April 2006

Volume 15 • Number 04

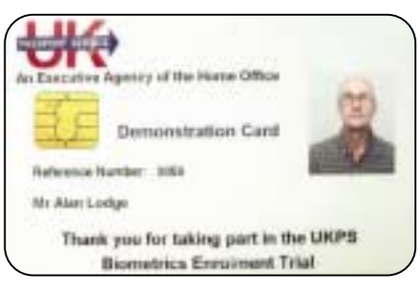
Smart Card News

Smart Cards, SIM, Biometrics, NFC and RFID

www.smartcard.co.uk

06 • GO!Card for Kazkommertsbank

06 • Payment Solution for US Parking



03 • UK Finally Set to Introduce ID Cards

14 • South Africa Smart Card Market Explodes

This Month's Lead Story

UK Finally Set to Introduce ID Cards

In This Issue

Regular Features

03 Lead Story - UK Finally Set to Introduce ID Cards
13 Events Diary

World News In Brief

04 Verifone to Acquire Lipman
04 New Russian Smart Card Centre
05 Singapore Unveils Biometric Passport
05 Beijing Adopts Transport Smart Card
04 Portuguese e-Passport
06 Electronic Driver License for Iowa
07 ACI Deploy EMV in Greece
07 Biometrics Market to Triple by 2008
08 Biometrics for Icelandic e-Passport
09 3 Billion RFID Tags for China by 2009
09 New CEO at INSIDE Contactless

Featured Articles

10 Australian Access Card or ID Card By Stealth
12 The Benefits and Limits of Smart Documents & Biometrics
14 South African Smart Card Market Explodes
15 Tackling Security the Smart Way
17 Security and Identity: The Shift to Employee Smart Cards in the Enterprise
18 Contactless Market to Soar By 2010
19 Reading, Writing and Security

© 2006 Smart Card News Ltd., Brighton, England. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, optical, recording or otherwise, without the prior permission of the publishers.

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

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@microexpert.com

Sales and Subscription Administrator
Lesley Dann
lesley.dann@smartcard.co.uk

Editorial Consultants
Dr Kenneth Ayer
Peter Hawks
Simon Reed
Robin Townend

This Issues Guest Contributors
Jason Smith
Thomas Burkhart
Arthur Goldstuck
Carl Norell
Marc Hudavert
Michelle Foong
Nathan Cummings

Printed by
Hastings Printing Company
Limited

Dear Subscribers,

Every time one picks up a journal or newspaper the hot topic is the various things we are or will be able to do with our mobile phones. Paying with the phone is now here with Asia leading the way. Residents of Caen in France have been using their mobile phones to pay for groceries and parking since October 2005 and football supports in the Netherlands will be able to enter their football teams stadium and buy their refreshments with their Nokia phones. In Hanau, in Germany commuters can pay for their bus tickets with the phone.

Near Field Communications is driving this technology, only this week Philips Semiconductors and Visa International released the results of a new usability study on NFC and contactless payments which showed that consumers liked the convenience, ease of use and "coolness" of making transactions with their mobile phone.

Sony and Philips, who collaborated to produce NFC have signed nearly 80 banks, computing and telecom companies including MasterCard, Visa, Nokia and Samsung. In Japan NTT DoCoMo have sold nearly 10 million of their credit card handsets and in the UK there are over 3 million Oyster cards in circulation which could eventually be transferred to mobile phones. And if that's not enough you can even control the phone remotely using sms command messages (www.iCamCU.com).

Having got over the excitement of the Gemplus and Axalto merger speculation is rife as to who comes next, Oberthur Card Systems and G&D both look a little lonely and China keeps appearing over the horizon. We always said that this was the decade of consolidation in the Smart Card industry and now we are over half way through. What's the betting we'll have more to report by the end of the year?

Please Note

From time to time, Smart Card News may include industry forcast and forward looking statements made by the compnaies 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

UK Finally Set to Introduce ID Cards

To say the UK identity Card has had a rough ride recently would be an understatement. The Identity Card Bill was originally expected to be passed last spring but was delayed by the General Election. This year the Bill has been held up further, after a prolonged standoff between the House of Commons and members of the House of Lords. The Bill has recently "pin-ponged" between the two Houses of Parliament as the proposal was rejected on five seperate occassions by peers over concerns including costs and whether the cards will be mandatory.

In response the government indicated that if the House of Lords continued to blocked the scheme, they would be forced into calling on the Parliament Act, a little-used law the government can use to force legislation through against the Lords' will in a time-consuming process. But using the Act in this case would bring further delays to the ID card scheme, something the government was anxious to avoid. However after Home Secretary Charles Clarke indicated he was prepared to accept a "workable compromise" then Peers and MPs finally agreed on the new legislation to introduce ID cards.

The government initially demanded that all applicants for passports in 2008 must apply for an ID card too. However under the new plans, anyone applying for a passport before January 2010 can opt out of having an ID card, but will still be put on a national database. In order to introduce compulsory ID cards after 2010 the government would need to pass a separate bill at a future date, the Home Office said. This compromise was finally backed 287-60, with only the opposition Liberal Democrats still opposing it. MPs later approved it in the Commons by a margin of 301 to 84. Home Office Minister Andy Burnham said, in a statement: "I am delighted that we have been able to give our backing to an amendment tabled by the cross-bencher Lord Armstrong. Mr Clarke said the compromise introduced "a little bit of uncertainty to the government's plans for implementing the scheme" but added that this was "manageable".

If now the Bill becomes law as expected, it would give Britain its first national identity card since World War II. The cards themselves, which will carry fingerprint, iris and face recognition technology, will become the world's most ambitious, say experts, and could be used as a model for other countries, including the United States. However initially the Home Office has revealed that bank card-style PIN numbers - and not biometrics -will be used to verify the ID cardholder's identity in some cases.

This change of direction in identity verification has attracted many critics. Phil Booth, the national co-ordinator of the No2ID campaign commented, "After all its overblown claims about the infallibility of biometrics and how highly secure its ID system will be, it turns out our identities are to be protected by nothing more than a four-digit PIN," he said in a statement. "The Home Office may as well give away all our personal data to organised criminals and fraudsters, who will always target the weakest point in a system."

The new agency that will issue passports and ID cards will be called the Identity and Passport Service (IPS). Incorporating the United Kingdom Passport Service (UKPS) and working closely with the Home Office's Immigration and Nationality Directorate, it will become operational on 1 April 2006. Mr Clarke said, "I believe that the National Identity Scheme will bring major benefits. It will give UK residents an easy and convenient way to prove their identity; deter illegal immigration and illegal working; help tackle organised crime and terrorism; and provide a means to defend against the abuse of public services. At the heart of the scheme, a secure national database linking basic personal details to unique biometric information will strengthen, not erode, civil liberties by protecting individual identities."

