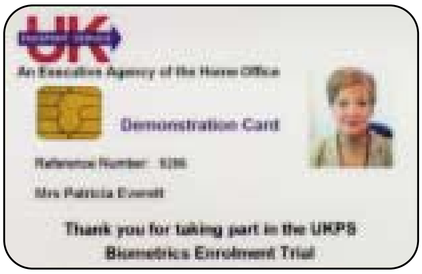
June 2005

Volume 14 • Number 6

Smart Card News

Smart Cards, SIM, Biometrics and RFID

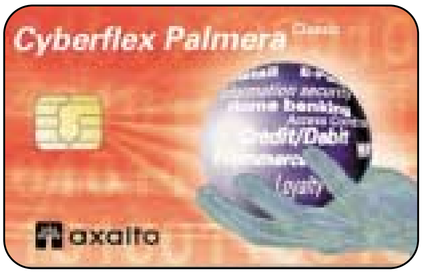
www.smartcard.co.uk


UK
An Executive Agency of the Home Office
Demonstration Card
Mrs Patricia Everitt
Thank you for taking part in the UKPS Biometrics Enrolment Trial

18 • ID Cards Back on the UK Agenda

05 • SIM Smart Cards for Tim Peru

05 • ExpressPay Moves to Blue



05• Java Cards for Afriquia Program

This Month's Lead Story

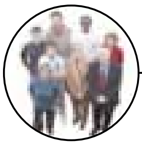
First EU Electronic Passport for Germany

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,

Transport and payments carries on behind closed doors. We know that Transport for London (TfL) is busy trying to find a consortium that will add small value payments to the Oyster Card while ITSO is pursuing the same goals for its Customer Media (e.g. Smart Cards). It now seems that people are starting to realise that any form of 'Open' ePurse is not straightforward in terms of maintaining an acceptable risk strategy and is certainly not the right way to use a Mifare card. The design and development of the ePurse goes back at least 20 years and it is incredible that so many people are re-inventing history or more precisely re-discovering the problems.

The ePurse path is littered with products cast by the wayside, Mondex, Digicash, Proton and VisaCash, just to name a few. All these approaches were in their own way technically sound but were found to be uneconomic in a classical payments infrastructure. Now we seem to be going backwards where even the basic security model is suspect. Of course if the scheme is a closed scheme then memory cards such as Mifare can be made 'fit for purpose'.

An interesting report was published this month by the Indian IT services company HCL which states that retailers they questioned believed RFID and Chip & PIN will be the priority investment next year and that digital TV and SMS was the biggest waste of technology investment for the retail sector over the last 18 months.

Alistair Darling (UK Minister for Transport) created some interesting dinner party conversations earlier this month over his announcement that the UK would implement a satellite global positioning system to enable the charging of motorists for the use of major roads during peak commuter times. GPS tracking of motorists is working in Singapore on their East Coast Parkway using a pre-paid Smart Card. Something has to be done about the UK's congested roads but with this country's appalling record on the implementation of large computer related systems I think we can look forward to interesting and expensive times ahead.

Managing Director
Patsy Everett
patsy.everett@smartcard.co.uk

Production and News Editor
Jason Smith
jason.smith@smartcard.co.uk

Technical Advisor
Dr David Everett
david.everett@smartcard.co.uk

Sales and Subscription Administor
Tina Mitchell
tina.mitchell@smartcard.co.uk

Editorial Consultants
Dr Kenneth Ayer
Peter Hawks
Simon Reed
Robin Townend

This Issues Guest Contributors
Smart Card Alliance
Gemplus International
Gary Watts
Dr David Everett
Steve Carter

Printed by
Hastings Priniting Company Limited

Please Note

From time to time, Smart Card News may include industry forcast and forward looking statements made by the companies concerned. Readers should be advised that Smart Card News Ltd cannot be held responsable for decisions and/or actions taken by readers of our newsletter, based on the information provided including any errors therein nor are we responsible for the opinions of the individual authors.

Don't Forget!
Our Website containing daily News On-Line, and information about the full range of SCN services, can be found at the following address: **www.smartcardgroup.com**

Certain images featured in this issue obtained from IMSI's MasterPhotos™ Collection 1895 Francisco Blvd. East, San Rafael, CA 94901-5506, USA

First EU Electroinc Passport for Germany

Driven by the United States' visa waiver program, which requires visitors to the country to present a machine readable passport when visiting the country for less than 90 days, governments around the world are starting to implement smart passports schemes. Germany is set to become one of the first European Union states to introduce the new passports. The German Interior Minister Otto Schily has stated that Germany plan to begin issuing biometric passports with a smart chip containing a digital photo of the holder from 1 November 2005.

This new German passport, called the ePass, will allow immigration officers quickly to make an electronic check matching the person carrying the document with the chip data, he said. In the new electronic passport, the printed information about the bearer's identity - such as the bearer's name, date of birth, photograph, and the passport's validity period and number - will be stored encrypted on a chip. And, starting no later than March 2007, fingerprints of each of the bearer's index fingers will also be stored in encrypted form. Current plans call for the chip to be invisibly integrated into the front cover. Iris scans may be added at a later date. All this technology will be phased in gradually at border control points to handle the chip passports, with full coverage expected by 2008.

The German passport printing authority, the Bundesdruckerei GmbH will be producing the passports and providing the necessary infrastructure including the background system and reading devices. Bundesdruckerei has selected, on behalf of German Ministry of Interior, both Royal Philips Electronics and Infineon to supply the contactless Smart Card chips for the new smart passports for the country's 80 million citizens. Philips will be providing the project with its 72Kbyte EEPROM memory, high-security chip with its high memory capacity able to hold biometric information such as fingerprints and facial images. The Philips chip used in the project has been certified by the German Federal Office Information Security (Bundesamt fur Sicherheit in der Informationstechnik), the central IT security service provider for the German government. It has received the organisation's Common Criteria EAL5+ certification, the highest level of security certification awarded to any secure contactless Smart Card solution available.

Infineon will be supplying a special chip package developed for identity cards and passports as well as the inlay containing the antenna and its connection to the chip. More than 50 individual security mechanisms burned deep inside the Infineon chip will help ensure that personal data is protected against unauthorised read-out and manipulation. Among other security features, the chips use the RSA method (a special computing algorithm for encrypting data, named after its inventors Ronald L. Rivest, Adi Shamir, and Leonard Adleman) to provide extremely high security. The security mechanisms integrated into Infineon's chips also include active protective shields on the surface of the chip and sensors that prevent hackers from being able to read the chip by applying different voltages.

There are currently around 24 million German passports in circulation, which are usually valid for ten years, with an annual replacement and renewal rate of about 10%."Smart passports enable greater levels of security than those provided by current passports, increasing safety for travelers and enabling governments to better protect their borders." said Reinhard Kalla, vice president and general manager, Business Line Identification, Philips Semiconductors. Schily hailed the new passports as a breakthrough in combating organized crime and terrorism by identifying people through their unique biometric data. "Issuing biometrically supported passports in Europe is a foundation stone in the battle against organised crime and international terrorism," Schily said.

Critics argue the technology is not yet reliable and have raised privacy concerns. Some say that because the chips can be scanned 'remotely', people could have their data read without their knowledge. Schily said this would not be possible with the German version, which can only be scanned when the passport is opened and the reading device has calculated a special access code. With the introduction of all this new technology the price of a new 10-year passport would rise to 59 euros from 26. However, some industry experts acknowledge they are not yet sure if the smart chips will withstand a full 10 years of wear and tear from being stamped at borders and stuffed inside people's bags and pockets.

Smart Cards

e-Visas for First European Trial

Axalto has teamed with Sagem in the European e-visa trial. The "Biodev" program is an initiative of a group of members of the European Union that aims to reinforce the control of borders and validity of visas in the "Schengen" free circulation zone constituted by 15 member states. The first deployments will be conducted by France and Belgium in certain ports, airports, embassies and consulates. The e-visa is one of the first electronic travel documents containing biometric data (digital photos and fingerprints) that can be authenticated each time the holder crosses a border.

