August 2005

Volume 14 • Number 8

Smart Card News

Smart Cards, SIM, Biometrics, NFC and RFID

www.smartcard.co.uk

05 • Amex Gold Card for Middle East

05 • New 512 kB SIM Platform

06 • Super Smart Card for Korea

05 • New Octopus Card Designs

This Month's Lead Story

Oyster Card to Incorporate "e-Wallet"

In This Issue

Regular Features

World News In Brief

Featured Articles

Smart Card News is published monthly by
Smart Card News Ltd
Columbia House, Columbia Drive, Worthing,
BN13 3HD England
Telephone : + 44 (0) 1903 691 779
Fax : + 44 (0) 1903 692 616
General Enquiries : info@smartcard.co.uk
ISSN 1745-7858

www.smartcard.co.uk

Dear Subscribers,

It's now well into the summer holidays and I decided to take a short trip to Italy leaving from Gatwick. It was quite reassuring to see the extra security as I am a nervous flier but this feeling of reassurance did not last long. The extra staff checking passports only gave them a cursory glance and did not check the human face against the passport photo. I can understand the time restraints and how deadly boring the job must be but one can't help but think that security falls down every time when it is reliant on human beings. Would machine readable biometrics be better? The manufacturers of this technology obviously believe so and governments are investing large amounts of money but I can't help but think that it may be a long way off and that what we currently have is only a ploy to help relieve anxiety in the travelling population.

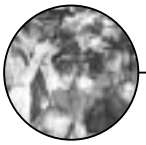
The National ID card for the UK appears to be trundling forward as witnessed by the OJEU notice out this month. Apart from a few vociferous groups the population at large seems remarkably laid back but not so amongst some of the MPs and members of the Lords. Will the Bill find its way through Parliament? We continue to watch with interest.

Security is back on the agenda again and this month we report again (see David Everett'd article) on the various disputes about whether you need a Smart Card. We may be biased but we're convinced that the security offered by today's Smart Cards will continue to outperform any of the alternatives and as for the ubiquitous PC, well.....

Enjoy the rest of your summer holidays,

Patsy.

Printed by
Hastings Printing Company Limited



Oyster Card to Incorporate "e-Wallet"

Trials to use London's Oyster Card as an 'e-wallet' will commence later this year. Under the plans, travellers across the City of London will be able to use their contactless travel Smart Card to pay for low-value items such as newspapers, milk, coffee, car parking tickets and fast food restaurants.

The plan to extend Oyster from travel to small value purchases demonstrates Transport for London (TfL) commitment to provide greater convenience for passengers and generate additional revenue for the transport network. It marks an important step forward for TfL's aspiration to extend the use of the Oyster card. The pilot schemes are currently being run in libraries and council leisure facilities in the boroughs of Greenwich, Newham, Croydon and Lewisham.

According to Jay Walder, Managing Director of Finance and Planning at Transport for London "Oyster has the largest customer base of all Smart Cards in the UK, with 2.2 million users and a significant level of public trust. Extending Oyster to include low value payments is a natural progression which will make the Smart Card even more convenient."

Mr Walder then proceed to say "The use of contactless Smart Cards for low value payments is growing in popularity around the globe. Such schemes are now well established in Hong Kong and Japan and significant trials are taking place in the United States. " One of these scheme Mr Walder is refering to is the Octopus transport card, which already exists in Hong Kong.

TfL expects to confirm its partner for the new scheme before the end of the year, having narrowed the field down from nearly 100 interested companies to a shortlist of seven. The successful organisations and consortia for the development of this e-money project are: alphyra, Barclays, EDS/JPMorgan, Nucleus/Dexit/Ericsson/Hutchison 3G/Euroconex, PayPal, RBS and BBVA/Accenture/MTR/Octopus.

Negotiations will commence this month and TfL hopes to trial the technology and confirm its chosen partner by the end of 2005. Work on the development and delivery of e-money on Oyster cards will then start in January 2006. However under current Financial Services Authority regulations, cash stored on the Oyster card chip cannot be used for non-ticket purchases. This could be a major stumbling block for the Oyster Card, so TfL has been exploring the possibility of becoming an FSA-approved 'E-Money Issuer' itself, or its other option is to find a partner who has the necessary credentials.

Commenting on the decision by Transport for London and Mayor Livingstone to begin exploring the possibility of turning London into a cashless zone through the Oyster card, London Assembly Liberal Democrat Transport Spokesperson, Lynne Featherstone, said: "While it is welcome that the Mayor and Transport for London are looking for innovative ways to use the technology behind the Oyster card it seems that they are trying to run before they can walk."

"The Oyster card must deliver on its original promise of providing ticketless travel for all Londoners on the whole public transport network. Before embarking on a bid to remove cash from society, the first thing that the Mayor and Transport for London must do is to get train companies in the capital to offer the Oyster card as an alternative to paper tickets. The Mayor also promised that the Oyster card would become a London Culture Card and yet so far we have failed to see this delivered. The Mayor and Transport for London must get the foundations in place and working properly before expanding into other wish-list areas."

Smart Cards

Alliance Opens Latin Chapter

The Latin American Smart Card market is growing, due to many market factors including the migration of mobile telecommunications operators to GSM, the financial sector migration to EMV, the move to smart transit fare cards and new government and commercial secure identification initiatives. Responding to these market factors, the Smart Card Alliance has announced the formation of a new Latin American chapter to bring together Smart Card suppliers, partners and customers in order to address the challenges facing Smart Card deployment in the region. The main mission of the Smart Card Alliance Latin American chapter is in line with the overall goal of the Alliance - to stimulate the understanding, adoption, use and widespread application of Smart Cards.

First EMV Migration in Pakistan

Axalto is supplying high-end EMV chip banking cards to United Bank Limited (UBL), pioneering the first EMV rollout in Pakistan. Axalto provided UBL with a complete EMV package including data preparation, cards supply and personalisation solution.

OMNIKEY Joins GeldKarte

OMNIKEY has joined as a founding member of the newly established association Initiative GeldKarte e.V. The association gathers the merchants that accept the German cash card as well as the suppliers of the necessary infrastructure for the GeldKarte, the chip-based electronic purse system which is jointly managed by the German banking industry. With its participation in Initiative GeldKarte, OMNIKEY aims to demonstrate and promote to potential users the advantages of the GeldKarte as a cashless payment method as well as a supporting medium for a variety of other innovative applications.

OTI Reports on US ePassport Project

On Track Innovations Ltd, (OTI) is one of several contractors that have received contract awards from the United States Government Printing Office (GPO) for the production of electronic passports. The GPO has, as required by law, issued a stop work order, effectively halting work on the program by all contractors pending a decision by the Government Accountability Office (GAO). The stop work order was issued due to a protest filed by OTI regarding the evaluation of its product by the GPO with the GAO.

The GPO's motion to dismiss the protest was denied by the GAO. Should the GAO rule in OTI America's favor, OTI, along with the other contractors, will continue work when the program resumes. (The contracts include several stages, running from testing and evaluation stages through production stages. OTI America successfully protested an earlier evaluation decision by the GPO at the outset of the program.)