The success of the ID Card Bill has meant the UK Prime Minister, Tony Blair, can breath a sigh of relief. After being dogged by sleaze allegations and questions over his future in the last few months. His authority has been waning since he said he would not seek a fourth term at the next election, due by mid-2010. So to see Labour's long time plans to introduce ID cards finally come to fruition means at least a smile is on his face for the time being. Who knows? Maybe some day soon all us Brits will all be smiling wondering how we ever managed to live a normal life without our ID card.

Smart Cards

VeriFone to Acquire Lipman

VeriFone Holdings has acquired Lipman Electronic Engineering Ltd. Following the acquisition, VeriFone will become the largest global provider of electronic payment solutions and services. Lipman shareholders will receive for each Lipman share 0.5 shares of VeriFone common stock and $14.304 in cash, adjusted for a special dividend. The amount of the special dividend has not been finally determined but will likely exceed $23 million. The acquisition is valued at $793 million.

$30 Million Investment in India

STMicroelectronics is to invest an additional $30 million on Indian operations. The company also plans to increase its headcount by adding 300 engineers to its existing 1,500 employees in the country. STMicroelectronics Indian centre is its largest design centre outside Europe. The Indian design centre, based out of Greater Noida, concentrates on chip-designing applications for STBs, camera phones and Smart Cards.

ITT for South Western Rail Franchise

The UK Department of Transport has issued an Invitation to Tender (ITT) for the South Western rail franchise replacement. Bidders for the new franchise will be asked to set out how a new smart ticketing system could be introduced across the mainline franchise area from 2009 onwards. The operator of the new franchise will have to ensure the new system also accepts existing Oyster products in London zones 1 - 6. In advance of this introduction a zonal fares structure will be introduced for single and return fares across the Capital's rail network.

Common Contactless Protocol

JCB and MasterCard have agreed on a common contactless communications protocol. The protocol is the MasterCard PayPass ISO/IEC 14443 Implementation Specification, which provides for a global standardised technology for contactless payment services. Visa International made an announcement to support this protocol in March 2005, and JCB`s adoption of the specification means that these major international card brands will be basing their contactless payment applications on the same communications protocol.

New Russian Smart Card Centre

Russian-German joint venture "Smart Cards Company" (KCK) has opened a new production and personalisation centre in Zelenograd near Moscow. The joint venture was established in May 2005 by Giesecke & Devrient (G&D), Munich (35 %) and Sitronics, Moscow (65 %) with the goal of producing Smart Cards and developing Smart Card based application solutions. With the joint venture, G&D is considerably expanding its existing Smart Card activities in Russia as well as in neighbouring countries belonging to the Commonwealth of Independent States (CIS). The facility will have an initial capacity of around 30 million Smart Cards annually.

GemProx Intergated into SureAccess

Gemplus has integrated its GemProx contactless reader into the SureAccess all-weather biometric Smart Card reader from Saflink. The new integrated Smart Card reader solution is designed to comply with the US government's stringent Federal Information Processing Standard (FIPS) 201 requirements.

BQT Upgrades Fiji Airport Security

BQT Solutions has secured a contract to supply Airports Fiji Limited (AFL) with a complete upgrade of its security and access control. Airports Fiji Limited has chosen BQT's Access Control System which includes miPASS Mifare 13.56MHz Smart Cards, readers and biometric technology. Due to stringent international compliance measures put in place, this major security overhaul and upgrade will now allow Airports Fiji Limited to conform to international standards. Stage 1 involves the replacement of all the existing access control system technology. For areas requiring higher security, BQT's Biometric fingerprint reader will be used for secure user identification.

National Entitlement Smart Cards

The new National Entitlement Smart Cards will be sent out by the Scottish Executive at a rate of around 200,000 a week in the lead up to the April 1 launch of the free Scotland-wide bus travel scheme. Already 100,000 cards have been delivered. The cards give disabled people and those over 60 free travel anywhere in Scotland at any time of day on local buses and long-distance scheduled coaches. Those eligible for concessionary travel are urged to apply for the new National Entitlement Card to access the extended Scotland-wide scheme.

Beijing Adopts Transport Smart Card

The Beijing Transportation Committee has said that Beijing is ready to adopt Smart Cards for the city's transportation system. From May 1st, a travel Smart Card will allow passengers to travel by bus, subway and certain taxis with greater convenience.The electronic ticketing system is expected to be a more reliable and efficient alternative to the workers currently employed in the already overburdened transportation system.

Czech Republic e-Passport

Axalto will provide the technology which will be used in future electronic passports for Czech citizens. Under the contract, Swiss secure printing expert Trüb will provide the Czech national printing agency STC (Statni Tiskarna Cenin) with the polycarbonate data page embedding Axalto's advanced secure electronic passport technology. The Czech government intends to deliver the first electronic passports to Czech citizens by early April. Initial quantities of e-passports will be produced to meet that deadline while STC expects to ramp up production to 200 000 e-passports by end 2006. The STC currently produces between 500 000 and 600 000 passports each year. The contract includes three million pieces by 2010.

Singapore Unveils Biometric Passport

Singapore's Deputy Prime Minister Wong Kan Seng, has unveiled the BioPass, Singapores new biometric passport. The e-passport will contain a polycarbonate page that is embedded with a contactless chip which will carry the owner's facial and fingerprint biometric identifiers. This new e-passport is compliment with the standards set by the International Civil Aviation Organisation (ICAO). The aim of the new e-passport will be to enhance its border security and will be available from August 2006**.**

Portuguese e-Passport

The Imprensa Nacional-Casa da Moeda (INCM), the Portuguese national printing agency, has selected Axalto to provide the electronic covers for their national e-passport roll out. Initial quantities of e-passports will be produced and delivered to Portuguese citizens in the next few months, while the INCM expects to ramp up production to 150 000 e-passports in 2006. By late 2006, all new Portuguese passports should have the electronic capability incorporated. The INCM currently produces 400,000 passports each year.

Chinese Offices Merge

Sagem Orga is merging its two sales and marketing offices in China to concentrated its position in the Asian market and to improve their support services. Sagem Orga's Beijing office will be merging with their Wuhan (Hubei province) office that they share with their joint venture partner Tianyu.

Axalto Rolls Out EMV In Indonesia

The PT Bank Central Asia, Tbk (BCA), Indonesia's largest retail bank, has selected Axalto as its exclusive provider for the commercial rollout of its EMV cards. With this deployment, BCA pioneers EMV adoption in Indonesia with Axalto, and its customers can now enjoy greater security and enhanced payment convenience.

Contactless Cards for Singapore

NETS, a Singapore based electronic payments provider, has selected ASK to supply a new generation of its contactless payment card "CashCard". CashCard is currently used in 30,000 access points available at more than 12,500 merchants in Singapore. The CashCard features Cepass, a new contactless payment standard. Contactless technology makes it even easier for CashCard customers to make retail purchases and Electronic Road Pricing (ERP) payments, and to pay for services at supermarkets, libraries, gas stations, car parks and kiosks. NETS pioneered the concept of cashless payment in Singapore. CashCard/Cepass complies with ISO 7816 and 14443 type B standards and is based on ASK customised TanGo platform, it can work in either contact or contactless mode and thus use the already installed base of readers.

