the move to easily access large volumes of information and data."

Delegates and visitors were undoubtedly impressed with the technology, but many were left wondering what practical use the US $80 unit could be put to. Company officials pointed to cardholders being able to check their card balance, look up their medical record, confirm credit miles on frequent fliers cards and use them for identification.

Discussions over lunch indicated that a customer shopping in Harrods would probably prefer to use the current unobstrusive pocket reader to check the balance on their electronic purse card, rather than attracting attention by looking through the SmartVue unit. You would not regularly want to look at your medical record; whilst a passport check using SmartVue seems rather far-fetched. But at the rate technology is advancing, SmartVue's successors may become essential tools in our everyday life.

Contacts: Youri Tolmatchov, *Banksys* ***- Tel: +322 727 6666. Fax: +322 727 6767. W K Liew,*** *Motorola Innovation Centre* ***- Tel: +65 486 2854. Fax: +65 83 4303. Flavie Gil,*** *Gemplus* ***- Tel: +33 (0)4 42 36 56 83. Fax: +33 (0)4 42 36 51 17.***

Electronic Cash Report

Research and consulting company Ovum has published a 250 page report, *Electronic Cash: Opportunities for Banks and IT Suppliers*, giving advice on how to exploit the electronic cash market.

Available in paper form £1,195 Europe, US$ 2,220 rest of world. Single-user CD-ROM (+paper) £1,434 (plus VAT) Europe, US$ 2,664 (plus expenses) rest of world - Tel: +44 (0)171 312 7318. Fax: +44 (0)171 255 1995.