Gemplus Selected for French e-Visa

Gemplus has also been selected to supply contactless Smart Card technology for the "Biodev" project. Gemplus will work closely with Sagem as well, who are the prime contractor. In this first phase of the "Biodev" project, Gemplus will deliver Smart Cards based on "GemBorder", its ICAO-compliant contactless chip technology for electronic passports and visas.

Thailand Begins E-Passport Tests

Thailand has begun pilot testing electronic passports on its general public. The initial tests where carried out on government officers. The Consular Affairs Department expects to issue 500 e-passports to government officers and another 500 to general citizens before the launch of the e-passports in August. It is estimated that over 7 million e-passports over the next 10 years will be issued.

The new passports have an embedded contactless 64-bit chip for storing personal information including name, date of birth, address, a right index finger print, face geometry and PKI (Public Key Infrastructure) on the outside cover.

Belgian's e-Passport Goes Live

ACG Identification Technologies is supplying contactless RFID readers to the Belgian government for the country's e-passport program. Belgium has started issuing to its citizens electronic, biometrically-enabled passports that fully comply with the recommendations set forth by the International Civil Aviation Organization (ICAO).

G & D Strengthens in Russia

Giesecke & Devrient (G&D) is expanding its Smart Card activities in Russia as well as neighbouring countries that belong to the Commonwealth of Independent States (CIS) by entering into a joint venture with Russia's Concern Nauchny Center (KNC). Representatives from both companies gathered in Moscow to sign the cooperation agreement. Before the end of June, joint operations will begin in Zelenograd /Moscow. In addition to production and personalisation of Smart Cards, the enterprise will develop and market Smart Card-based applications and system solutions.

32-bit Smart Card Microcontroller

Renesas Technology Corp has unveiled its latest 32-bit Smart Card microcontroller, designed specifically for the high-security needs of the financial and ID sectors. The AE55C1 offers an eight-fold improvement in performance over the previous 16-bit AE-4 series, meeting the increasingly complex demands for multi-application Smart Cards which require higher performance and flexibility from the Smart Card microcontroller.

Smart Cards Help Fight AIDS

India is testing a new Smart Card system that will electronically keep track of its HIV/AIDS patients and is expected to facilitate medication through anti-retroviral cocktails as well as track their potency. The cards will be given to more than 300 patients receiving anti-retroviral drugs. They would need to bring the cards each time they come to the hospital for anti-AIDS drugs or for any other medical problem. The cards would help health workers keep track of India's more than five million HIV/AIDS affected patients and act as a portable medical record. They fast-track treatment and medical response in emergencies, provide greater security to medical records and ensure immediate access and easy storage of data.

ORGA Joins Smart Payment Alliance

ORGA is the newest member of the Smart Payment Alliance (SPA). The SPA pools the expertise of the world's leading Smart Card manufacturers: Axalto, Gemplus International S.A., Giesecke & Devrient, Oberthur Card Systems, SAGEM and now ORGA. The SPA plans to foster Smart Card based payment applications, optimise the interoperability of value-added applications, develop the necessary specifications and improve security and quality.

Java Cards for Afriquia Program

Axalto is providing Smart Cards to Afriquia, a Moroccan oil company, for its private payment system. The Afriquia program is the first implementation of a private payment program using Java-based cards by an oil company in Africa. Afriquia issues Smart Cards from Axalto's Java Palmera line, as a proprietary charge card that lets Afriquia's business customers pay for, manage and control all fuel and service expenses for their vehicle fleets and employee owned cars. Under the program, the cards also can be used to pay for highway tolls and related services, such as auto repair, at Afriquia's partners.

270m for South African ID Card

South Africa's Home Affairs Minister Nosiviwe Mapisa-Nqakula has announced in her budget that 270 million rand will be supplied this year to South Africa's proposed smart identity card scheme. She said "The introduction of the smart ID (identity document) card which is the outstanding component of the Hanis (project) was approved by cabinet on July 25, 2001 pending the finalisation of the procurement model for such a card."

Chinese Network Card Solution

Gemplus has reached an agreement with East Port Technology Co., Ltd. (East Port), the founder of China Custom's Electronic Port Platform, to jointly explore business opportunities in China's e-government market for Smart Card-based network security applications. These will provide first-class, secure information and e-services for government and Chinese enterprises.

SIM Smart Cards for Tim Peru

Incard has been selected by Tim Peru' as the first supplier for the launch of its 128kb SIM card. Part of Telecom Italia Group, Tim Peru' is the first GSM Operator in Latin America to adopt the 128k card. Incard will provide the technical expertise to complete the new SIM profile implementation and aid TIM Peru' in the migration from standard 32k SIM cards to 128k STK SIM cards with tailored applications.

Tim Perù 128K cards are based on Incard's MoKard, a (U)SIM card which has been recognized as one of the most powerful SIM cards available on the market. The MoKard is fully compliant with the JavaCard 2.2.1 standards.

ExpressPay Moves to Blue

American Express has announced that it has begun issuing Blue from American Express with the ExpressPay feature in all 50 states. ExpressPay, a contactless chip for secure payment, will be embedded in all new Blue cards from American Express. ExpressPay is a new payment feature that consists of a secure computer chip powered by radio frequency technology.

Designed for purchases at locations where speed and convenience are important -- such as convenience stores, quick-serve restaurants, supermarkets, drug stores and gas stations. Users simply hold Blue with ExpressPay next to a special reader at the checkout to make purchases. Payment is authorised in seconds and no signature is required. The computer chip enables end-to-end transaction security.

ACG RFID Reader Goes MIFARE

ACG Identification Technologies has received official MIFARE certification for its new HF Dual ISO RFID Read/Write Reader from the independent MIFARE certification institute Arsenal Research, located in Vienna (Austria). The combination of using a standard EMV payment chip card such as OneSMART along with the secret PIN results in a strong, two-factor authentication process that deters identity phishing attacks and reduces the fraudulent use of stolen cards.

Visa Cards for Ethiopia

ACI has licensed its BASE24 e-payment processing solution to Dashen Bank, a private commercial bank in Ethiopia. ACI's software will help Dashen Bank to become the first bank in Ethiopia to issue and acquire Visa cards. Dashen Bank will deploy ACI software to issue cards and authorise, route and switch both ATM and POS transactions while meeting processing requirements for EMV (Europay, MasterCard and Visa) Smart Card transactions.

First EMV Card for the Philippines

ORGA Singapore is supplying the first EMV MasterCard chip card to the Bank of the Philippine Islands (BPI). BPl launched the BPI Express Credit Gold Card program for privileged customers. The BPI MasterCard is based on the open operating system MULTOS 4.06 from MasterCard. The Smart Card was issued as part of the OneSMART MasterCard program that accompanies the successful rollout of Smart Cards.

New Gemplus Proximity Readers

Gemplus is reinforcing its contactless access control offer by introducing "GemProx", a contactless reader product range dedicated to rapidly growing markets such as identity, proximity payments, physical access control and mass transit.The GemProx range is specifically designed to provide system integrators with a cost-efficient and easily deployable 13.56 MHz proximity contactless technology.

Easyflex for Lisboa Viva

Axalto has announced the successful delivery of 50,000 dual interface Easyflex CD Light Smart Cards to the train operator in Portugal, Caminhos de Ferro Portugueses (CP), for its "Lisboa Viva" transport card project. The cards will be used as monthly subscription-based traveller cards for the train in Lisbon. This delivery marks the first deployment of Axalto transport cards in Portugal and introduces dual interface Smart Cards to Portugal's train operator system for the first time.

Successful Litigation for Gemplus

Gemplus has been successful with its appeal in a lawsuit concerning an alleged breach of contract by Gemplus S.A., a subsidiary of Gemplus International S.A. in France, regarding the promotion of Smart Card solutions for casino slot machines.

On May 26, 2005, the Aix-en-Provence Court of Appeal rendered a decision in favour of Gemplus S.A., reversing the judgement of the Marseille Commercial Court of March 18, 2004 which had found that Gemplus S.A. had breached the contract and had ordered Gemplus S.A. to pay the plaintiffs 22 million euros in damages. The Court of Appeals dismissed all the plaintiffs' claims for damages and ordered the plaintiffs to pay court costs and expert's fees.