Supercom Receives Follow-on Order

SuperCom Ltd has received a follow-on order from one of its Governmental customers, following the successful implementation of an e-ID system that was delivered to the customer in 2005. The contract, which includes raw materials supply, maintenance and software support services over a period of 5 years starting from the first quarter of 2006, is valued at $1.25 million.

WorldCell Acquires Mobile-Mind

WorldCell, Inc has acquired Mobile-Mind, Inc., a developer of SIM and Smart Card technologies. Financial terms were not disclosed.

GO!Card for Kazkommertsbank

Kazakhstan's largest bank, Kazkommertsbank, has chosen Welcome to launch their new GO!Card credit card. GO!Card is an innovative credit card product designed to stimulate spending with the use of enhanced payment features such as bonus points accumulated instantly on the card's chip, which can then be spent at any participating merchant location.

Credit Cards For Transit

Peppercoin has demonstrated a prototype of a first-of-its-kind contactless mass transit fare collection system at the American Public Transportation Association's annual Fare Collection Workshop. This prototype system enables consumers to use their existing credit or debit card as their transit pass for the first time. Peppercoin's approach allows transit passengers to use their preferred credit or debit card as a ride pass, rather than purchasing a separate specialised transit pass. Riders can also use the system to prepay for multi-ride, season or period passes, which can be virtually loaded onto the rider's credit or debit card. The card can then be automatically replenished similar to toll collecting systems such as EZPass.

Electronic Driver License for Iowa

Iowa Department of Transportation (DOT), USA, has successfully completed implementation of a new and highly secure digital driver license system designed to deter counterfeiting and identity theft, curb underage drinking and enhance Homeland Security. As part of the new system the digital driver license is loaded with advanced innovations in ID security, including Digimarc IDMarc and Digimarc ExianDual card architecture for instant issuance environments.

Nigerian Driver's License Program

Liska Biometry has announced that DCS Europe has completed the installation of the upgrade to the Nigeria Driver's License program. In February, Liska signed a definitive agreement to merge with the parent company of DCS Europe, DCS. DCS Europe supplied a software solution for secure live image and data capture at 68 locations. The order included 68 custom-engineered DCS-8000 FlashSync video cameras, digital signature tablets and live fingerprint scanners. The value of the two initial orders exceeds $250,000.

Payment Solution US Parking

QI Systems Inc and Parcxmart Technologies have announced the US's first installation of a true one card solution for on-street parking, small-dollar transactions, and chip based loyalty applications. The New Haven installation incorporates QI Systems' proprietary card payment and tracking technology for Smart Card solutions. The first system installation is now in revenue service in the City of New Haven, Connecticut. QI, Parcxmart and Cale Parking Systems USA Inc. have worked together to produce this convenient multi-application Smart Card program for the City of New Haven.

John M. Fabrizi, the Mayor of Bridgeport, has announced the decision to also integrate Parcxmart Technologies' parking and local merchant Smart Card payment system throughout Bridgeport, Connecticut's largest city. The City of Bridgeport expects to replace its entire downtown on-street meter inventory with high-tech Parcxmart compliant meters over the next year. Bridgeport is the second city in Connecticut, following New Haven, to adopt the interoperable Parcxmart payment solution. Parcxmart Cards are interoperable between all participating municipalities, which means that consumers can use their Bridgeport or New Haven Parcxmart Cards for parking and for purchasing items in participating stores in both cities.

SCM Terminal Secures US Air Force

SCM Microsystems, Inc has announced that its PACT physical access control terminals are being used in a recently implemented physical access system supporting both contact and contactless secure access applications at a US Air Force facility.

HID Global is Formed

ASSA ABLOY's Global Technology Division (GTD) has announced the formation of HID Global, a new business entity focused on providing products and services targeted to the needs of key channels within the access control industry. The HID Global structure combines the HID and Indala brands of access control readers and cards, Access ID secure card solutions, Synercard digital identity and photo card management software solutions, Interlock custom card manufacturing services based in Switzerland, and BUGA electronic cylinders. HID Global products will be supported by regional offices in North America, Latin America, EMEA and Asia Pacific.

New Smart Card Merger

Enlighten Software has announced that the corporation has acquired 100% of Smart Card Marketing Systems Inc, a provider of prepaid cards, value storage card and payment transaction management. The company is now listed as SMKG, and has changed the corporation name to reflect this change. SMKG operates its head office in San Antonio, Texas and business development office in Montreal, Quebec.

Europay, MasterCard & Visa

New Axalto Personalisation Package

Axalto now provides a turnkey Smart Card personalisation offer through the Visa Smart Breakthrough program. Axalto now offers a "fee-per-card" scheme that allows banks to migrate to EMV standards without a large upfront investment. As part of the Visa Smart Breakthrough program, Axalto offers Visa member banks its field-proven personalisation package which includes data preparation, personalisation software suite for EMV cards, quality control software, as well as ongoing technical support.

New Secure Pay-at-Pump Solution

Trintech Group Plc has partnered with Dresser Wayne to supply the fuel retail market with a range of forecourt payment technology products that support the latest EMV Smart Card and PCI terminal security standards. The companies will integrate Trintech's OpenPay EMV and PCI security into the new Dresser Wayne PT 4000 EMV pay-at-pump terminal. This solution was recently granted Visa's PCI Certification for its encrypting PIN Pad (EPP) technology - the first EPP class device to win Visa's approval. Trintech will also license its PayWare software to Dresser Wayne to streamline the rollout and management of pay-at-pump systems by fuel retailers globally.

ACI Deploy EMV in Greece

ACI Worldwide has enabled the deployment of one million EMV debit cards for Emporiki Bank, Greece. This deployment, driven by ACI Smart Chip Manager, will enable Emporiki Bank's cardholders to use their EMV card for secure POS purchases, ATM transactions and international payments. Emporiki Bank issues its multi-application EMV cards using ACI Smart Chip Manager for Card and Application Management to manage and automate the process of Smart Card issuance.

Qatar Banks Achieve EMV

QCB Deputy Governor HE Sheikh Fahad bin Faisal al-Thani of Qatar has announced that Qatar banks have now complied with the EMV specifications Qatar has become the first country in the region to achieve near-total compliance of EMV.

EMV Cards for CartaSi

Axalto is working alongside Ghirlanda, an Italian provider of banking cards, to supply EMVcards to credit card issuer CartaSi. Under the contract, Axalto supplies the modules and the related digital security technology, while Ghirlanda is in charge of local card production and personalisation. The Shipment of EMV Smart Cards to CartaSi should top around 2 million.

EMV for Gulf and Middle East

Network International and Oberthur Card Systems have signed a MoU to provide a host of EMV Compliant Chip Personalisation Capabilities to the Gulf and Middle East regions.