New Way for Smart Card Deployment

GlobalPlatform has created the industry's first interactive curriculum that will educate Smart Card technology end users of the advantages in deploying a standardised Smart Card infrastructure. GlobalPlatform has developed an instructor-led program to provide those operating in the Smart Card market with an educational understanding of why GlobalPlatform technology is the solution to the business problems associated with lack of a standardised Smart Card infrastructure.

The technical workshop addresses the value of each component within the Smart Card infrastructure - the card, device and system and what each component brings to the marketplace. From a business perspective, the curriculum highlights why standardisation within the industry is important, the role that each of the Specifications play in the Smart Card environment and the value of bringing all three components together to form a complete standardised Smart Card infrastructure.

38m EMV Cards for Asia Pacific

Vice-president and regional head Advanced Payment Systems of MasterCard International, Shuan Ghaidan has announced that the EMV (Europay-MasterCard-Visa) card has reached 38 million at the end of June in the Asia Pacific region. The number has soared following a significant increase of 15 million EMV cards issuance so far to add to the 23 million registered in the region last year.

ID Card for Turkish Military

Keycorp's MULTOS Smart Card technology has been selected for a new multifunction ID card for the Turkish Armed Forces (TSK) and their families. With an initial rollout of two million Smart Cards carrying Keycorp MULTOS technology within 12 months, the new military ID cards will incorporate a number of applications including e-purse, access control, digital signature and health. The cards are manufactured by Oberthur Card Systems (OCS).

ActivCard Aquire Protocom

ActivCard has acquired Australian-based Protocom Development Systems in a deal valued at $21 million in cash and 1.65 million shares of ActivCard common stock. ActivCard has also initiated a plan to restructure the combined companies. This restructuring will include a reduction in force of approximately 13% of the combined companies' workforce over the next five quarters, though the majority of the reductions will take place in the September 2005 quarter. The restructuring is expected to save the combined company approximately $11.0 million per year in functional expenses.

New 512 kB SIM Platform

Giesecke & Devrient (G&D), together with Samsung Electronics, are to provide the first 512 Kilobyte (U)SIM card. Based on Java Card technology, the new chip platform combines the advantages of an extended memory capacity with high flexibility and short time-to-market for new mobile applications and services. The new UniverSIM Callisto 512 kB enables operators to have an extensive selection of Java card applets like information on-demand services, SIM browser solutions or mobile commerce applications on their (U)SIM card while still offering a vast memory space for user specific information like telephone numbers or short messages.

Amex Gold Card for Middle East

American Express Middle East has announced the launch of its new American Express Gold Credit Card in Qatar and Bahrain. The new Gold Credit Card is a Smart Credit Card with an embedded Chip featuring 'ID Keeper'. ID Keeper is an application on the card's chip which allows card members to securely store their favourite website addresses, personal details, passwords, user names and auto-fill online shopping order forms. This enables cardmembers to shop online more securely, swiftly and conveniently. Gold Credit Cardmembers are automatically enrolled in the global award winning Membership Rewards programme.

New National ID Smart Card System

Intercede Group has teamed with Oberthur Card Systems to build the first end-to-end fully functioning National ID Card provisioning system. This solution will use Intercede's MyID Smart Card and identity management system and Oberthur Card Systems' ID-One Smart Card to securely enroll, manage and maintain Smart Card-based biometric ID cards.

In a seamless process, these cards will be electronically and graphically personalised and distributed by Oberthur Card Systems' secure card personalisation bureau in Tewkesbury, UK.

Smart Card Key to Liverpool

In a bid to help attract visitors to Liverpool in the run up to 2008, when the city becomes European Capital of Culture and is expected to attract an additional 1.7 million tourists, Applied Card Technologies (ACT) has been chosen by Livesmart to implement Liverpool's first smart city card system. Launched with backing from both Merseytravel and The Mersey Partnership, 'your ticket to Liverpool' is provided and powered by ACT"s sophisticated web-enabled destination management solution, enabling visitors and citizen's alike admission to every participating attraction with free, VIP or discounted entry. 'Your ticket to Liverpool' is ITSO compliant and will be integrated with Merseytravel, to allow visitors to travel to their chosen destination using their ticket to Liverpool

£4m for Smart Card Growth Strategy

ID Data plc has won an extra £4 million in cash to support its growth strategy in providing secure Smart Card-based transaction systems and services to the banking, retail and government sectors. Investors have further signalled their commitment by agreeing to convert £3.6 million of long-term debt into equity, giving them shares in the AIM-listed company. This will strengthen ID Data's balance sheet, enabling the Company to build on their recent success in gaining significant contracts in retail, banking and expanding government sectors for Smart Card technology.

New Octopus Card Designs

To meet changing market demands and requests from tourists and local collectors, Octopus Cards Limited began issuing Sold Octopus to the public in 2004. Every 6 months, a new series with a different theme will be issued - the first series was "Pearl of Lights", featuring scenic night views of Hong Kong, followed by "Pearl of the Orient", highlighting several famous local tourist attractions.

Overwhelming response has been received for both. This month, Octopus presented its newest series, "Pearl of Heritage". "Pearl of Heritage" takes the theme of transport heritage to unveil the distinctive and representative means of transport that appeared in Hong Kong's earlier years.

G&D Opens Branch in Berlin

Giesecke & Devrient (G&D) have opened their Government Solution Center (GSC) in Berlin, Germany. The heart of the GSC will be a presentation room showcasing innovative products and solutions for government agency related applications. The branch office, located directly next to IT security service provider Secunet AG. Their proximity to G&D's new premises will allow visitors to acquaint themselves with the technologies and solutions offered by the G&D affiliate all in one location.

G&D Expands into Italy

Giesecke & Devrient (G&D) also reported the opening of a subsidiary in Milan, Italy that has been set up to supply its new Smart Card technology to BNL, one of Italy's largest banks. The Italian market is strategically important for G&D. By the end of the year, there will be a total of 1.2 million chip-based payment cards in circulation. G&D has about 60% of the payment card market in Italy.

Super Smart Cards for Korea

e- Smart Technologies has rolled out its inaugural Super Smart Card, in Busan (Pusan), Korea. Pursuant to the Agreement signed on July 23rd between e-Smart Technologies, Inc., and Mybi Company Ltd., e-Smart began distribution the e-Smart-MYbi card, the first multi-application e-currency biometric Smart Card to be used in Busan as a digital city, e-government ID card, payment card for mass transportation, banking, point of sale, internet and other diverse financial payment card transactions.

Common Infrastructure for Suica

East Japan Railway Company (JR East) and NTT DoCoMo, Inc. (DoCoMo) have signed a basic agreement to discuss joint development and management of common infrastructure for JR East's Suica e-money and DoCoMo's upcoming "Osaifu-Keitai" credit card service, both based on FeliCa Smart Card technology. Suica is JR East's IC card for railway travel and shopping, while Osaifu-Keitai refers to DoCoMo mobile phones equipped with contactless IC cards that can serve as credit cards and perform other useful functions. Under the agreement, the two companies will consider the development of a reader/writer compatible with both companies' services and the creation and management of a common center that connects the reader/writers with various settlement systems.