T-Mobile Selects GemXplore

Gemplus has been selected by T-Mobile to provide its new GemXplore Generations operating system as the basis for future card and service deployment for their customers. GemXplore Generations responded to T-Mobile's requests by complying with the latest multimedia features and standards releases, both of which can be updated over the air at any stage of the SIM lifecycle. This reduces time-to-market and increases the value of the SIM as a platform for future service updates and deployment.

GemXplore Generations offers the flexibility necessary for T-Mobile to license the Operating System and outsource personalisation in a highly secure way.

Mobiles Answer Credit Card Debt

A new independent survey, commissioned by mobile payment technology provider Upaid, reveals that 77% of British adults want to regain control of credit card debts by using mobile phone text messages to authorise payment of varying amounts. The research found that one in four people using direct debit to pay credit card bills find their debts mount-up because they automatically pay only the minimum amount each month.

One in four British adults avoid paying by direct debit all together because they feel they lose control over their bank account. The study revealed that one third of 18 to 64 year olds want a text message to remind them when a credit card bill payment is due, of which 62% want to be able to reply to that text message to authorise payment for varying amounts. The figure is even higher in the more technology-savvy age group of 18 to 34 year olds, with half of all respondents wanting a text message reminder, of which seven in ten want to reply to instruct the payment amount. The survey indicates that three quarters of all UK adults believe this would give them more control over their finances.

Mobiles Tackle Card Fraud Threat

Mobile phones are set to join the battle against card fraud after Ingenico, a supplier of secure transactions, announced it is to offer UK banks further protection from fraudulent 'card-not-present' transactions. With Chip & PIN already making significant inroads against card fraud, Ingenico UK has announced that it has signed an exclusive UK distribution agreement with card fraud specialist and solutions provider Telsecure.

The agreement will see Ingenico distribute securePay which uses the UK's existing mobile phone network to provide consumers with an additional guarantee of protection against fraud. The solution works by linking a person's credit card number with their mobile phone. When a card is presented for payment a person receives a message on their mobile asking them to authorise the transaction. securePay has the benefit of requiring no architectural changes to current financial transaction systems or mobile networks.

Ingenico and OTI Form Partnership

On Track Innovations Ltd. (OTI),has partnered with Ingenico North America. Ingenico and OTI will provide secure contactless solutions for the payment and identification markets. Ingenico is integrating OTI's contactless technology with the eN-Touch 1000, as well as the i6770 and i6550 customer-activated payment terminals. Additionally, Ingenico will interface and offer OTI's flagship Saturn 5000 contactless reader as a "plug 'n play" option for merchants currently equipped with Ingenico terminals.

Smart ID Cards for Turkish Military

Oberthur Card Systems' multi-applicative dual interface Smart Cards will be issued to the Turkish Armed Forces (TSK) and their families as part of a major ID Smart Card program. Oberthur Card Systems was chosen by OYAK Bank, which is in charge of implementing the program for the Turkish General Staff. The contract calls for the delivery of several million cards, starting with an initial roll out of 2 million in 2005. The dual interface multi-application cards will include several applications including e-purse, access control, digital signature and healthcare.

FacePrint Aquires Apometric

FacePrint Global Solutions, Inc. has aquired Apometrix Technologies, Inc. This addition to FGS's portfolio provides the company with impending access to a significant and previously established client base, as well as to Apometrix Smart Card technologies. This acquisition enhances FGS's mission of being a full-service provider to the multi-application Smart Card industry.

BC Card implements ANDiS 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. Since January 2005 over 300,000 cards have been issued. These cards includes a variety of MasterCard and Visa card types, with both GlobalPlatform and MULTOS specifications supported.

Biometrics

SAFLINK and BAI Partner

SAFLINK Corporation and Biometric Associates, Inc. (BAI) have formed a strategic partnership that will offer integrated biometric physical access control solutions to the Department of Defense (DoD) and other government organisations for installations and facilities.

e-Passports Improve US Security

The US Department of State has implemented an Entrust solution to deploy the next generation of passports. The chip-enabled passports will utilise digital signatures to help improve homeland security and establish more efficient travel management. Entrust's digital signature technology is being used by the US Department of State to provide seamless authenticity and security for personal biometric information to help protect against illegal entry, fraud and counterfeiting.

Biometric ID for US Bases in Iraq

The Defense Department is fine-tuning a $75 million biometric identification system designed to improve force protection at US military bases in Iraq, according to officials involved with the project. DoD officials said the system will use biographical data, facial photographs, fingerprints and iris scans collected from Iraqis and other non-US citizens who want to work on U.S. bases in Iraq to develop ID cards that can't be counterfeited. Work on the new biometrics-based system began in late January, when then-Deputy Defense Secretary Paul Wolfowitz pushed for an improved base-access system to provide better protection for US troops in Iraq.

VeriFone and Pay By Touch Partner

VeriFone Holdings, Inc has signed a joint development and marketing agreement with Pay By Touch, aimed at furthering the adoption of consumer biometric payment solutions. Under the agreement, the companies will work together to enhance the security, encryption and compatibility of each other's solutions. In addition, both companies will offer the Pay By Touch consumer biometric payment service as an integrated offering with VeriFone's family of payment solutions. Both companies will also collaborate on new product development, marketing and sales of the integrated solutions.

Radio Frequency Indentification

The Returns on RFID Recognised

Manufacturing executives are now focused on deploying RFID technology based more on its potential benefits, rather than retailer mandates, according to recent research from Datamonitor. The Datamonitor survey of IT decision makers at 150 of the top 300 manufacturers in Europe and North America found that 60% of manufacturers surveyed are already working on RFID projects, and about 90% of those surveyed said their next RFID project will be based on systems and data integration.

Worlds Smallest 13.56 MHz RFID

Atmel has released the world's smallest and lowest-cost 13.56 MHz RFID single chip reader. Radio frequency identification (RFID) readers allow devices to wirelessly interrogate and write to tags and Smart Cards. This technology is now being used in applications such as consumer, healthcare, transportation and logistics products.

IE and LG Embed Iris Technology

LG Electronics USA's Iris Technology Division and Integrated Engineering (IE) have collaborated to integrate IE's new card readers with LG's Iris Technology for use in ICAO-compliant travel documents and e-passports. The two companies will initially work to combine two new products unveiled at ISC West: LG's third generation of IrisAccess, an iris recognition platform and Integrated Engineering' new e-Document (T=CL) reader, which was rated the fastest and most versatile OS independent ePassport reader tested at the ICAO interoperability trials in Japan last March, to provide a new standard in performance and versatility for border control and immigration management.

New UK RFID Centre

Unipart Logistics, Intermec Technologies and SAP have opened the world's first logistics centre dedicated to improving business process through the use of Radio Frequency Identification (RFID) technology at Unipart's million sq ft warehousing facility in Oxford. The facility, called the Global Enterprise Model (GEM), is a scaled down working model of the end-to-end value chain from raw material supplier to the final customers.

Market in Figures

BIO-key Announces Revenue Growth

BIO-key International Inc has reported revenues for the first quarter ended March 31, 2005 were $3.9 million an increase of 1150% from the $312,000 reported in the same period in 2004. Net loss for the quarter was $2.7 million compared to a net loss in the comparable 2004 period of $912,000 in the most recent quarter ended December 31,2004.

VeriFone Reports 2nd Quarter Results

In its first earnings report as a public company, VeriFone Holdings, Inc, a provider of technology that enables electronic payment transactions, has announced financial results for the three months ended April 30, 2005. Net revenues, for the three months ended April 30, 2005, were $117.9 million, an increase of 32% over net revenues of $89.5 million for the comparable period of 2004.

The increase was driven by a 68% increase in net revenues from VeriFone's international business and a 16% increase in net revenues from its North American business. VeriFone's acquisition of GO Software, which closed on March 1, 2005, contributed 1% of net revenues for the three months ended April 30, 2005. Systems Solutions net revenues rose 34% versus the prior year while Services net revenues rose 14%.

Pacific Reports 3rd Quarter Results

Pacific Biometrics has announced its financial results for its third fiscal quarter and nine-month period ended March 31, 2005. Revenues for the third fiscal quarter ended March 31, 2005 increased by 91% to $1,048,000 from $548,000 during the third fiscal quarter ended March 31, 2004. Net loss for the quarter ended March 31, 2005 improved 8% to $592,000 from a loss of $641,000 during the third fiscal quarter ended March 31, 2004.