Thai Follow-Up Order for Precise

Precise Biometrics has received a follow-up order from the Thai authorities concerning biometrics for their national ID cards. Precise Biometrics estimates that the expected revenue during a three-year period will generate about SEK 20 million. The Thailand project in its entirety means that Precise Biometrics, together with Smart Card Systems International Co, Ltd (SSI), will be delivering biometrics for the national ID card to all of Thailand's 64 million citizens.

Biometrics

Biometrics Market to Triple by 2008

Frost & Sullivan has reported that the North American biometric applications market is expected to rise to $1.4 billion by 2008, almost triple the $527 million generated in 2004. While traditional fingerprint technologies currently make up the largest portion of market revenues, new technologies such as facial recognition and iris scans hold the greatest potential for expansion, Frost says. They belive that although the market would benefit from companies developing more than one biometric application, only 15% of the companies studied offered multiple types of biometric technologies.

UK Consumers Supports Biometrics

A Unisys Corp-sponsored survey of 1,000 households has shown that two out of three consumers believe their banks should be using biometric technologies, such as fingerprint and iris recognition, to combat identity theft ahead of security tokens or Smart Cards. The survey demonstrated a surprisingly high level of support for biometrics, said Ed Schaffner, director at Unisys Corp, while also adding that the success of a biometrics deployment will depend on the geography and the application, not to mention the technology choice.

In the UK, supermarket customers at three stores in the Oxford area are currently trying a system that allows them to pay for their shopping using a fingerprint. The shoppers have a finger scan linked to their bank details with payment switched directly from personal to retailer accounts. By contrast, fingerprint biometrics systems are apparently not popular among Australians, but Schaffner said they do not mind biometrics based on face recognition for immigration and customs checks. The program works by taking a live image of a person's face and using facial recognition algorithms to match the image with a digitised image stored in a microchip embedded in the traveller's passport

Biometrics for Icelandic e-Passport

The Ministry of Justice and Ecclesiastical Affairs of Iceland has selected Viisage identity solutions to gather the multi-biometric data required to issue new electronic passports for its citizens. Iceland is one of the first countries to integrate finger and face biometrics into their ePassports. The company's technology will be used to gather ICAO/ISO-compliant biometric data (face, fingerprint, and signature) on Iceland citizens applying for electronic passports at all civil registration offices throughout the country.

Seamen Fingerprinted at US Ports

Merchant mariners from most countries whose ships call at American ports will soon be fingerprinted as part of ongoing measures to safeguard its borders, according to an official from the US Department of Homeland Security. Currently, sailors manning commercial ships that dock in US seaports only show their seamen's book when they disembark from their ship and are not fingerprinted.

Financial

Year End Financial Results for OTI

On Track Innovations Ltd. (OTI) has reported revenues for the year ended December 31, 2005 increased by 54% to $35.7 million from $23.2 million in the same period of last year. Revenues for the fourth quarter of 2005 were $9.3 million, up 19% from $7 million in the same period last year. Gross margin for the year declined to 39% from 45% in 2004.

2005 Financial Results for Ingenico

Ingenico has reporetd 436.9 million euros in consolidated revenue for 2005. On a like-for-like basis, this translates into annual growth of 3.7% and 6.8% growth in the second half. Consolidated profit from operations was 8.2 million euros in fiscal year 2005, compared to 15.7 million euros in fiscal year 2004 (IFRS accounting). Equal to 1.9% of revenues, this figure is in line with the Group's September 2005 forecasts. As part of a program to dispose of non-strategic assets announced last September, Ingenico in some cases recognised losses based on firm or likely offers received during year-end closing.

Year End Results for SCM

SCM Microsystems, Inc has reported their revenues in the fourth quarter of 2005 were $14.4 million, in line with the company's preliminary results of $14.2 million to $14.4 million and up 7% compared with revenues of $13.4 million in the fourth quarter of 2004. Revenues for the year ended December 31, 2005 were $48.7 million, compared with revenues of $49.1 million in fiscal 2004. Sales of digital TV modules accounted for 43%, PC Security products for 36% and Flash Media Interfaces for 21% of total revenue in 2005. Gross margin in 2005 was 36%, compared with 30% in 2004.

Year End Results for Saflink

Saflink Corporation has reported revenues for the fourth quarter of 2005 was $768,000, compared to $2.4 million for the third quarter of 2005 and $2.3 million for the fourth quarter of 2004. Saflink reported a net loss attributable to common stockholders of $7.6 million, for the fourth quarter of 2005. Revenue for fiscal 2005 was $7.1 million, compared to $6.4 million for fiscal 2004. Saflink reported a net loss attributable to common stockholders of $47.1 million, for fiscal 2005.

Radio Frequency Indentification

3 Billion RFID Tags for China by 2009

RFID technology has arrived in China in an unprecedented manner, with over 100 million tags shipped in 2005, and more than 2.9 billion tags forecast to be shipped by 2009, reports In-Stat. From 2005 through 2009, a major RFID application will be for human ID through China's second-generation Resident ID Card program, the high-tech market research firm says. With a population of over 1.3 billion, the issuance of RFID-tag-inlaid Resident ID cards by the Ministry of Public Security is one of the biggest RFID projects in the world. More than one billion ID Cards will be issued before the end of 2008.A recent report by In-Stat found the following: 1) Beginning in 2008, RFID tags used for items will exceed those used for resident ID cards, making the retail industry the biggest consumer of tags. 2) Incompatible RFID standards remain the obstacles for an open supply chain that crosses industries and territories. 3) Tag prices are still relatively expensive, ranging from a low of around US$0.15 to a high of over US$200.

Supercom Step into the RFID Market

Supercom aim to target the RFID market to increase their company's revenue. Newly appointed CEO Eyal Tuchman said that this was his main marketing focus in the coming year. In February this year Supercom launched the "Pure RF Movement Detection Solution". This RF Solution uses license-free radio frequencies to track a small, low-powered RF tag attached to a person or object, according to a company statement. Supercom's software then manages the transmissions and can track several items simultaneously. The system issues alerts when the tag moves in an unexpected way.

UPM Raflatac and Magellan Partner

UPM Raflatac and Magellan Technology have formed a strategic partnership to address the most challenging aspects of tagging pharmaceuticals by using RFID: high-speed issuing at pharmaceutical manufacturers, reliable identification throughout the supply chain, fighting counterfeit products and dedicated RFID labels. Due to the rapidly growing demand to tag pharmaceutical products with RFID, companies are facing the limitations of applying today's available RFID technologies to their existing manufacturing and distribution systems.

On the Move

New Executives at SCM

SCM Microsystems, Inc has announced that its Board of Directors has authorised management to pursue certain restructuring and strategic efforts that ultimately will consolidate the Company's executive offices into Ismaning, Germany. As part of the restructuring, the Company has announced that Steven Moore, the Company's current Chief Financial Officer will transition to a role, which is focused on certain strategic projects for the Company. Stephan Rohaly, Vice President, Finance, has been appointed by the Board to assume the responsibilities of Chief Financial Officer of the Company.