The companies feel that working together will promote their services more effectively than if they were to act separately. JR East and DoCoMo aim to reach the final agreement within 2005.

ANDiS Card for BC Card

Bell ID's Korean business partner HiSmarTech (HST) signed an agreement with BC Card for the implementation of Bell ID's ANDiS Management Systems. BC Card is using ANDiS to issue and manage approximately 17 million EMV-compliant credit cards for 11 Korean banks and credit card companies over the next 3 years. The project went live in January 2005 and has issued over 300,000 cards since then. HST is providing all required professional services locally to ensure optimum availability of expertise and support.

TNS Rolls Out Aconite EMV Solution

Aconite is partnering with Transaction Network Services (TNS) to better enable banks to deliver safer bankcard transaction services to UK customers. TNS is rolling-out Aconite's EMV (EuroPay, MasterCard, Visa) authorisation, transaction and post-issuance scripting solutions to UK banks to increase operational and cost efficiency and help address mounting card fraud.

Atmel Receives F&S Award

Atmel Corporation has received the Frost & Sullivan 2005 Award for Global Market Penetration Leadership in recognition of its outstanding achievement in the Smart Card microcontroller integrated chip (IC) market over 2004. In particular, the award commends Atmel for capturing the number two position in the microcontroller IC market in terms of unit shipments and technology development with an enhanced product mix.

Biometrics

3M to Deliver Biometric Passports

The UK Foreign & Commonwealth Office (FCO) has appointed 3M to develop, test and implement the UK's first biometric passport issuance system. The new system will use biometric technology to prevent multiple passports from being issued to the same person under different identities. 3M will equip 104 British Embassies, Consulates and High Commissions around the world with new passport issuance systems that can identify biometric information.

1 in 10 British passports are issued outside of the UK and the new web-based 3M Identity Document Issuance System will ensure that these passports are as secure as those issued in the UK by the UK Passport Office.

Fingerprint Security for the ThinkPad

Lenovo has chosen UPEK's fingerprint authentication solutions to secure their ThinkPad Series of notebooks with the introduction of the new ThinkPad X41 Tablet. Lenovo incorporated UPEK technology on select models of the ThinkPad X41 Tablet. UPEK delivered its TouchStrip fingerprint authentication solution with "dual-swipe" technology, which provides the user with the ability to swipe the sensor in either direction, complementing the unique display orientation flexibility of the tablet form factor.

Financial Results

Gemplus Second Quarter Results

Gemplus International S.A has reported results for the second quarter ended June 30, 2005. Their net sales were 236.2 million euros which is +12.2% on the previous years result. Gross profit was recorded at 80.0 million euros and gross margin was up 1.6% to 33.9%, the highest in 4 years. This was driven by a favorable business mix and improved manufacturing efficiency. Operating expenses decreased 5.8% mainly driven by the reversal of a 5.2 million euros litigation provision. Consequently, operating margin almost tripled to 7.0% and attributable net income quadrupled, to 29.0 million euros.

Axalto Second Quarter Results

Axalto has reported their second quarter 2005 revenue of $260.9 million, a 15% increase compared with $226.9 million second quarter 2004 revenue. For the first six months of 2005 Axalto posted revenue of $498.2 million, a 16% growth over the $430.3 million revenue recorded in the first half of 2004. Revenue in Axalto's Cards segment came to $243.1 million, up 16% compared with the second quarter of last year. During the period Axalto delivered over 110 million microprocessor cards, a 36% volume growth. The Americas region took over as the second-largest revenue contributor. In their financial card section Axalto again posted solid expansion in this product line during the second quarter. Revenue was up 14%, at close to $55 million, with all regions progressing.

The volumes of microprocessor cards delivered posted a steep rise of 17%, with over 20 million cards sold in the quarter, while the average selling price of microprocessor cards for banking was essentially stable, up 2%.

Oberthur Q2 Sales up 13.6%

Oberthur Card Systems, has reported results for the second quarter ended June 30, 2005. Q2 sales amounted to 121.1 million euros, up 13.6% on a year-on-year basis. Sales for the first semester have reached 239.2 million euros, an improvement of 15.3% compared with the previous year. Second quarter sales growth is mainly due to the microprocessor cards segment, with 45 million cards delivered, a 34.9% increase versus the previous year. Despite intensified pricing pressure in the GSM market, sales for this segment are up 18%.

Payment cards sales was up by 38.5% year-on-year, reflecting the gain of market share in UK and France, as well as the first deliveries of contactless cards in the US and EMV cards in Italy.. Identity & Security, segment volumes increased by 44%, due to a combination of significant deliveries of Pay-TV cards and the deployment of e-passports programs in Belgium and Thailand.

STM Reports Second Quarter Results

STMicroelectronics has reported net revenues for the second quarter was $2,162 million, up 3.8% sequentially from the $2,083 million reported in the prior quarter, and 0.4% below the $2,172 million reported in last year's second quarter. Gross profit increased 4.4% to $714 million from $685 million in the first quarter of 2005 despite continuing price pressure in memory and standard products. For the 2005 second quarter the Company reported operating income of $12 million, and net income of $26 million, or $0.03 per share. In the prior quarter the Company reported an operating loss of $68 million, and a net loss of $31 million or $0.03 per share.

Atmel Reports Second Quarter Results

Atmel Corporation has reported revenues for the second quarter of 2005 totalled $412.2 million, versus $419.8 million in the first quarter of 2005 and $420.8 million in the second quarter of 2004. Net loss for the second quarter of 2005 totalled $42.6 million or $0.09 per share. These results compare to a net loss of $43.0 million or $0.09 per share for the first quarter of 2005, as well as a net income of $11.7 million or $0.02 per share for the second quarter of 2004.

Near Field Communication

Cingular Chooses (U)SIM Cards

Oberthur Card Systems has been selected as a primary SIM vendor by Cingular Wireless, the largest wireless company in the United States, with more than 50 million subscribers who use the nation's largest digital voice and data network. Oberthur Card Systems will begin delivering SIM cards to Cingular this month

Ticketing Applications for Mobiles

Royal Philips Electronics has joined other members of Taiwan's Proximity Mobile Transaction Service Alliance (PMTSA) in demonstrating a prototype mobile phone capable of making secure payments using Near Field Communication (NFC). The development of this phone by alliance member BenQ, with support from Philips, is a milestone and paves the way for the alliance to develop ticketing and payment applications.

As a result, residents of Taipei can use NFC-enabled mobile handsets to access the city's Mass Transit Rail, as well as other public transport networks in Taiwan. The first practical PMTSA application will be the use of NFC-enabled mobile handsets to make payments on the public transportation system in Taipei. The network already has an existing contactless Smart Card infrastructure based on the company's MIFARE technology, which is compatible with NFC. This enables the new technology to capitalise on the incumbent technology, without the need for additional development.

Radio Frequency Indentification

Chipless Devices Could Grow by 30%

Research and Markets in their report "The Future of Chipless Smart Labels" have stated that chipless RFID smart labels can be electronically interrogated to reveal ID and other data. They do not contain a microchip and therefore cost much less than chip RFID. From being just 2.5% of the RFID market today, chipless devices have the potential to grow to 30% of the market by 2010. Some of the biggest names in the business now offer both chip and Chipless RFID in order to cover a full range of user needs. From AstraZeneca to Calvin Klein, companies are already using them in large volumes and many paper and packaging companies have licensed the various processes.