Revenues for the nine-month period ended March 31, 2005 decreased by 27% to $2,492,000 from $3,390,000 during the nine-month period ended March 31, 2004. Net loss for the nine-month period ended March 31, 2005 increased 34% to $1,785,000 from a loss of $1,337,000 during the nine-month period ended March 31, 2004.

On the Move

New Managing Director at Orga

Paul Naldrett (41) has been named the new Managing Director of ORGA UK, effective June 6, 2005. Naldrett is a proven expert in the industry with international experience.

Paul Naldrett, who has a degree in business management and many years of experience in management, sales and marketing in the technology sector. In 1991, Naldrett joined Gemplus Ltd, initially as Sales Manager and later as UK General Manager, where he had primary responsibility for building the company's business in the UK. Beginning in September 2000, he was the head of the entire European Telecommunications sales operation of Gemplus International S.A. In his last position before moving to ORGA, Naldrett was General Manager at Netsize Ltd., one of Europe's fastest growing technology companies.

Ingenico CEO Steps Down

Gérard Compain

During a meeting of the Ingenico Board of Directors, the disagreements that surfaced last May between company CEO Gérard Compain and the Board on strategy and other business issues could not be settled to the mutual satisfaction of all the parties involved.

The Board of Directors formally noted that Mr. Compain no longer holds the office of CEO. Acting on a proposal by the Compensation and Appointments Committee and the Chairman of the Board, the Directors meeting at company headquarters unanimously moved to appoint Mr. Amedeo d'Angelo the new CEO. The Board has now entrusted its Chairman, Mr. David Znaty, with a number of tasks involving oversight and information.

HID Employ's New Marketing VP

HID Corporation, a manufacturer of contactless access control cards and readers for the security industry, has announced that Holly Sacks has been promoted to executive vice president of Marketing.

This promotion increaes Ms. Sacks' role to include the company's product management functions including product planning, life cycle management, program management, and technology partner integration. In addition, she will maintain her current worldwide marketing and communications responsibilities for market research, advertising, web marketing, media relations, customer communications, trade events, promotional programs, and branding.

New President at Pay By Touch

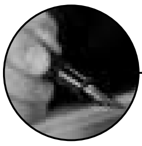
Pay By Touch has appointed John Morris as the company's new President and Chief Operating Officer. Morris will manage company-wide operations for Pay By Touch, and will lead the company's vision to transform the way the world transacts.

New Sales Director for OMNIKEY

OMNIKEY Americas has appointed David Koma as their regional sales director. In this new role, Mr. Koma will primarily focus on supporting OMNIKEY's strong OEM customer base in the Americas and the development of new OEM opportunities.

New VP of Operations for Pacific

Pacific Biometrics Inc has appointed Michael Murphy, Ph.D., as the new Senior Vice President of Operations. Murphy will play a key role in managing all aspects of the PBI service business including lab operations, client and information services, and quality assurance/control. Murphy will also work directly with the rest of the senior management team to help grow the service business.



US Leads Secure Applications Market Using Contactless Smart Card Technology

By Randy Vanderhoof, Executive Director, Smart Card Alliance

Randy Vanderhoof

The United States has taken a strong leadership position in adopting new payment and identification applications that use secure contactless smart chip technology. Smart Card technology is being widely used for many applications in other parts of the world, but recent developments illustrate how the US market is leading the way towards the use of contactless smart chip technology, especially for fast, secure payments.

MasterCard, Visa and American Express have all launched contactless payment initiatives and major retailers, such as McDonald's, 7-Eleven and CVS, have committed to deploying new point-of-sale terminals to accept the new contactless payment cards. Just recently, leading credit card issuer JP Morgan Chase announced that it would issue millions of new contactless credit cards; we are expecting other issuing banks to follow."

Industry experts agree, predicting tens of millions of contactless payments cards in the next few years. Contactless smart chips are designed to work in many form factors - a plastic card, key fob, document cover or even a mobile phone cover. They are invisible to the eye, and are easily used by waving them near a reader device or payment terminal. Research shows that consumers, issuers and merchants benefit from the use of contactless payments. Consumers enjoy added convenience, speed and ease of use, while issuers and merchants enjoy faster transaction times, increased spending per transaction, lower operational costs and penetration into the cash payment market.

Contactless chip technology is not only growing for retail payments, but for transit payments as well. Major cities around the country are moving to contactless Smart Card-based fare collection system as they upgrade their payment infrastructure. Examples include over one million contactless SmarTrip cards now in use in the Washington D.C. area for transit payments, and the technology is in various stages of deployment in 15 other major US cities including Atlanta, Boston, Chicago, Los Angeles, and San Francisco.

I see security as a primary factor motivating financial institutions' investment in the higher-priced contactless smart chip-based cards. Having the information embedded in contactless smart chips eliminates and virtually makes it impossible to replicate the card as can be done with today's magnetic stripe cards.

Contactless cards offer more security for the issuers and fewer worries for consumers because the data can't be copied to fraudulent cards. Getting more security and convenience is a win-win. These strong security features have also attracted the US federal government, which will use the same secure contactless technology chosen by the payments industry in the new electronic passport for enhanced travel security. It will also be used in new Federal employee ID cards, providing more secure building access at government facilities. The federal IDs also have a contact Smart Card chip that is used to secure access to networks and computers, provide machine-based verification of credentials and digitally sign documents.

February 2005 study from Frost & Sullivan, World Contactless Smart Card Markets, forecasts increased use of contactless technology in all regional markets. In 2004, 121.7 million units were shipped and Frost predicts this number to climb to 847.3 million in 2009. Surely the US market is going to account for a significant share of this volume, and that will give this part of the global Smart Card industry a definite American feel.

Smarter Security in the Enterprise

By Carl Norell, Gemplus International S.A.

Ever told a colleague your security password? We're all guilty of it. Chances are that if you're like much of the population, you probably don't take security seriously enough. You may even work in the security industry but there's still a good chance that you're a little too relaxed about your approach to passwords. To further underline this statement, a recent report shows that a whopping 70% of the people surveyed (Infosecurity Europe study 2004) would happily reveal their password in exchange for a bar of chocolate….Not a sweet deal for IT security departments.

More than a third of us choose passwords based on the names of our pets, partners, family, date of birth or favourite football teams. Unsurprisingly, it doesn't take a genius to work out what our passwords might be. And, of course, some of us make finding out our password even easier. How many offices have you worked in where 'secure' network passwords were written on bits of paper stuck to the computer screen? These questions may seem trivial, but they are becoming increasingly important as macro-environmental issues such as terrorism and company infiltration put pressure on organisations to beef up their levels of security and trust. What used to be an issue for IT departments has now become something that is decided at a high management level, because a vulnerable enterprise network is also an acute business risk.

Today, businesses are starting to wake up to the fact that if they don't adequately protect their infrastructure they could be targets of an attack that might prove financially costly - not to mention a major PR disaster. Paying lip service to security is no longer an option with most businesses now understanding the inherent risks of operating an insecure system. Today's widespread use of information systems and Internet technology has revolutionised the way we work, communicate and conduct business, providing phenomenal cost, time and resource savings. However, in spite of the endless advantages created by the new generation of IT-based communications, we have also become more exposed to threats on sensitive and confidential corporate data. While most companies tend to focus on external threats, recent reports claim that 80% of network intrusions result from insider abuse of network access (CSI 2003).

Standard password-based systems continually prove an inadequate approach to engage these problems, which is why alternative technologies have emerged to help us make the workplace more secure.Smart Cards are recognised by many large organisations as the most secure and reliable form of electronic identification, acting as the cardholder's access key to information and services in both on- and off-line mode.

With the ability to store, protect and modify information written to the card's microchip, Smart Cards offer unparalleled flexibility and options for information sharing and transfer. The card's dynamic ability to communicate with information systems expedites traditionally lengthy identification processes, virtually eliminating paperwork and manual data entry, while streamlining operations and reducing costs.