New CEO at INSIDE Contactless

Rémy de Tonnac, already Chairman of the Board at INSIDE Contactless, has accepted to be the company's new CEO, replacing Jacek Kowalski, who founded INSIDE in 1995 and managed the company until now. On his side, Jacek decided to focus his activities on founding new companies within the contactless and NFC space as there is a huge potential for the value creation in the fast growing contactless market. INSIDE has also appointed Charles Walton as Executive Vice President of Sales and Marketing and Philippe Martineau as Vice President of the NFC Business Line in order to help the company capitalise on the emerging markets in contactless.

New Board Members at Hypercom

Hypercom Corp has appointed Todd S. Nelson and Philippe Tartavull, to its board of directors effective April 3, 2006. The election expands the number of directors on the Hypercom board to six, five of whom are independent outside directors

New Senior Appointment at Infineon

Thomas Weber has been appointed Corporate Vice President and Head of Global Corporate Communications at Infineon Technologies AG, Munich, effective April 15, 2006, and will report directly to CEO Wolfgang Ziebart.

New Product Director at Fargo

Stephen D. Blake has joined Fargo Electronics, Inc as Product Marketing Director for secure systems.

Australian Access Card or ID Card By Stealth?

By Jason Smith, Staff Reporter, Smart Card News Limited

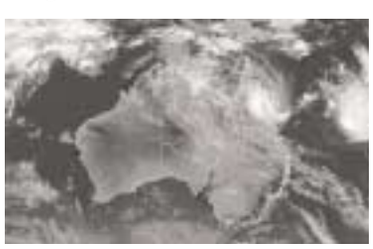
Jason Smith

The Australian Federal Government is currently planning to roll out a health and welfare Smart Card. The new card will feature a photograph of the holder and the card's microporocessor chip will also feature the holders facial image. On a voluntary basis, families and individuals will be able to include medical conditions such as allergies, blood type and whether the bearer is an organ donor. However it is said that the card will not contain biometric information such as a fingerprint or iris scan. The new card will reportedly be able to be used like an Eftpos card for every financial transaction with the Australian Government.

The submission for this new Smart Card scheme has been prepared by the Human Services Minister Joe Hockey and has the support of many government departments including the Treasury and Finance. Implementation will cost more than $1 billion over several years. Funding for the card could start in Australia's May budget. The cabinet submission for this new card includes a review from KPMG, that found that without a photo on the card, there was limited chance of effectively cracking down on fraud and it would not be worth the cost. The review by KPMG also involved a cost-benefit analysis that showed that the card would pay for itself in four years by reducing fraud and identity theft.

The scheme is being championed due to its ability to stamp out identity theft, help distribute aid after disasters, and streamline processes for benefits. Once established, this single card would replace around 19 other cards currently in use covering, among others, Medicare benefits, family tax benefit payments, all pensions and pensioner concessions, veterans entitlements, pharmaceutical benefits scheme entitlements, unemployment benefits, child-care benefits, Austudy, maternity payments, emergency relief and emergency drought assistance payments.

The Australian government each year processes over $90 billion in welfare payments across Centrelink, Medicare, aged pensions and pharmaceutical benefits. Currently, the human services department estimates around 400,000 letters a day are issued by six government agencies involved in health and welfare payments. However with this new Smart Card proposal the government has said they can save "hundreds of millions of dollars a year" in reducing the abuse of welfare payments and lowering postage and administrative costs.



The aim of the card will also be to tackle emergencies such as the recent devastation caused by Cyclone Larry, which hit Australia. In these instances, relief payments could be credited to the card, allowing families to buy supplies through hand-held ATMs that do not require electricity. The use of this new Smart Card system could have avoided the need to ferry huge amounts of cash into the region by the government.

If the proposal is successful, the government aims to start the intial roll out of cards in 2007, but this process will be a massive and unprecedented federal operation that will take several years to complete. Although the Smart Card will not be compulsory, most people will need one because it will be the only way to get money from the government. Government sources have stated that this new card was not a "Trojan horse" for a national ID card, which was being developed separately as an option by Attorney-General Philip Ruddock. Nor is it a health card storing detailed patient information. However, the technological features and photo identification required for fraud protection coupled with the fact that up to 20 million cards could be distributed to Australians over the age of 18 is raising concern that if implemented, the Smart Card could be the thin edge of the wedge for a national ID card.

Labour's Kelvin Thomson has been reported as saying that the card would be a national identification card by stealth and the proposal should not have gone as far as Cabinet without public discussion. "On the one hand you have Joe Hockey working on Smart Card technology to manage private medical files of Australians, meanwhile Attorney-General Philip Ruddock has been quietly seeking to gather support for a national identification system, and I'm concerned that by dividing the work between them and taking small steps, they're seeking to dodge media and public scrutiny with what amounts to a political pincer movement." he said. "This involves a plan to essentially introduce the ID card without proper public consultation. This is the introduction of an ID card by stealth "

Philip Ruddock

Peter Costello

However Treasurer Peter Costello replyed to this by saying that although the new Smart Card would act as an identity and authentication document for people when accessing government departments, it was not intended to be an Australia Card-style national ID. In the 1980's, after a massive public backlash, the Hawke Labour government at the time was forced to back down after they planned a national identity card in Australia. Mr Costello has said he believes the new Smart Card would suffer the same fate as its predecessor.

"The Australia Card started with quite considerable support but as it wound its torturous way through parliament and public opposition grew it was eventually defeated in the Senate when public reaction was such the government more or less abandoned it," he said. Mr Costello believes that this new proposal, which he personally supports, will not face the same fate. "I'm a supporter of a Smart Card. I believe that it will be an important addition both as to entitlements and protection of the public purse. In many respects this new Smart Card will hold much more information than the Australia Card which was proposed in the 1980s," he continued.

He believes the same backlash will not occur again because the new war on terrorism had changed Australians' attitude to new security measures, such as identity checks and airport scanning. "I do believe that recent terrorist events throughout the world has changed our perception as to what is permissible and indeed what may be necessary in order to protect civil society and civil safety," he said. Mr Costello then moved to down play fears about the security of the Smart Cards, saying institutions including banks and the military had shown that with the right technology, digitally stored information could be protected from potential hackers. Mr Costello said. "If you are prepared to invest enough, in the expertise, you can make these things secure against hackers". He also rejected suggestions that Smart Cards were an invasion of privacy, saying the data they would store was already used in hard copy format.

From this we can see that even though this Smart Card proposal has the potential to streamline services and reduce costs, to date the government hasn't really done enough to address the issues of security and privacy of data, or provide total confidence that information stored will not be used across government agencies and departments. Due to this the opposition of the card are still calling for a broader public debate on whether or not these Smart Cards should be introduced. However with the government's persistence to distance this proposal from the Australia Card and the accumulating backing from cabinet ministers such Alexander Downer, who urged a national boycott of the National ID card in the past, this means of improving access to benefits seems to be on a path to success, even if it is a slow one.