Chipless RFID smart labels with up to 10 meters range and 256 bits of data, can cost one tenth of their silicon chip equivalents and have a greater physical performance. Chipless RFID can be materials based, or can consist of transistorless circuits. Transparent polymer transistor circuits will also be available in volume by 2005, directly mimicking the circuit on a chip. All this will let Chipless technology address mainstream RFID applications and rapidly grow the market by price reductions of one to two magnitudes. Beyond RFID we will enter a world of science fiction. Transparent packages will light up with moving colour advertisements and speak to you when you approach; disposable smart labels will detect viruses, specific chemicals and many other things. Meanwhile there are both electronic and non-electronic Chipless labels for a wide range of diagnostics and brand enhancements.

Wheres My Beer?

Sokymat are supplying RFID tags to mobile asset management company TrenStar Inc. to track beer kegs for clients in the U.K. including Coors. The percentage of kegs owned and managed by TrenStar in the U.K. is now close to 70%. Sokymat filled an initial order of 1,200,000 TrenStar-branded tags. TrenStar's RFID-enabled container management system, TrenStarCM, tracks the location of each beer keg and collects information including usage data, enabling better control, visibility and asset utilisation for the sake of securing the distribution channel and making it transparent to the customer.

New US DoD Passive RFID Agreement

The Department of Defense has awarded Unisys Corporation a blanket purchase agreement (BPA) to connect the Defense Logistics Agency (DLA) and its suppliers through an integrated Radio Frequency Identification (RFID) infrastructure to track and trace assets. Under the terms of the agreement, Unisys can now be selected by the DLA, or any other agency within the Department of Defense or the United States Coast Guard, to integrate passive RFID infrastructure within their supply chain.

UPM Rafsec Uses UHF RFID Tags

UPM Rafsec has developed manufacturing technology for the mass production of RFID tags which are now in use in the company's facilities. After the successful completion of piloting, UPM Rafsec deploys this proprietary and patent pending process at its new North American manufacturing site in Fletcher, North Carolina.

On the Move

Infineon Board Member Steps Down

Dr. Andreas von Zitzewitz has steped down as Member of the Board of Infineon Technologies AG. Dr. von Zitzewitz is under investigation based on allegations of Udo Schneider, Managing Director of BF Consulting GmbH.

This is in context with payments made for contracts regarding motorsport sponsoring. The company immediately terminated all sponsoring engagements in motorsports as far as possible after the departure of the former CEO Dr. Ulrich Schumacher. Infineon Technologies AG is not under investigation and cooperates fully with the authorities. Dr. von Zitzewitz declared his resignation, to spare the company the burden of the ongoing investigation and to be able to fully concentrate on the expected court case.

Infineon Re-organisation

Infineon Technologies AG has announced that the supervisory board has approved a re-organisation of the responsibilities within the Management Board and the appointment of Prof. Dr. Hermann Eul.

Kin Wah Loh will assume responsibility for the Memory Products Business Group. Professor Eul is appointed Deputy Management Board Member and in this capacity he will take over the responsibilities of Kin Wah Loh.

New Board Memeber for ActivCard

ActivCard has announced that Jason Hart, Chief Executive Officer of Protocom, will join the Board of Directors of ActivCard and assume the role of Senior Vice President, Sales and Marketing, responsible for global sales, marketing, business development, and product management functions. Yves Audebert will retain his position of President and Chief Strategy Officer of ActivCard.

In addition, the Company has appointed Thomas Jahn, Managing Partner of Kainos Consulting, LLC to the new position of Chief Restructuring and Integration Officer to help manage the integration efforts of ActivCards $21 million acquisition of Protocom Development Systems.

BIO-key Announces New Co-CEO

BIO-key International, Inc has announced that Tom Colatosti, BIO-key non-executive Chairmen of the Board will become Co-CEO with Mike DePasquale in a newly formed Office of the CEO.

News Sales Director at OMNIKEY

OMNIKEY has announced that Patrick Comiskey has joined OMNIKEY Americas as regional sales director. Patrick will focus on growing and supporting OMNIKEY's reseller, VAR, and distribution partner base in the Americas.

ASSA ABLOY ITG Names New VP

ASSA ABLOY Identification Technology Group (ITG) has announced the appointment of Michael Pilato to Vice President and General Manager.

Mr. Pilato will be responsible for leading ITG's Business Development activity in new identity management markets, made possible through a strategic partnership with CoreStreet, Ltd.

New Finance Manager at ACT

Applied Card Technologies (ACT) has appointed Nikki Osborne as Finance Manager. Nikki will be responsible for the production, management and reporting of all financial data, as well as contributing to overall business and financial strategy.

Keycorp Board of Directors Changes

Keycorp Limited has announced that Mr Andrew Lockwood, a director of the company, has resigned from the Keycorp Board of Directors.

Management Expansion at Versatile

Maciej (Matt) A. Pcion has joined Versatile Card Technology/QualTeq Division Senior Management Team. Pcion will be responsible for the entire card manufacturing operation and will continue his active involvement in new card technology and manufacturing methods.

Smart Cards Monitor Food Choices in Schools

A team led by the Institute of Food Research has completed a 2-year study of food choices made at a North London school, to be published this month (August 2005). Scientists tested the viability of using "Smart Card" technology to monitor pupils' mealtime choices. Project leader Dr Nigel Lambert said: "School dinners are currently a highly political and emotive social issue. The government has pledged to tackle menus, but measuring children's eating habits at school is fraught with difficulties. Accurate information is necessary to support the government's public health policies. Smart Card technology could provide a practical and accurate solution."

One in five English secondary schools makes use of basic Smart Card systems for meal payment. This takes cash out of schools and reduces queuing times. The cafeteria at Haberdashers' Aske's Boys' School routinely serves around 1000 diners aged 7-16 and their system was upgraded for the study. For over a year, a full electronic audit was made of every transaction that took place and each food chosen was converted to its nutrient composition.

"No questionnaires were required, nor an army of researchers, but the system succeeded in objectively recording food choice with 99% accuracy. It can also be continued long term, unlike the more usual three to seven day 'snapshot' studies", said Dr Lambert

The aim of the project was to test whether Smart Card technology could be used in this way, but it also produced a wealth of data on foods selected. Senior nutritionist on the study Professor Ian Johnson said: "Not all the data has been analysed, but we can already see that despite a vigorous healthy eating policy operated by the caterers and the school, and healthy foods being readily available, the children generally preferred products high in sugar and fat. This reflects the preferences of most UK children.

"The research using Smart Card technology has demonstrated the ability of the system to identify individuals who persistently choose highly inappropriate meals. What a school does with that important health information presents society with an ethical issue."

Smart Card systems could be used to help schools with healthy eating programmes through personalised feedback on food choices, or reward schemes for children who choose healthy options. The technology could be applied to other cafeteria settings such as in the armed forces, universities or prisons where monitoring food choice would be beneficial.