Within a corporation, Smart Cards allow secure and convenient access to company networks from any fixed or wireless terminal. Whether it's from an office workstation, or remote access via a VPN or WLAN for travellers and remote workers, there is a need for security in terms of access control, protecting user identity, mutual authentication, confidentiality, session integrity and reliable key exchange, in order to prevent a third party from unlawful access to intellectual property assets. The Smart Card's ability to store and manage employee identity credentials, passwords and encryption keys, in combination with a compelling and easy-to-use form factor, opens up possibilities that standard username/password solutions - both from a security and convenience standpoint - cannot compete with. Not only are basic password systems insecure, but due to their proliferation they also create additional overheads.

A recent survey shows that on average people have 4 different passwords to remember, some of us have even more.As soon as one is lost or forgotten, a company's help desk staff must spend time issuing a new one.

Figures from market analysts such as Gartner Group and Forrester Research put the cost of resetting a password at about $50, while a survey from software giant Computer Associates estimated 70% of help desk calls concern password replacements. Smart employee cards can engage this issue in a secure and user-friendly fashion. Rather than having to remember several passwords to multiple applications, employees can instead use their Smart Card to manage all of those with just one PIN. More importantly, the 2-factor authentication achieved through something you have - the card, and something you know - the PIN, drastically reduces the risk of someone else accessing your computer, as the card automatically locks your workstation when removed from the reader. Moreover, Smart Card-based solutions can add new security services beyond traditional authentication, such digital signing and encryption of e-mail, documents and web forms.

More than security: Already, a large number of corporations are using Smart Card technology for enterprise security. As mentioned above, such cards may act as a means of accessing computer networks, but the very same badge can also be used for building access, or even for basic purchases in the corporate canteen or vending machines. The beauty of this approach is that there is something in it for everyone: the card holder gets access to discounted corporate facilities, while the company has a more secure access system backed up by an audit trail of who has entered the various areas of the enterprise.

For example, IBM uses Smart Card technology for both employee security and vending. Other technology companies now adopting Smart Cards for enterprise security include SUN Microsystems, which uses a solution called JavaBadge for network and physical security.

Meanwhile, Microsoft operates a scheme that is used by more than 25,000 employees, as well as contractors and other authorised users, for physical access control and remote access to Microsoft's corporate network.Of course, we should probably expect the big names in the technology world to be consumers of strong authentication technology. But it doesn't end there. A raft of other organisations, spanning car manufacturers, pharmaceutical firms and aviation companies are using or have signed agreements to adopt the technology. Also, as the business climate changes, the use of Smart Cards as a means of employee ID is no longer restricted to the major corporations demanding volumes in the tens of thousands. The new IT era, with its subsequent impact on communication and information sharing, has significantly raised the bar for creating secure corporate environments. As a result, companies of all sizes are now beginning to evaluate the technology. A Frost & Sullivan study in 2003 found that over a third of the Fortune 500 companies interviewed plan to implement Smart Cards to enhance network security by 2006.

Multiple applications: During 2003, one of the biggest contract announcements for enterprise-wide smart cards came from Boeing, which announced plans to issue chip-based identity cards from Gemplus to more than 200,000 employees, contractors and partners worldwide over a five-year period. These cards are based on Java Card technology for optimised multi-application capacity, and will initially provide access to both systems and buildings.Of the car manufacturers embracing Smart Card technology, Mercedes in Italy has issued employees with cards to control access to the car storage area. Nissan, meanwhile, is expected to roll out Smart Card technology to 100,000 employees worldwide. These cards will be used for data storage, access control and ID applications. Volkswagen is using digital certificates based on PKI technology and smart cards to enable their employees to send secure e-mails, log in to SAP and other business systems, and create electronic signatures.

A sound decision: Interest in Smart Cards for enterprise-wide security is hotting up for a number of reasons. On the technology front, the development of multi-application cards delivered via both contact and contactless interfaces enables businesses to use the technology throughout the enterprise for a host of applications. Furthermore, smart cards have experienced a large boost in awareness in the corporate enterprise community in the last few years. A recent Frost & Sullivan report showed a 100% awareness among those interviewed, an extraordinary figure considering that only 3 years ago most companies had never heard of Smart Cards. Growing interest in the use of digital certificates on multi-application cards is also helping fuel demand. Such technical developments are making the business case more desirable - and an increasing number of organisations can see the advantage of deploying a single card that addresses needs as varied as logical and physical access control, e-purse, time and attendance management, employee profiles and access to corporate leisure facilities.

As digital technology develops, companies of all sizes have growing requirements for secure digital communications, remote access and encryption. By adding strong levels of authentication, such developments are enabling more organisations to enjoy the financial benefits of operating 'hot desk' environments. Many of the obstacles that were previously slowing adoption of Smart Cards have been now removed. Reader infrastructure has become easier to deploy thanks to standardisation of reader drivers in Microsoft operating systems and widespread integration of Smart Card interfaces into desktop PC keyboards and notebooks. In addition, integration of Smart Cards in Microsoft environments has been simplified due to increased support in Windows 2000 & XP clients and Windows 2003 server and PKI technologies. For remote authentication, Smart Cards are now able to replace one-time passwords through SSL and IPSEC based VPNs.

Another important advantage of Smart Card technology is its capability to be added into an existing legacy system for physical access. A contact chip for logical security services can easily be embedded in already issued proximity or magnetic stripe cards, hence preserving previous security investments and fully utilising current resources without disruption. Instead of being costly to implement, Smart Card technology is now emerging as a major force, thanks to its capability to host several functions on one identification device, which in turn promotes user friendliness and helps lower administration and support costs.

Fraud Expert Becomes Victim of Crime

"Credit card fraud is the fastest growing crime and it's taking over from breaking into houses and stealing because it's easier and there's no chance or very little chance of being caught." That's according to Andrew Goodwill, one of the country's leading experts in the prevention of credit card fraud. He recently found himself the victim of the very crime that his company is dedicated to preventing.

Far from being embarrassed by becoming a victim of a credit card fraud, Goodwill is adamant: "This can happen to anyone. I was shocked when I found that someone had spent $600 on one of my cards to pay for online poker in the States. This shows that no-one is immune whether they're the head of a major bank or a fraud prevention company!"

Andrew Goodwill's news comes as a new survey commissioned by Intervoice, a software firm, found that 17 % of people had stopped online banking and another 13% had given up ordering shopping on the web. CNP (Cardholder Not Present) fraud in the UK has grown nearly 50 times between 1994 and 2003 to £116.4 million.

Events Diary

July 2005

6 - 9	Sensors Expo & Conference - *Rosemont, Illinois, USA*
17 - 18	Cards Australia 2005 - *Sydney, Australia - www.worldofcards.biz/2005/Cards%5Fau/*
17 - 18	RFID World Australia 2005 - *Sydney, Australia - www.terrapinn.com/2005/RFID_AU/*
31 - 2nd Sep	Securing 2005 - *Australia - Sydney, Australia - http://svc030.bne147v.server-web.com/events/*

September 2005

13 - 15	SmartCards Expo 2005 - *New Delhi, India - www.electronicstoday.org/SMARTCARD05.htm*
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*

Chips Are Good for You!

By Gary Watts, Managing Director, Applied Card Technologies

Gary Watts

Smart Cards in the public sector: The past few years have seen growing government interest in the potential that Smart Cards can offer in terms of improved efficiency and service delivery. In addition, the security benefits of Smart Card technology enable both the cardholder and service provider to establish an appropriate degree of trust at the time of transaction. An increasing number of government projects around the world are harnessing the benefits of Smart Card technology with projects such as social welfare, identification and driver licensing. Indeed national pre-paid systems - combining public transport, public telephones, merchants and vending - have already been announced in a number of countries and road tolling speeds at full highway speeds are in the offing.