To sum up the fate of this new Smart Card proposal, Australian Prime Minister John Howard said "I've had a number of discussions with Mr Hockey and my own department about it. I can see advantages, but the debate is yet to be exhausted, and we'll see what comes out of it."

But the big question still remains; if they distribute this card to everyone over 18 throughout Australia, and it has the ability to hold biometric data, then why would they need another card as identification? Surely that's just duplication of resources and a waste of money! So if cabinet passes this new card scheme it will be interesting to see the fate of Mr Ruddock's purposed identification card. Maybe Kelvin Thomson is right, maybe this is all part of an elaborate scheme to introduce an ID card by stealthily bypassing public consultation. Lets wait and see!

The Benefits and Limits of Smart Documents & Biometrics

By Thomas Burkhart and Mr Georg Hasse, Cross Match Technologies

Thomas Burkhart

There are various ways to secure a document against counterfeiting, but there is no way so far to tell if the holder of a genuine document is the legal owner of this document! Biometrics promises to fill exactly this gap. If we want to use biometrics in combination with machine-readable travel documents (MRTD) - without a central database - we need a way to store the biometric identity of the legal owner somehow on the document. As there currently is no standard for exchanging biometric templates, it is necessary to store the original biometric image (face, finger, iris). Therefore we are in need of new solutions.

ICAO (International Civil Aviation Organisation) recommends since this year that all newly issued documents shall include a high capacity, contactless integrated circuit chip also called RFID (Radio Frequency Identification). According to these recommendations, the chip should have a minimum of 32KB memory although certain user groups already claim that such a capacity is not sufficient. Data on the chip will be organised in a Logical Data Structure (LDS) and will be protected through Private-Public-Key infrastructure.

Georg Hasse

The LDS is a structured standardised repository for data that guarantees global interoperability. The printed MRZ (Machine Readable Zone) data on the passport page is mirrored in the LDS. At least one biometric feature will be stored in the LDS. In its Berlin Resolution, ICAO has recommended that if only one biometric feature will be stored, it should be the digitally stored facial image of the document's owner. If more than one biometric feature is stored, ICAO suggests the usage of standardised digital fingerprint and/or iris images.

To read the data from an RFID, the document containing the chip must be brought into a range of 2-4cm to an RFID reader. For that purpose, any RFID reader that supports ISO/IEC 14443 (proximity) and ISO/IEC 15693 (vicinity) can be used. To read 40KB currently takes between 3 and 0.75 seconds. The RFID allows for an easy update of existing data as well as the storage of additional data, as for example electronic visas. The data stored in the chip has to be secured against alteration and counterfeiting. For this purpose, ICAO demands the usage of an asymmetric encryption similar to PGP (Pretty Good Privacy). When issuing a new document, the government encrypts the LDS with a "private key", thus serving as the country's central signing authority. This "private key" must be kept absolutely secret, while the government distributes the "public key" to the border control authorities. This procedure ensures that they can read the data, however, they are not able to create new documents. ICAO announced that they would support this project by distributing the respective keys. (In this case, the terms "private" and "public" are used the opposite way compared to standard PGP).

As successful as the RFID may be, the system still has some limitations as well. Currently only a few transponders on the market have a storage capacity of more than 16KB. Current RFID chips support only 106Mbps; therefore it would take 3 seconds to read 40KB. However, faster chips will be available in the near future. It is important to protect the chips and antennas against damages caused by stamping and crimping during the entire lifespan of the travel document. The RFIDs have a number of advantages compared to traditional (paper based) documents. First of all, the RFID can store much more data than any barcode and can be read very reliably. Secondly, since biometric applications demand so much storage, no other technology apart from the RFID could fulfil the necessary requirements. Thirdly, RFIDs are very secure concerning counterfeiting as long as the "private" key is kept secret. However, an unauthorised person gaining access to such a "private key" can make reliable checking of a document impossible. In such a case, a forged RFID cannot be distinguished from a genuine one. Another important advantage is the cost: pure RFID readers are very small and inexpensive.

Having described all the advantages of the RFIDs, the question arises whether we are still in need of traditional documents. The answer is definitely YES, because a trained person can always distinguish a forged traditionally secured document from a genuine one even if the embedded RFID is forged. In addition to that, an official should still be in the position to check a travel document without the help of an electronic device. Given these circumstances, is it necessary to still have optical document readers? That question can be answered clearly: YES! If we still need traditional documents, we still need optical document verification and reading devices as well. Other reasons why these devices cannot be completely disposed of is the possibility of the RFID being damaged or the "public key" of a country not having been distributed to all checkpoints. Documents of most countries will not even be equipped with an RFID within the next 10-15 years, in some cases even longer. In this case, there must still be a possibility to verify the genuineness of a document. Even if a document does not contain an RFID, a comparison between the holder's face and the printed picture on the passport page can be carried out.

However, the new smart documents can also cause problems during the control process due to the new technology. It is possible that border control officials will not trust information they cannot see. Another possible scenario is that the RFID is not readable. In such a case, how can the validity of the document be checked? One could imagine the opposite case as well: The document might look as if it was forged but the RFID is valid nonetheless. These unresolved problems will require some attention during the months and years to come. Solutions and accepted procedures will have to be found and agreed upon.

Meanwhile, let us have a look at the ideal document verification scenario: There should be a device that automatically reads the document optically and, at the same time, reads out the RFID including the biometric image. The device should then compare the data of the printed page with that of the RFID and verify traditional security features (e.g. UV, IR). Furthermore, the device should inform the user about any discrepancies between the two sets of data. Capture devices for biometric data, such as cameras or live scanners, should be attachable to the device. The biometric match should be made inside the device so that no external networking is necessary. In addition, the device should host the border management application as a thin client, so that there is as little technology required at the checkpoint as possible. To sum it up, smart documents will increase security provided that the respective infrastructure is established and the users are trained accordingly.

Events Diary

May 2006

2 - 4	CardTech/SecurTech 2006 - *San Francisco, USA*
6 - 8	The CardEx International Conference - *Cairo, Egypt - www.egytec.com/home.htm*
17 - 19	8th Smart Cards + Smart Label (RFID) Expo- *Beijing , China - www.scfc.org.cn*
22 - 23	Cards Middle East - *Al bustan Rotana, Dubai - www.worldofcards.biz/2006/cme*
24 - 25	RFID Global Partnering Symposium 2006 - *London - www.rfidpartnering.com*
30 - 1st June	The 9th International Fair of Smart Cards - *World Trade Centre, China - www.smartcards-china.com*

June 2006

8 - 9	The Electronic Passport Forum - *Paris, France - www.electronic-passport.com*
13 - 14	CardEx Asia 2006 - *Kuala Lumpar, Malaysia - www.cardexasia.com*
14 - 17	CardExpo 2006 - *Lagos, Nigeria - www.cardexpoafrica.com/index_wa.htm*
26 - 27	Contactless Cards - *London - www.smi-online.co.uk/events/overview.asp?is=8&ref=2351*
21 - 22	Extended Retail Solutions Symposium 2006 (Europe) - *Munich, Germany - http://erssummit.extendedretail.com*
27 - 28	Smart Label Summit Americas 2006 - *Miami, Florida, USA - www.smartlabelsevents.com*

South African Smart Card Market Explodes

By Arthur Goldstuck, Managing Director, World Wide Worx

Arthur Goldstuck

The Smart Card industry is poised for an unprecedented explosion in South Africa, with three large-scale rollout began in 2005 and several more waiting in the wings. More than 50-million Smart Cards were issued in 2004 and 2005 combined. And, by 2009, more than 100-million Smart Cards will be in active use in South Africa. From 1 January 2005, all new credit and debit cards issued in South Africa are required to be Smart Cards, meaning a roll-out of a minimum of about 12-million Smart Cards to banking customers over the next five years.