The UK Government has pledged an extra £280million to tackle the "school meals crisis in England". As recently as May 2005 the Government set up a new School Meals Review Panel chaired by Ms Suzi Leather. An early objective for the panel is to create compulsory nutritional standards for school meals.

A proposal has been sent to the NPRI (National Prevention Research Initiative) to set up a network of similar Smart Card systems across 4 mixed state schools and to use this network primarily to monitor the effectiveness of a Department of Health-supported dietary intervention based upon the "whole school approach". In addition, the new study plans to explore the moral and ethical issues raised by the technology.

Clamping Down on Cardholder Not Present Fraud

THALES

By Paul Meadowcroft, Head of Transaction Security, Thales e-Security

Paul Meadowcroft

Card fraud is big business. In the UK alone it totals over £400 million a year and internationally it prompted the multi-billion pound rollout of the EMV Smart Card standard. However, the shear scale and sums involved means that fraudsters are not going to be easily put off and have shown themselves to be more than capable of increasing the level of fraud sophistication to circumvent preventative measures such as EMV. This growing and increasingly sophisticated threat has kept card fraud as a high priority for banks everywhere, especially when the 'soft' costs of the tarnish to reputation and potential legal costs are taken into account.

To date, the most prevalent and commonly known type is counterfeit card fraud. However, as new banking channels have opened up, for example internet, phone banking and e-commerce, combined with the boom in credit card use, crime has migrated to seek any opportunity to attack these new and immature transaction methods. Already fraudsters have begun to abandon the traditional card crime of counterfeit fraud and figures show that this has been overtaken as the most costly type of card fraud by a newer method, that of Cardholder-Not-Present (CNP) fraud. In the UK last year, CNP fraud was responsible for losses of £116.4m - more than any other type of card fraud.

CNP transactions are performed remotely, when neither the card nor the cardholder is present at the point-of-sale. CNP transactions take many forms such as orders made over the phone or internet, by mail order or fax. In such transactions, retailers are unable to physically check the card or the identity of the cardholder, which makes the user anonymous and able to disguise their true identity. Fraudulently obtained card details are generally used with fabricated personal details to make fraudulent CNP purchases. The card details are normally copied without the cardholder's knowledge, taken from discarded receipts or obtained by skimming. This means that while the three or four digit Card Security Code on the back of cards can help prevent fraud where card details have been obtained, it does not prevent fraud on cases where the card itself has been stolen.

Of course, a major reason CNP fraud is on the increase is because of the migration to EMV Smart Cards which was introduced to tackle counterfeit fraud. The major advantage of Smart Cards is the increased security they provide. The chip technology uses sophisticated processing techniques to identify authentic cards and make counterfeiting extremely difficult and expensive. Combining this with a PIN is a proven system for combating fraud as it provides the two-factor authentication of 'something you have' (the Smart Card) and 'something you know' (the PIN). This makes the probability of fraudulent transactions taking place in an ordinary retail environment extremely low.

Two factor authentication is key: Banks are having to face up to the realities of the modern highly connected world, which now provides a vast array of opportunities for banks to interact with customers. It has meant that whether as a consumer or a business, the number of transaction channels is now extremely varied and continuing to grow, yet it is a scenario that few banks are fully prepared for. At the moment the maximum level of security available to consumers for e-transactions is user ID and password authentication, although these have become increasingly sophisticated such as through 3D Secure. However, this is already seen as being inadequate for securing financial transactions. Instead, pioneering banks and credit card providers are turning to the obvious candidate for reducing CNP fraud, the EMV Smart Card.

The reason that the EMV Smart Card is not already used within consumer e-transactions is the difficulty in including the card within the transaction process. The solution for this, an unconnected reader, is not new. However, the barrier has always been around cost. In other words, is it more cost effective for the bank to accept low levels of fraud rather than the expense of rolling out millions of unconnected readers to consumers? The continuing rise of CNP fraud is beginning to tilt the argument in favour of the rollout option.

In terms of the technology behind the unconnected Smart Card readers, it is the introduction of a common standard that is the most important innovation. APACS, in association with MasterCard, released specification standards for unconnected Smart Card readers which have allowed leading manufacturers to offer products for mass consumption at a commercially viable cost.

The reader provides the user interface to the card and displays a one-time passcode once it has read the smart card and the user has entered his/her PIN. The user then manually types this passcode into the computer at the appropriate prompt. Only the issuing bank can authenticate this one-time passcode. To avoid repeat attacks, the one-time passcode can also be linked to the individual transaction by a more secure, yet still simple, challenge-response process. In this case, should the passcode be intercepted, it is of no use whatsoever beyond this particular transaction.

Assuming that consumers will not resist the introduction of unconnected readers, this new system will have an extremely positive effect on fraud and in turn help boost consumer confidence in e-Commerce. However, it is not just internet-based transactions that will benefit. Theoretically, any transaction where the card has to be used, and the cardholder is not present, could use this scheme. For example, if purchasing goods or services over the phone, the buyer could simply read the one time passcode to the person at the other end who could then validate it in the usual way through the payment system. As such the Smart Card is transformed into a personal security module to validate every financial transaction the user wishes to make.

The security benefits are clear to see. The inclusion of a Smart Card in every financial transaction will add a crucial second layer of authentication. This two-factor authentication process of something you have as well as something you know should dramatically reduce fraud.

Events Diary

September 2005

13 - 15	SmartCards Expo 2005 - *New Delhi, India - www.electronicstoday.org/SMARTCARD05.htm*
14 - 15	The 4th Asian High Security Printing Conference - *Hanoi, Vietnam - www.cross-conferences.com*
21 - 23	e-Smart and World e-ID Conferenced 2005 - *French Riviera - www.strategiestm.com/conferences/*
21 - 24	Labelexpo Europe 2005 - *Brussels, Belgium - www.labelexpo-europe.com/*
26 - 27	6th International Conference Smartcards in Transport - *Paris, France*
27 - 29	Loyalty World - *London, United Kingdom*

October 2005

1 - 2nd	eyefortransport RFID Opportunities for Transport and Logistics Providers - *Las Vegas, Nevada, USA - http://www.icma.com/meetings/annual-expo.htm*
6th	Radio Rrequency Identification 4 Reatilers - *London, UK*
17 - 19	Banking Technology - *Budapest, Hungary*
18 -21	2005 Annual Fall Smart Card Alliance Conference - *Miami, Florida, USA - http://www.smartcardalliance.org/*
10 - 12	RFID Journal Live Europe - *Amsterdam, Hotel Okura - www.rfidjournallive.com/europe*

November 2005

15 - 16	CARTES 2005 - *Paris-Nord Villepinte Exibition Center - http://www.cartes.com/en/2005/index.htm*

Secure Software Key Protection Accelerates Smart Card Applications

By Rod Stuhlmuller, Director of Product Marketing, Arcot Systems, Inc.

Rod Stuhlmuller

At first glance, a secure software-based key protection solution would seem to compete directly with a hardware-based Smart Card-based solution. Quite the contrary. By accelerating the deployment of digital signature credentials within the client organisation, Smart Card solution providers can become stronger partners with their clients, as well as reduce the "lag time" between when the contract is signed, and when the client actually begins reaping the benefits of the newly enabled applications.