UK Deployment: Within the UK, Smart Card activity is still at an early stage, although certain vertical sectors, such as transport and finance, are actively rolling out Smart Card technology (ACT recently enabled the Cheshire County Council Travelcard to offer a fully integrated transport solution, for residents in and around Cheshire). As UK Smart Card deployment is set to rise so will the opportunity for Public sector service providers to avail of the electronic and secure delivery mechanism Smart Cards offer. The common application for most citizens is ID - the first thing a citizen typically does when interacting with public or private service providers is prove his / her identity. Indeed identity (accepting there are different levels of identity that can be established) is fundamental to citizen service delivery. The ubiquitous need to establish that trusted relationship with the citizen is best demonstrated by a quick look at common citizen transactions - all personal non-cash transactions are known by the banks; telephone companies have details of every phone call; retailers know what consumers buy; and ISPs (Internet Service Providers) know every move on the Internet.

Big Brother? This is also the era of freedom of the individual; no one likes to think of themselves being watched and tracked by some faceless government institution more concerned about trust worthiness than about looking after the needs of the man, or woman in the street. However, the truth is that service providers do not need to know the citizen to provide him / her with better-targeted information or services, but rather they need to know the profile, not absolute identity. Smart Cards, together with the appropriate infrastructure and supported by appropriate policy and legislation, provide the means to establish and improve the trust between government and citizens by protecting the privacy and confidentiality of citizens' personal data. This is widely viewed as paramount to the acceptance of electronic services by the citizen. Remember, it is not the Smart Card that is being discussed here but rather the service and the method in which it is delivered via the Smart Card; the latter will determine the citizen uptake of Smart Card technology. After all, the citizen will not buy into technology itself but rather what it can deliver.

Multifunctional: The public sector maintains a vested interest in leveraging emerging technologies in its pursuit of seamless government service delivery to the citizen. However the fragmented approach by public and private sectors providers seen to-date presents the prospect of the citizen carrying additional cards to those already in the wallet, creating a negative reaction, together with the segmentation of technology. With this in mind, greater collaboration between private and public sector is needed to achieve a common Smart Card infrastructure, from which the citizen can receive and access government services. Of course, we have seen (and ACT readily support) the growth in influence of ITSO, who are successfully using Smart Cards to integrate the use of public transport through inter-operable multi modal services.

The coming about of greater collaboration between stakeholders can only be obtained through a common strategy that attempts to reverse the current models of 'supplier and technology' push to 'consumer and service' pull. A strategy here is defined as a structured framework offering a set of rules and technology initiatives for promoting the adoption of Smart Card applications within the public sector. After all, widespread adoption and use of Smart Card applications is predicated on consumer confidence, perceived value and need in the services delivered via Smart Card technology.

Mifare Security Overview

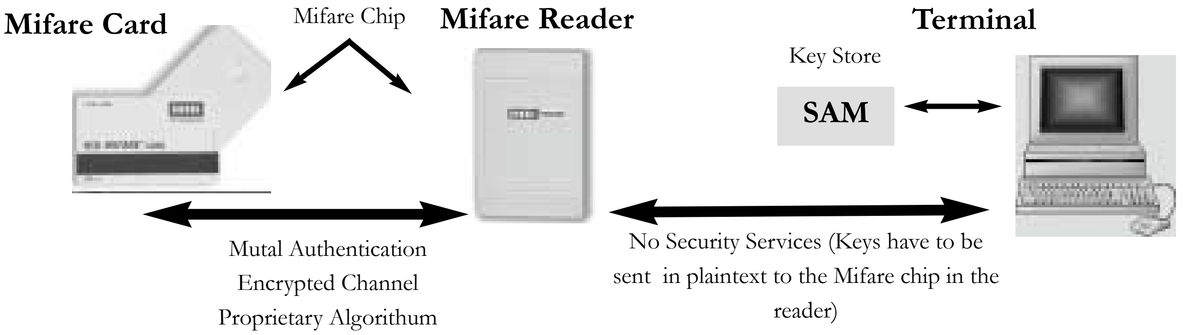
By Dr David Everett, CEO, Smart Card Group

David Everett

There has been a lot of discussion recently over the security of the Mifare card particularly because of the extended business applications such as an ePurse being proposed for this platform. Expressions such as low security are thrown around in a way that could confuse or even misrepresent the platform. In any scheme it is the overall security that matters not the individual components. It is also fundamental to ensure that the components are used in the right way, in most high visibility failures it has been a protocol or procedure failure that has resulted in the end disaster. However memory cards such as Mifare do have restricted security functionality.

The Mifare chip technology is based on a simple contactless memory device with discrete logic to provide some security functionality across the air gap with the reader (i.e. at the radio frequency level). This technology is proprietary to Philips Semiconductors and requires their IPR to be available in both the Smart Card chip and the Mifare reader. In practice this means that both the smart card and the reader need to have a Philips (or a Mifare licensed chip, e.g. Infineon) chip embedded within them. The original Mifare 1K memory was introduced in 1994 and there are now 6 chips in the Mifare range from Philips; Mifare Classic (1 Kbytes of EEPROM non-volatile memory), Mifare 4K (4 Kbytes of EEPROM), Mifare DESFire (4 Kbytes of EEPROM), Mifare Ultralite (64 bytes of EEPROM), Mifare ProX (1 Kbytes or 4 Kbytes Mifare emulation in a microcontroller chip. Total chip EEPROM including Mifare emulation memory is 16 Kbytes) and Smart MX (a Mifare ProX upgrade with 72 Kbytes of EEPROM). The Mifare ProX and the Smart MX are microcontroller based chips and provide the Mifare functionality as an emulation in the chip. These chips are used for example by the IBM JCOP30 and JCOP40 Java Cards respectively. The discussion that follows relates to the Classic 1k Mifare but the arguments would hold for most other memory cards.

Mifare Card Operation: The Mifare 1K card has its 1 Kbyte memory arranged as 16 sectors, each with 4 blocks of 16 bytes. The last block in each sector stores two keys, A and B, which are used to access (depending on the access conditions also set in this block) the other data blocks**.** The Mifare reader interacts with the card as follows; 1) Select card (ISO 14443 allows multiple cards in its field), 2) Log-in to a sector (by providing key A or key B) and 3) Read, Write, Increment, or Decrement a block (must conform to the access conditions). The Increment and Decrement operations allow the block to be treated as an electronic purse.



It is important to note that the cryptographic interchange takes place between the reader and the card and more precisely between the Mifare chip in the reader and the Mifare chip in the card. The terminal has to present the appropriate key to the reader and normally this key would be derived from a Master key stored in a Secure Access Module (SAM) at the terminal. The card ID and parameters, which are unique to each card, can act as the derivation factor. This means that each card is using a different key set to protect a particular sector. Breaking an individual card will not reveal the Master keys.The Log-in process referred to above implements a mutual authentication process (a challenge/response mechanism) which then sets up an encrypted channel between the card and the reader using Philips proprietary Crypto-1 algorithm. These security services operate at the RF (Radio Frequency) level and cannot provide any cryptographic audit trail. In essence this means that you must trust the terminal but more particularly you have no evidence if it misbehaves.

Mifare Vulnerabilities: The threats to the Mifare scheme are in three area's; 1) Attacker breaks the cryptographic algorithm, 2) Attacker effects a key exhaustion attack and 3) Attacker obtains the cryptographic keys. The scheme opens uphas an additional vulnerability in that Mifare cannot provide secure messaging. In other words because the Mifare chip doesn't have a CPU it can't cryptographically protect transactions for confidentiality, data integrity, or authentication on any form of end to end basis. This also means that message replays and deletions cannot be detected which is fundamental to most security schemes.