The single biggest Smart Card project this country will see, however, will be the new Home Affairs National Identification System, known as HANIS, which will require the replacement of identity documents with around 30-million Smart Cards - one for every eligible South African - during the same five-year period.

Telkom and the mobile network operators are expected to add another 20-million cards in 2005 alone, through the issue of new prepaid and SIM cards, while all pension payments handled by the Department of Social Welfare are expected to move to a Smart Card system from 2005 onward, following successful projects in most provinces. More than a third of all South Africans already hold a Smart Card in their hands indirectly, thanks to the SIM cards in their mobile phones. Now they will start getting to grips with the card itself as it becomes an everyday tool.

The reason for the explosion in Smart Card usage is simple: it is more secure than any other identification technology that is economically viable and available, can contain updateable information ranging from personal details to fingerprints to identification photos, and is far less prone to forgery than existing systems. We will begin to see an unprecedented range of applications for Smart Cards from 2005 onward, starting with the telecommunications cards we already have and extending to financial services. But it will not be long before almost every service that requires some form of identification or secure payment will take advantage of Smart Card technology. The massive Smart Card rollout will require major upgrading and acquisition of new equipment - all retailers who accept cards will have to be ready for Smart Cards next year - as well as a clear understanding of what Smart Card technology is best for what purpose.

Not only do we have memory cards and microprocessor cards, but each of these offers two different categories of technology. Contact cards and contactless Smart Cards dictate what kind of card reader has to be in use, since contact cards must be inserted into a reader, or swiped, while contactless cards only have to be passed near the reader." Contactless cards have both a microchip and an antenna embedded in the card, which allows for it to be detected at a small distance by the reader.

Many South Africans already use such technology without realising it, for accessing restricted areas, paying for road tolls, or managing agricultural stock control. The most promising applications we have seen so far involve pension payouts. It shows how the technology can be used today by the most disadvantaged members of our society in the remotest areas and with a minimum of information at their disposal. Imagine how much more it can do for South Africans in the future."

www.theworx.biz

Tackling Security the Smart Way

By Carl Norell, Marketing Communications Manager, Gemplus

Carl Norell

Facing new threats: 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 relaxed about your approach to passwords. Surveys show that more than a third of us choose passwords based on the names of our pets, partners and family, date of birth or favorite football teams.

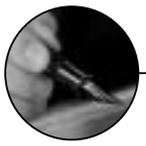
Unsurprisingly, it doesn't take a genius to work out what our passwords might be. And, of course, some of us make finding out our password even easier. How many offices have you worked in where 'secure' network passwords were written on bits of paper stuck to the computer screen? This may seem relatively minor to those of us guilty of such misdemeanors, but the issue has grown in importance as macro-environmental issues such as terrorism and company infiltration put pressure on organisations to safeguard their IT systems. They need to secure the e-business flow, ensuring that data, networks and applications are protected, and that each individual's access to the network and the facilities is verified and authorised. Hence, 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.

Standard passwords not good enough: Standard password-based systems continually prove to be an inadequate approach to tackle enterprise security problems. Not only can a password be easily guessed by the internal hacker, as they normally are only between four and eight digits long, but they can also be easily cracked by using a simple software program widely available on the Internet. The fact is that any half decent cracker will figure out your network or web-application password in a matter of minutes.

In addition to high security risks, password management tends to be an expensive affair. Gartner Group, an IT research company, has shown that 20 - 50% of calls to a company's helpdesk are related to password resets. Couple this with figures from Forrester research, stating that each call for a single password reset clocks in at about $70, and before you know it a sizable chunk of your IT security budget is wasted. Thus as compromising on security is no longer an option, most businesses are starting to grasp the inherent risks and costs and take appropriate actions. As a result alternative technologies have surfaced to help us make the workplace more secure and convenient.

A smarter approach to security: In recent years the Smart Card has emerged as the security device of choice for strong authentication and management of passwords in the workplace. By now, the Smart Card format is familiar to most people. In the course of our daily lives, we encounter Smart Card technology to one degree or another - GSM mobile subscriptions, credit cards with chip 'n' pin, Pay TV subscriptions and more. Within a corporation, the Smart Card acts a tamper-proof and highly versatile miniature computer with the core function of protecting company resources from unlawful access. Smart Cards are used as part of an identity management solution for the storage and processing of user credentials and authentication to secure networks, applications, web servers, email communications, Internet transactions, and more. They combine the privacy, integrity and authentication functionalities provided by cryptographic algorithms with the simplicity, portability and convenience of the 'card' form-factor. Private keys, digital certificates and all sorts of personal information can be securely stored, thus preventing fraudulent use of the user's electronic identity.

Double authentication: The key strength of Smart Cards lies in the ability to add an extra layer of authentication by combining the knowledge of a PIN with the possession of a card. Today people are all more or less used to the idea of a PIN (Personal Identity Number), which we enter when turning on our mobile phone and using an ATM card. We are also more capable of remembering a 4-digit number than a complicated string of characters defined by our IT departments. Smart Cards allow us to maintain the user-friendliness of basic PIN codes while still doubling the security.



When logging on the network, the employee is asked to insert their card into a reader (inbuilt or as an accessory) and then enter a PIN. This way, they are authenticated by something they have, i.e. the card, and something they know, i.e. the PIN. Both must be matched accurately before access to the corporate network is granted. The card can also act as a 'password wallet' eliminating the need for employees to remember several passwords to multiple applications, as all of those can be accessed and managed with just one PIN protected card. Finally, the card automatically locks the work station when removed from the reader, which heavily reduces the risk of someone else gaining access in your absence.

Host multiple functions: Many Smart Card-based solutions have two main functions: physical access to buildings and departments therein, and also logical access to the network. This is why a large number of corporations are using Smart Card technology for enterprise security. But beyond these traditional authentication and access control functions, it is easy to deploy further applications and value added services once that Smart Card infrastructure is already in place. Such features include encryption of e-mail, digital signing of documents and web forms, attendance management, e-purse, etc.