Contemporary thinking views secure, software-based credential protection as an enabler for accelerating the deployment of applications which drive the adoption of Smart Cards. Applications are often delayed as user training, client hardware distribution, and installation logistics are put in place. After all, it is the scaled roll-out of the functional application with its attendant business benefits -- not just the Smart Card infrastructure -- which delivers the "return-on-investment" that justifies the Smart Card deployment budget.

Consider the growing trend of combining both physical and logical access onto a single Smart Card that enables both secure access to the building and support for a new digital signature-based application. Consider also the existence of a secure software-based credential protection solution that is functionally equivalent to a Smart Card, from an application's point of view. Of course, a "virtual Smart Card" solution is not designed to deliver physical access capabilities. However, by leveraging an existing Smart Card management system, secure software-based digital credential containers can be generated and issued securely and rapidly throughout an organisation. This allows the client to realise a significant portion of the project's projected "return-on-investment," in the short-term by replacing a less efficient paper process with a new digital signature-based process. Then, as the Smart Card infrastructure is rolled out over time, user credentials are securely transferred from the secure software-based credential container to the new Smart Card, without any impact to the application's functionality.

The client and the Smart Card provider can now manage the rollout of the hardware infrastructure at a pace that budgets and business pressures will allow. The client has been introduced to a robust solution for replacing/fortifying weak password protection even to areas where Smart Card deployment is not feasible, thus providing Smart Card providers with "stickier" client relationships. Smart Card News readers, familiar with hardware-based key protection solutions, might be quick to challenge the validity of this assertion, saying, "Secure key protection in software is not possible!" This stance is justified and absolutely accurate, if not for Arcot Systems' patented "Cryptographic Camouflage" technology. This technology forms the basis for the ArcotID, Arcot Systems' secure software-based credential protection container, and defines the distributed, multi-key method for protecting an individual's digital credentials. An ArcotID, like a Smart Card or USB token, is a secure digital key container, but, instantiated completely in software. Unlike traditional software key containers, which are vulnerable to brute force attack, the ArcotID leverages its "Cryptographic Camouflage" technology to thwart this and other types of attack scenarios to provide a security level approaching that of hardware solutions, and that is orders of magnitude more secure than any other commercially-available software-based alternative.

The Cryptographic Camouflage Difference - The benefit of cryptographic camouflage can be easily understood by comparing the impact of a brute force attack upon a typical software-based key container and the software-based key contained protected using Arcot's cryptographic camouflage technology. Consider a brute force attack on a typical software key container, accessible using a 6 digit PIN. First, any local lock-up counter is easy to circumvent by merely making as many copies of the key container file as required. Second, the hacker simply employs a "dictionary" attack, attempting every possible 6 digit PIN (1 million). It is important, at this point, to understand that PKI private keys have particular and well documented characteristics. Let us assume, for the purpose of this example, that they all begin and end with 1 and are hexadecimal numbers.

Each PIN attempt produces a result. Incorrect decryption keys or PINs result in jumbled character results that do not meet the "hexadecimal and beginning and ending with 1" criteria. Eventually, the right PIN is entered producing the expected hexadecimal number beginning and ending in 1. The hacker is able to thus identify the correct formula, and the key has been compromised.

Now consider the same attack against an ArcotID software-based key container. Using Arcot's cryptographic camouflage technology, the key is encrypted, based on the user's PIN, using standard encryption methods, but using the patented Arcot process. The effect of this process is that decryption using an incorrect PIN will produce a result that meets the specific, particular and well documented characteristics of a private key. So, in this 6 digit PIN example, the brute force attack will produce 1 million plausible, but invalid private keys. Keys produced as the result of using an invalid PIN meet all the characteristics of a valid key, so they can be functionally used to encrypt or "sign" a challenge received from the Arcot server as a part of the authentication and digital signing process. The attacker has to encrypt or "sign" the challenge with the PIN-decrypted, "de-camouflaged" key and respond to the Arcot authentication server which then validates whether or not a valid PIN was entered. If not, an invalid PIN counter is incremented and, just as with a hardware-based solution, the server can lock any use to the ArcotID container after a configurable number of invalid attempts. The hacker has essentially fallen into a camouflage trap. Thus secure key protection in software IS possible, and available today.

Financial institutions and other security conscious enterprises, pressured by the growing public perception of rampant online fraud and identity theft, as well as greater regulatory scrutiny, need a strong authentication solution today. As such, the offering of software key protection as a precursor, supplement to, and rapid enabler to Smart Card implementation can make the valuable difference in the way of larger and longer term contracts, and deeper customer relationships. In fact, it is favorably arguable that the complementary use of software strong authentication with Smart Card deployments could change the very reputation upon which the Smart Card industry is sometimes viewed - from one of high security coupled with high organisational complexity - to one of rapid response and implementation.

UK Oversells the Benefits of ID Cards

The UK's plans for a national identity card were in disarray after a statement this moth made by the Home Office which confirmed one of its ministers had admitted that the UK's ID Card scheme's benefits had been "over-emphasised".

Tony McNulty, the minister responsible for the ID card programme said "Perhaps in the past the Government in its enthusiasm oversold the advantages of ID cards. We did suggest or at least implied that they may well be a panacea for ID fraud, benefit fraud, terrorism and entitlement, and access to public services."

This shows that the UK Government has misrepresented the benefits of ID cards to the public. Mr McNulty also disclosed that the Government's long-term plan for moving from a voluntary to a compulsory scheme could end in parliamentary deadlock, with the Commons and the House of Lords at loggerheads. These remarks came as polls show that public support for the ID card scheme is falling dramatically amid fears about spiralling costs and the infringement of civil liberties.

This new revelation shows a significant change in gear in the Home offices towards the UK ID card under the new home secretary Charles Clarke. In light of this the Conservative and Liberal Democrat Party's now demand that the ID card project should be abandoned.

Labour MP John Denham, chairman of the Commons home affairs committee, is urging the government to clarify their position. "If the government is backing off ID cards I think they need to say so because that would be a very big mistake," he said.

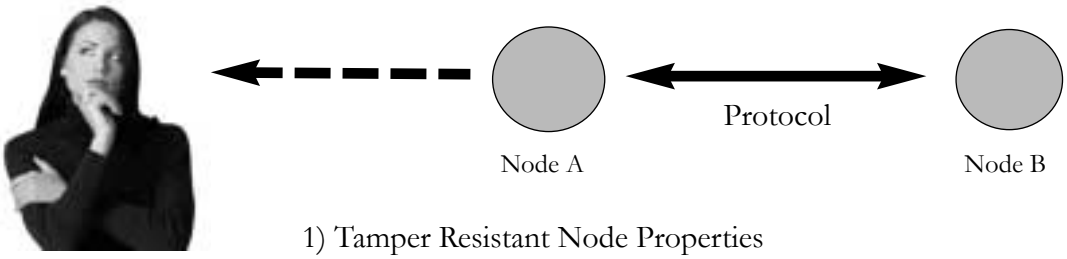
Can You Keep a Secret?