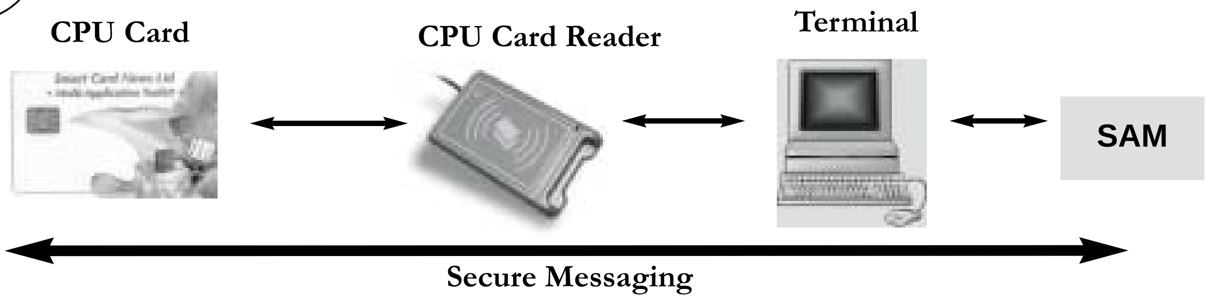
Strength of the Cryptographic Algorithm: The Philips algorithm is proprietary and has not been published. Without knowledge of the algorithm it is impossible to comment on its strength only to point out that the design of strong algorithms is known to be difficult and many acclaimed experts in the field have fallen down quite quickly when they have offered their designs for review. When a cryptographic algorithm is widely available one suspects it is only a matter of time before it gets into the public domain either due to a malevolent employee or by a reverse engineering attack on the chip. This has happened in many other cases such as the GSM world and the DVD protection algorithm. Public attacks on the Internet swiftly followed. It is believed that counterfeit Mifare chips are available from China, the companies concerned would need to have reverse engineered the chip in order to produce such chips.

Key Exhaustion Attack: The design of cryptographic algorithms is normally based on the assumption that knowledge of the algorithm is assumed. In other words the algorithm itself is adequately strong and that the security depends on obtaining the secret cryptographic keys. Assuming there is no flaw in the algorithm or its implementation then the security of the scheme falls down to key exhaustion. Key exhaustion would require an emulation of the algorithm where all the keys in the key space are tested one by one using matching plain text and cipher text. Alternatively the keys in the key space can be tested one by one against a valid implementation of the algorithm (e.g. an authentic card). The first condition requires the algorithm to be known as per the above comments and for the key space to be practically realisable.

The Mifare algorithm uses a 48 bit key, this gives a total key space of 2^48 or approximately 3 with fourteen noughts. With today's processing power this would not be deemed adequate by experts in the field. The single DES algorithm with its 56 bit key has long since been dismissed (it has been practically exhausted in 10 hours) in favour of triple DES with an effective key length of 112 bits (in practice it can be attacked with slightly less effort but still insurmountable). Today anything much less that a 96 bit key would not be deemed secure against such an exhaustion attack.An alternative approach would be to take a valid card and literally try each key in turn from the key space. This would require a card select followed by a log-in process. Just assuming this could be done in say 10 mS then an attack would take, 2^48 X 10 mS = 89194 years. This attack is clearly not viable.

Key Vulnerability: The vulnerability of the keys arise from these considerations; 1) An exposure in key management (including the terminal and reader) and 2) An exposure to an attack on the card. As mentioned previously because the keys have to be transmitted to the reader there is an assumption that the terminal can be trusted. This may be reasonable in some closed schemes such as a mass transit application but in the more general case this would not be an acceptable assumption. Apart from the obvious invasive attacks on the chip, we have in recent years, seen very successful attacks on Smart Cards by intercepting the power consumed by the chip whilst undertaking cryptographic operations. Called Differential Power Analysis (DPA) by their inventor Paul Kocher these techniques were originally applied against the RSA secret keys but later used against symmetric algorithms such as DES. Such forms of attacks may well be applicable to the Philips Mifare algorithm.

Secure Messaging: In a transaction-based scheme it is standard practice to protect the messages with some Cryptographic Check Value (CCV) or digital signature. This ensures the authenticity of the source of the message and that the message has been unchanged in transit from source to destination. This requires that the Smart Card is able to both create and check such CCVs or digital signatures. Without such security services being applied it is not easy to resolve disputes and the scheme is vulnerable to a wide range of attacks. The Mifare card because it hasn't got a CPU is not capable of creating or checking such cryptographic messages. Consider the operation of a CPU Card as shown.



Both the card and SAM can encipher messages or create and check crytographic checksums as necessary and approprate 3DES

In this case the transactions operate between the SAM (Secure Access Module) and the card. Cryptographic protection operates between these end points. Consider for example the case where you want to increment the value of a purse stored on the card. The card is set up so that the command to increment the purse has a CCV attached, the chip checks this CCV before it effects the value load process. This cryptographic CCV is created by the Secure Access Module (SAM) attached to the terminal. No where in this scenario are the cryptographic keys available in plain text. Even if the terminal is attacked with some Trojan software, the transaction records can be subsequently checked for authenticity. It is not possible for the Trojan operation to fool this process. In addition sequencing controls can be incorporated in the messages which are checked by the CPU to stop replays.

Summary: Memory cards with discrete security logic such as Mifare can offer adequate security for many closed business scenarios. In the more open transaction model the increased security functionality offered by a CPU chip with cryptographic capability is highly desirable.

Fingerprint Scanning on the Menu

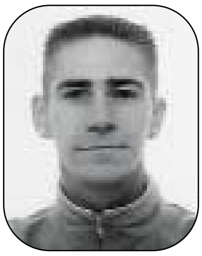
By Steve Carter, Senior Consultant, Savantor

Moves to fingerprint pupils so that parents are sent monthly bills for their school dinners could result in chaos in the canteen. Dirt, cuts and grazes on children's hands could have huge implications on the effectiveness of this forward thinking means of identification. We should be urging schools to take into account that fingerprinting in this environment is not a seamless solution, and advises that additional measures must be considered if school children are to be guaranteed their lunchtime meals and parents sure they're getting the right bills sent to them. While this system of fingerprint biometrics works best in closed systems such as schools with a controlled and fairly small population, the school canteen environment, where grubby and grazed hands are likely, is far from ideal and could have major implications not just on the smooth day to day running of the canteen, but on parents' pockets too. Using fingerprint identification with children can be tricky. As many school lunches such as sandwiches and burgers require the children to eat with their hands, fingerprints may not be identified clearly by the readers if their hands are dirty which could result in bedlam.

Biometric measurement is prone to errors in both directions. False positives, whereby one child's fingerprints would access another child's account could potentially mean that parents are presented with bills and food lists that have not been racked up by their child but by another pupil. In most cases, you can improve the error rate on one of these criteria by adjusting the sensitivity of the measurements, but this is inevitably going to be at the price of accepting a worse error rate on the other criteria. This move into fingerprint biometrics is already being pioneered at Humphrey Perkins High in Loughborough. The Live Register system is already used to speed up taking the morning register in classrooms, but pupils will now use the £50,000 custom-built biometric equipment in the canteen to charge parents for meals. The move which was inspired by TV chef Jamie Oliver's campaign for healthier school meals does have several advantages however, and Steve admits he's interested to follow the progress of the school where it's already in action.Providing the school has set the levels such that parents don't get hefty bills for someone else's child, this could be a big success. Fingerprinting at the POS in the canteen is cheaper than issuing Smart Cards are in use elsewhere. It also cuts out the possibility of the child losing the card or having it used fraudulently by the other pupils. Only time will tell whether this method of identification is suitable in a canteen environment.

ID Cards Back on the UK Agenda

By Jason Smith, Staff Reporter, Smart Card News Limited


Jason Smith

The idea for an ID Card for the UK has been up and down more times than most roller coasters. A bill to introduce a voluntary ID card was lost in the last Parliament because of the general election, but after their election win, Labour's Home Secretary Charles Clarke made it the centre piece of his program for Labours new term and has finally put our minds at rest. The government's decision to introduce a national Identity Card Scheme was announced in the Queen's Speech in May 2005 and the Identity Cards Bill was reintroduced to Parliament.

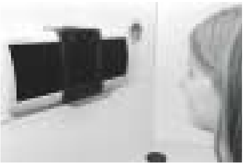
The UK Prime Minister, Tony Blair, has stated that the cards will seek to combat Britain's £40billion organised crime network - as well as identity fraud, illegal immigration and benefit scams. "Abuse of identity costs this country billions of pounds a year.," said Mr Blair. The ID scheme will be officially launched in 2008 and over the next ten years it is estimated that 49 million people within the UK will carry an ID card.

So what of this new card? Well firstly the ID card will actually double up and replace the UK's current passport for international travel. According to the UK Passport Office's official website, "For many UK citizens the identity card will be issued as passports when they come up for renewal or on initial applications." As a result, The Home Office, the UK Passport Service (UKPS) and other government departments will now work together "to start to lay the foundations for the scheme, which will establish a more secure means of proving people's identity."

How effective will these cards be? The results of the UK Passport Service Biometrics Enrolment Trial have been released this month in the wake of the government's decision to push ahead with ID cards. Atos Origin ran the trial and delivered and installed the project's equipment and software. NEC Corporation supplied its Automated Fingerprint Identification System; Identix Inc handled the fingerprint capture and facial matching technology; and Iridian Technologies Inc. provided the iris recognition technology.

The trail involved more than 10,000 participants over an eight-month period, however the more detailed research released by the UKPS focused on 2,000 "quota" people picked to match the general population, and 750 disabled people. The results of this trial, rather than justify a case for the Identity Cards Bill, actually painted a different picture altogether. The results exposed concerns over the accuracy of the biometric technology used for the ID card.

In the trial, disabled volunteers had significantly greater problems giving biological details. 4% could not register their fingerprints, compared with 0.7% of the other volunteers. Some 98% registered their face scans but nearly half could not be verified by the system. And 39% could not give iris scans, including many blind people.



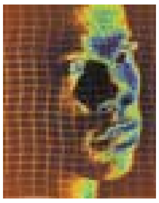
Iris verification was a success at a rate of 96% overall and 91% among the disabled volunteers. It was revealed that the facial verification system, which measures the distance between a person's features, was the least successful technology tested. The UKPS points out that the fingerprint devices used in the study increased the failure rate because they occasionally failed to record sufficient details.

The machines also had difficulty scanning the irises of dark-complexioned people and those over the age of 59. Fat fingers appeared to pose occasional problems for the fingerprint scanner. People with eye infections and individuals wearing bandages also resulted in the likelihood of a rogue result.

Another potential headache for the UKPS could be the amount of time it takes too physically gather the biometric information from individuals. According to the report, it took an average of 7 minutes, 56 seconds for the quota group to be enrolled and an average of 8 minutes and 15 seconds for the disabled group.

There are currently about 60 million people living in the UK, with approximately 80% of the adult population currently holding a passport. Between 3 million and 4 million people renew their passports each year, the UKPS has stated.

So what's the real cost of the ID Card? The overall estimated 10-year cost of the project has grown from £3.1bn three years ago to more than £584 million now as new problems emerged over the biometric technology. The Home Office now intends to incorporate three biometric indicators into the ID card - fingerprint, eye recognition and digital facial scans - instead of just one or two, after the enrolment trial placed questions over the effectiveness of certain technologies.



The Home Office has admitted that the cost of the new ID card, estimated at £77 last year, has now increased to £93. These are the figures that the public are being told. But experts at the London School of Economics (LSE) are forecasting a final bill of up to £18billion, which would mean the real cost rocketing to about £300 a head.

The LSE report says the government has hugely under-estimated the actual costs of the technology involved. They state that scanners would cost up to £4,000, not the £250 to £750 the government is budgeting for.

The government believes each card will have a ten-year lifespan but studies suggest that biometric data becomes less accurate over time. It states: "All technical and scientific literature indicates that biometric information diminishes over time, and it is therefore likely that a biometric - particularly fingerprints and facial features - will have to be re-scanned at least every five years.

The LSE claims that the government appears not to have factored in the "substantial" administrative costs of changes in personal details, handling people who do not co-operate. If human management is necessary to ensure changes are verified. These issues could add up to £4 billion to the overall cost of the scheme over 10 years. A Home Office spokesman said, "We do not accept the figures quoted by the LSE."

"Instead of funding a new Big Brother society with all the adverse implications for our civil liberties, that money should be used to invest in our public services and manufacturing where it will deliver real benefits to people." said Shami Chakrabarti, director of human rights group Liberty. Shami continued "The horrendous economic costs of the ID card scheme are clear, the social costs will be with us for decades.

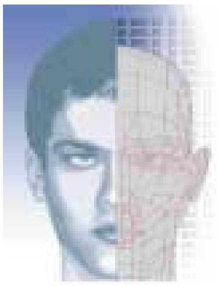
What are the potential pitfalls? The LSE revelations will put more pressure on the government, which has a reduced majority of 67 and is facing a backbench revolt. There were 22 Labour rebels at the last Commons vote and if 34 were to vote against, the government's majority would be wiped out. The Liberal Democrats oppose the scheme and although Conservative leader Michael Howard has backed the idea of a UK ID Card, he is stepping down form his position as leader of the party.

Critics of the scheme, including some Labour members of parliament, say that the new ID scheme poses a dangerous threat to civil liberties. They argue the scheme is too costly, especially as it is still unclear how effective ID cards will be in tackling crime and terrorism. Human rights group Privacy International states that these ID cards would make it impossible for many of the 10 million disabled to use public services. They estimate 600,000 will be unable to register any of their biological data on to cards, and they state that the ID Card Bill is in breach of the Disability Rights Act.

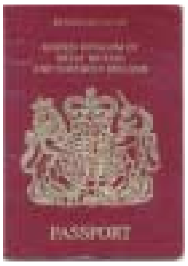
So who will get the contract? The government has not officially awarded the contact for this ID Scheme, and a spokeswoman said she knew of no timeline for doing so!

However *"The Times"* a UK newspaper has learnt that the Government has begun talks with companies for the lucrative ID contract, even though the Identity Cards Bill has not yet been passed by Parliament. The Home Office is said to have already had meetings with BT, Sun and Accenture to discuss how the scheme will operate. Other meetings are scheduled with EDS, which was responsible for the disastrous introduction of the Child Support Agency's £456 million computer system and Fujitsu.

However the Home Office denies that an "unofficial" procurement process is under way and insists that contracts for the scheme will not be negotiated until after the Bill receives Royal Assent. Atos Origin, who was the prime contractor for the UK Passport Service Biometrics Enrolment Trial, has kept quiet and has not shown any indication that they may be part of the procurement process for this actual ID roll out contract.



Conclusion: Personally I feel ID cards will be a positive step in the right direction for the UK! For one it will help towards preventing identity theft within the UK, which is an increasing threat to companies and consumers, estimated to be costing £1.3 billion a year. ID cards could also make a significant contribution to improving the efficiency of public services by making it easier to exchange data within the public sector, and between the public and private sector. Surly this is a good thing! Daily in the press we hear about illegal immigration, benefit scams, abuse of the NHS and people moan about the government not doing anything about any of this.



Currently the UK Passport has to come into line with the requirements laid down by the new US Visa Waiver Program and the standards of the International Civil Aviation Organization (ICAO), which state that all passport's need to have machine readable biometrics embeded within them. So the UK's idea of linking the British passport to the ID Card in a common format using biometrics, means that the card will provide direct USA access to the ID Card/Passport database allowing visa free travel to the USA. This hybrid card means the UK can kill two birds with one stone, a secure means of national ID and a passport with biometric indictors for hassle free international travel.

The moment the government takes steps to actually do something, using an official ID system, suddenly the public perception changes and people start to lobby and state they don't want to live in a Big Brother society! To be honest the government is always going to be under fire whatever they do, but I believe a majority of the UK will just except the change and adopt. But it is a change! And society always fears change. The Government will never be able to avoid the extremists and conspiracy theorist.

Now I'm not totally advocating the ID scheme. I do feel that the government is being a bit ambitious in its three factor biometric policy for the ID card. It is obvious there are still issues that need to be addressed for the scheme to work to its fullest potential and become a success. The results of the UK trials have showed us this! But, as the UKPS have stressed, the aim of the trails was to measure people's reaction to having biometrics data collected, ***Not*** the technology's effectiveness at gathering facial, iris and fingerprint information. However glitches are glitches and there is still a long way to go for the whole scheme to work effectively.

There is no doubt in my mind that the Identity Cards Bill will become part of UK law and ID Cards will play a key role in our daily lives within the UK. It appears the Home Office feels the same way, seeing as they have "unofficially" started talks over the contract for the implementation of the scheme. The Home Office is obviously aware of all the problems they will face once the bill has passed through Parliament but their opinion is "the technology is moving in the right direction." Lets just hope the UK's infrastructure for such a scheme to work is following suit, otherwise it could have serious consciences.

The UK Shadow Home Secretary David Davis warns: "If the proposed system is built as a center piece of our security and it fails, we will be worse off than when we started."