By Dr David Everett, CEO, Smart Card Group

Dr David Everett

The remarkable thing about security is how people keep on rediscovering old problems. Last month we talked about biometrics and in particular the need for 2-Factor authentication (at least). We assumed that the Smart Card would represent one of the Factors - something you own. It was implicit in our discussion that the smart card offers the necessary security properties but this month we are going to look a little more carefully and show you how people are breaking the rules and heading obliviously into well known problems.

When you take the Smart Card as an authentication token then by default you have to put in place some method of verification that differentiates the real card from a counterfeit. The path is littered with techniques around the plastic including visual ideas such as holograms. It is well known that the hacker can easily circumvent these controls so it is the chip that forms the security object and more particularly it is a secret held securely inside the chip that provides the authentication lever. Proving you know a secret without revealing the secret is the name of the game and here's where we need some protocol to make this happen.



1) Tamper Resistant Node Properties
2) Strength of Protocols and Mechanisms
3) Node Processing Integrity
4) Node Identification
5) User Binding

In the general case (referring to the above diagram) Node A needs to prove to Node B that it is authentic. Using a challenge response protocol and strong crypto can solve problem 2 above , but how about number 1, the Tamper Resistant Node? Well again the Smart Card provides the answer because it has been specially designed to be tamper resistant (not proof, but very difficult). So in practice we may happily store our secrets in a Smart Card. Number 5 above refers to the linking of the user with the card for two factor authentication and this could be a PIN or biometric as discussed last month, and again we can securely store these secrets in the Smart Card.

So what is the problem? Well it's just that there are a number of schemes that seem to believe you can do all this in a PC and you don't need the Smart Card. In other words there is an assumption that you can store secrets (crypto keys or whatever) in a PC and that it is resistant to attack. How wrong can you be, there is an army of experts out there who know the PC and the operating system inside out and given access there is nothing to stop them exploring until they find what they want. Take the work of Adi Shamir and Nicko van Someren as an example who in their paper 'Playing hide and seek with stored keys' show how the entropy of keys (measure of uncertainty) is high (because they should look like random numbers) and which therefore offers a practical method of finding the key storage area on the hard disc drive or in memory.

In short you must assume that if a hacker has access to your PC then it is possible to find secret keys and other confidential information such as PINs and passwords. In no way can a PC be considered a Tamper Resistant Module. If you want better security, or to use PCs that you don't trust - use a Smart Card!

e-Identity: Empowering Services and Upholding Privacy

By Neville Pattinson, Director of Business Development Technology, Axalto

Neville Pattinson

The need to find ways to securely link individuals to their identification documents is increasingly under consideration by governments around the world. Recently published figures from the US show identity theft - the ability to masquerade under somebody else's identity - is increasing at a rate of 24% per year. The need for secure identification credentials - whether a passport for travelling, healthcare card, voting registration or driver licence - is part of a wider public debate over national security, individual privacy and protection of personal information. The challenge for public decision makers is reassuring all stakeholders that e-ID based identification schemes will deliver a secure, trusted and cost-effective identity system.

Existing system under attack: Government credentials issued to citizens today are generally based on plastic or printed paper and use a variety of either printed security features or low grade machine readable technologies, e.g. static technology magnetic stripes and/or bar-codes which are seen as more and more vulnerable. Counterfeiting or tampering with passports is a notorious weak-spot exploited by criminals in order to perform various kinds of fraud. A primary root cause is the nature of 'breeder' documents (i.e. birth certificate, marriage certificate, etc.) which are easily forged or reproduced along with poor identity proofing procedures beyond inspecting the presented paper document. Many existing IDs have limited or no physical security features at all, and are just visually inspected by a guard and are not verified by machine.

Forgers with readily available equipment, are quickly able to create acceptable documents that allow them to obtain valid IDs. Once this has been affected the ID remains good, albeit fake, until such time as the ID expires or is somehow found to have been obtained fraudulently. Some governments are now putting in place new extended citizen and employee identity vetting and proofing procedures when applying for government identity documents. Recently the US passed the Real-ID Act 2005 which now requires not one, but several forms of identification to be presented at application and all documents to be proofed and vetted prior to the issuance of a government issued ID card such as a Driver's License.

Putting intelligence into the solution: Governments have already looked to technology for a way to align issues of security and privacy. In the domain of travel security, the US e-passport will integrate a smart chip into their passport booklets to strengthen document security and directly combat counterfeiting. US Visa Waiver countries are also required to add similar smart chip technology to their passport booklets by Oct 2006. Some of these will even have machine-readable biometric identifiers, such as fingerprints, included in the smart chip to help verify the correct person is presenting the document.

In Belgium the e-ID card (BELPIC), which will be issued to 11 million citizens, exploits similar Smart Card intelligence to secure access to e-government services whilst protecting personal information. Both are examples of a growing trend towards incorporating secure, privacy enhancing, active electronic components to government identification credential documents - e-Identification.

E-identifications incorporate proven Smart Card technology, although they are not necessarily in the form of a traditional card (as in the US e-passport example). Adding an electronic chip into any document makes an e-identity virtually impossible to counterfeit thus providing a strong countermeasure against identity theft. The smart chip can also perform all the necessary real-time authentication required to irrefutably link the user to the document being presented by using PIN codes or biometrics or both.

The high levels of security of a chip-enabled e-identity can help increase public confidence in a national credentialing system and provide government and citizen accountability. The technology can also deliver more compelling administrative and financial benefits to the issuing authority that target such areas as benefit fraud or voter fraud etc. As an enabler of e-government, an e-identity can help governments conduct securely more of its business online, lowering costs and eliminating paperwork.

Privacy and secure identification: In discussions on identification schemes, citizen privacy and protection of their personal information emerge as key issues. Whilst security concerns cover the confidentiality, integrity and availability of information, privacy encompasses the protection of personal information during its entire lifecycle from collection, through usage and storage to eventual end.

Smart Card technology provides features that can help reassure citizens that e-identity is an effective way to deliver better security whilst protecting their privacy. A smart chip acts as a secure vault that protects an individual's personal information and controls access to the information. It can quickly validate a citizen for a requested action - e.g. voting, traveling, access to online services - but also ensure privacy by only accessing the specific information required for any action.

When using e-IDs there is no need to have expensive on-line connections to centralised databases to verify either the owner or to authenticate the e-ID at the time of use. e-IDs are capable of internally matching one-to-one biometrics, or PIN codes, thereby ensuring the owner is present and in control of the credential at the point of use. e-identities can be secured (e.g. digitally signed or otherwise protected) by the issuer allowing the e-ID to assert its authenticity off-line. The use of PIN codes and/or biometric verification on the smart chip proves the correct owner of the document is present and prevents unauthorized hijacking of an e-identity credential when lost or stolen. An important factor to point out is that the e-ID also puts the e-ID owner in control of their private information. Until the owner enters their PIN or presents their live biometric verification their e-identity cannot be accessed.

Securing the future: Governments must improve the security of their citizens while modernising and securing access to services. The authentication of both the identification credential issued to citizens and the verification of the physical document belonging to the citizen is becoming increasingly important to combat instances of identity fraud or unauthorized entry into sensitive areas or critical systems.

e-identification is now a proven application and gathering momentum around the world, bringing benefits to both government and citizens. Defining and implementing e-ID systems requires combined expertise across a number of different domains from security practices such as logical and physical security, information systems, to biometrics and appropriate national privacy policies. Lessons learnt from large-scale implementations of healthcare cards, national ID cards and corporate e-ID badge programs will prove invaluable in the creation of new national identification initiatives incorporating e-Ids that are to be considered secure and trusted by all those involved.

The Smart Card Epidemic

By Jason Smith, Staff Reporter, Smart Card News Ltd

Jason Smith

Over the last five years the Smart Card integrated circuit (IC) market has been some what erratic. However more recently the Smart Card market has seen a sudden surge in growth. According to figures released by Frost & Sullivan, the market generated revenue totalling $1.40 billion in 2003 rising to $2.1 billion in 2004. The company predict that this figure will reach around $4.2 billion by 2010.

According to figures released by EuroSmart, 1469 million microprocessor Smart Cards where shipped worldwide in 2004 - which shows that Smart Card sales have increased by 50% since 2003. In a breakdown of the Smart Card market, the biggest growth segments, beween 2003 and 2004, which where recognised were the telecommunication segment which grew massively by 57% to 1050 million units, the financial segment which grew by 37% to 280 million units and the transport segment up by 25% to 15 million units. EuroSmart estimated that the total worldwide Smart Card unit figure, by the end of 2005, will reach 2 billion units.

Within this industry, Gemplus is the undisputed leader according to a market survey conducted by Gartner Inc. Gemplus tops the Smart Card market with a 27.1% market share. Furthermore, Gemplus has also generated the most revenues with 865 million euros gained in 2004. Axalto remains in second place in the total chip card rankings, with market share of 20.4%. Giesecke & Devrient, Oberthur Card Systems, and ORGA Kartensysteme make up the remainder of the top five in market share. Presently, Europe accounts for 68% of the demand for Smart Cards, but by the end of this decade Europe, Asia, and the United States are expected to equally share one third of the total demand according to figures released in Reserach & Markets paper on the Smart Card Market. As per projections, in 2005, North America will require approximately 543 million cards, while there will be a requirement of 3.75 billion cards across the world, which is a lot highter then Eurosmart's prediction.

In 2003, the total Smart Card reader market was around 9.4 million units and is expected to reach 35.5 million units by the end of 2005. Also, in 2003, the total Smart Card terminals market reached 4.8 million units and is expected to grow significantly reaching 14.3 million units by the end of 2008. One reason for this new rise in demand for Smart Cards, was the unexpected growth of the subscriber identity module (SIM) within the telecommunications segment between 2003 and 2004. Prior to this - in 2001 - the Smart Card market was affected by the fall in mobile handset sales, with mobile operators and handset vendors seemingly overestimating the extension of the installed base on a market already considered very mature - thus accumulating large stocks in 2000. However the rapid adoption of global systems for mobile communications (GSM) technology in 2003 and 2004 worldwide, created a strong demand for high-memory 64k and 128k SIM cards, as well as for Java cards. As telecom operators strived to provide value-added services, they started pushing for higher-memory SIM cards. In addition to this, the arrival of 3G boosted the high-end Smart Card IC chip sales since 3G and 2.5G services require larger memory capacity to store new features and bigger files.

As we can see from the growth in Smart Card readers and terminals, this growth is not just being fueled by the SIM segment. The uptake of Europay, MasterCard, and Visa (EMV) cards has increased and this has been significant enough to help drive the growth in the overall market. "Migration to the EMV standard in the banking sector is creating substantial opportunities for Smart Card IC chips," states Industry Analyst Jafizwaty Haji Ishahaq. The use of contactless technology by retailers and in various transit projects worldwide is another factor spurring this high uptake of Smart Cards. Early in 2005 ABI Research forecast that "the coming year will see a sharp increase in the number of contactless payment opportunities for consumers." According to Erik Michielsen, the firm's director of RFID and ubiquitous networks, that forecast has not only proved correct, but is an understatement. The related market for near-field communications is also seeing a surge in activity although according to Michielsen, 2006 will be the year of NFC.rd are backing the use of contactless technology as a faster and more convenient way to conduct payment transactions, a sign that has worked in favour of the Smart Card market.

Contactless Smart Cards are identified as among the best ways to store biometric data on travel documents such as passports, visas and identity cards, says Frost & Sullivan. In addition, the International Civil Aviation Organization's (ICAO) recommended a combination of contactless Smart Cards and face recognition biometrics for new secure biometric-enabled passports and travel documents. Since United States' law mandates that the 27 countries under the Visa Waiver Program follow ICAO recommendations to improve security, the contactless Smart Card market has received a tremendous boost as countries worldwide start issuing passports with contactless chips.

While the firmest commitments for Smart Card technology are seen in North America, interest is also strong in Europe and Asian-Pacific countries, because such technologies can be deployed anywhere in the developed world. Asia/Pacific is the most dynamic area because of the market size and the high growth rate of applications in such areas as mobile communications and mass transit. This approach is unique as Smart Card deployment is not isolated to one or two vertical markets and deployment is therefore organic. Singapore and Hong Kong constitute 'hotspots' for Smart Card deployment with Japan (Tokyo) following suit.

The market in every tier of the value chain is relatively fragmented, especially in the card integration sector. As Hong Kong and Singapore prove, however, the market for new, high-value, multi-application cards relies on partnerships, interoperability, openness and further impetus from the banks. China play a significant role in the market during 2004, accounting for 15% of total chip card unit production.

One reason for this organic growth is that Asia-Pacific countries generally have strong government control. Asia-Pacific governments exert influence on key vertical market operations, perhaps to a larger extent than their European or US counterparts by encouraging standardisation and co-operation if technology is designed to facilitate and synchronise a citizen's daily life. This brings us onto another area that is fueling this sudden growth surge in the Smart Card market - Government and Identification (Gov & ID).

The Gov & ID sector includes applications such as national and corporate ID cards, healthcare, e-passports, driving licenses, and military and police cards. Given that security concerns are increasing by the day for many countries, just consider the 911 tragedy and more recently the Madrid and London bombings, these applications will drive strong global growth over the next 10-15 years.

According to Eurosmart figures it is seen that between the Govenment and corporate segments of the Smart Card market, there has been a combined growth worldwide of a staggering 129% between 2003 and 2004 bringing the total units sold in 2004 to 1.06 billion. The launch of high volume national ID projects such as the China national ID project has generated enormous opportunities for this industry. These ID Card projects require massive databases containing personal information on citizens, leading to concerns about their integrity and security. Getting public approval for such initiatives is a great challenge and calls for huge efforts on their part to protect personal privacy and data security by providing adequate safeguards against potential abuse and failures of the system.

Conclusion: With the Smart Card market now developing into an established mass market for the two leading applications - mobile communications and banking - major industry vendors must continue to sell large volumes of cards worldwide to banks and mobile telco issuers, while customising their products to their specific needs.

Despite industry consolidation in the last three years, I believe there is still room for niche markets, especially for growing applications such as corporate and network access, electronic identification and egovernment, which require contactless communication in order to be in a better position to adapt to the needs of corporate and public customers. Can you Keep a Secret?