At Gemplus, we use our own technology to enter the building, to restrict access where necessary, to log on to the network and encrypt emails, but it doesn't stop there. We can use the very same cards in our canteen and in vending machines in order to buy lunch, coffee etc. We were even given a euro each, already credited onto our badges, when the system came into play, by way of introduction to the new services available.The beauty of this approach is that there is something in it for everyone: the cardholder 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.

A sound decision: Interest in Smart Cards for enterprise-wide security is growing 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 100% awareness among those interviewed, an extraordinary figure considering that only a few years ago most companies had never heard of Smart Cards. Growing interest in the use of digital certificates on Smart Cards is also helping fuel demand as it allows portability of private keys rather than locking them onto a workstation, thus making PKI (Public Key Infrastructure) technology more practical. 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, more organisations can enjoy the financial benefits of operating so called 'hot desk' environments, where workstations are securely and privately shared between many employees.

Many of the obstacles that were previously slowing adoption of Smart Cards have been removed. One good example of this is the reader infrastructure which 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. Furthermore, 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. Thus, instead of being costly and difficult to implement, smart card technology is now emerging as a major force in the corporate community.

As a result, smart employee cards have become a household staple among large enterprises, which are recognizing the many benefits enabled by the technology. World leading companies including Barclays, Boeing, IBM, Microsoft, Pfizer, Sun Microsystems, and many more, all operate a Smart Card-based identity management system for secure employee access to networks and facilities. While the security advantages of Smart Card technology are impossible to argue, the Smart Card is also unique as an identity device in the sense that one can update information on the card after it has been issued, a.k.a. "post-issuance". By utilising open Java Card technology, the issuer can add, update or remove employee applications and data on the over time, hence controlling and extending the card's life-cycle. This enables huge advantages for the issuing enterprise, who can easily introduce new technology and functions to its employees without having to replace their cards. Needless to say the smart employee card is here to stay, and the sooner corporations learn this, the better its management will sleep at night.

Security and Identity: The Shift to Employee Smart Cards in the Enterprise

By Marc Hudavert, Vice-President & General Manager, ActivIdentity EMEA.

Marc Hudavert

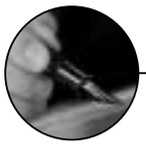
How many forms of identification do you carry around? Passport, driving licence, ID card to enter your place of work, credit cards, debit cards. How many usernames and passwords do you have to remember in order to access the information you need at work every day? One set for network access, one for email access, one to log onto your favourite daily news site, one to use each application on your PC, another to check your bank balance at lunchtime, then one more to check your private Hotmail or Yahoo! account; maybe then you head home and log into your Skype account using yet another password to speak to a friend overseas.

It's not surprising that helpdesks across the world are inundated with calls to re-set passwords for employees and customers. It's even less surprising that we continue to use our dates of birth or a pet's name for all of them because they're easy to remember, and that this makes us more susceptible to identity theft. There is a clear need to consolidate different methods of authentication, in order to reduce fraud as well as ease the headache for individuals required to remember so many different credentials.

ID theft and beyond: Some UK-based organisations are starting to invest in increasingly sophisticated identity authentication technology, with the financial services sector leading the way. Banks including LloydsTSB and HSBC are already starting to roll out token-based solutions, which combine the traditional username and password with a one-time code generated by a keyring-style token, in order to combat ID fraud. However these deployments focus on their customers in a bid to protect them from sophisticated key-loggers and phishers, whilst employees have been all but overlooked. This is even more noticeable in other industry sectors where take-up of two-factor authentication amongst has been even slower. Aside from the password headache and threat of identity fraud, there is a pressing need for enterprises to become more transparent in their business dealings. Sarbanes-Oxley is casting its shadow over enterprises that operate on the global stage, forcing them to be more accountable. US-based regulations, such as HIPAA in healthcare and FFIEC in financial services, are starting to mandate that companies have systems in place that protect information and can legally prove the identity of individuals involved in certain activities. Regulatory bodies in the UK, such as the Financial Services Authority, seem set to follow suit. In the not too distant future, passwords and tokens simply won't be enough.

Smartie-pants: Smart Cards take strong authentication into a new realm, because they are capable of storing multiple credentials and have a vast number of uses. One card, issued by an employer, can allow staff access to office buildings as well as the IT network, thereby combining physical and logical security into one device. Multiple applications on the network can be accessed via a single sign-on mechanism, removing the user's headache of remembering many different passwords and cutting down calls to the IT helpdesk for password resets. What is more, remote users can access the network with the same level of security as office-based workers using the same card. Not only that, Smart Cards can be used to make a digital signature, which in future could make electronic documents permissible as evidence in a court of law. As we continue to move rapidly towards a completely digital age with complex regulations to adhere to, the ability to prove beyond reasonable doubt that an email or document was sent or received will be essential, not just a nice-to-have. There are many non-security-based applications of Smart Cards such as operating a cashless environment within the business, which could see staff using the same cards at the canteen and for vending machines.

Public and private partnership - the future? Increasingly, private enterprises are working with government bodies to deliver commercial and public services to citizens via Smart Cards, because they are capable of storing multiple credentials for access to different buildings, systems and accounts. Further development depends on public and private sector investment in new infrastructure, and the most cost-effective approach is to work together in order to develop the technology then use it according to the needs of their individual organisations.



The North East Regional Smart Card Consortium (NERSC) for example, created and primarily financed by Sunderland City Council, allows students at the local college in the area to use the same Smart Card to access their college building and IT network. A number of locally-based companies are already working with the Consortium to provide access to their own offices and computer systems with the Smart Cards. The cards will soon allow local residents to use public transport, in much the same way as London's Oyster scheme. In addition, the e-ticketing functionality could enable local football fans to buy tickets for matches and enter the ground to watch them. This is a prime example of a Local Authority working with local enterprise to deliver services to citizens and could become a model for the roll-out of regionally-run schemes.

Further afield, the US Department of Defense has issued 10m Smart Cards to date to personnel stationed all over the world. Soldiers use them as personal ID, as passport ID at checkpoints, to access buildings, networks and PCs according to their rank, make a digital signature and even to pay for goods to avoid the need to carry cash. The potential benefits of stronger identity authentication technologies to commercial and public sector organisations alike are immense, encompassing increased efficiency, compliance issues and better access to public services for all. Surely it's about time that UK businesses started to realise them?

Contactless Market to Soar By 2010

FROST & SULLIVAN

By Michelle Foong, Research Analyst, Frost & Sullivan Asia Pacific

Successful projects around the world, like transit and ID programs in APAC, along with advances in the U.S. payments market, are stirring up interest in the rest of the world where these applications are slower to take off. Lessons learned and flourishing use of these contactless cards in some countries give confidence to other regions to follow suit. In March 2005, MasterCard International and Visa International announced that they had reached an agreement to use a common communications protocol for contactless payment cards and devices. This is expected to increase and ensure interoperability between contactless payment cards and devices. The use of a common protocol for conducting contactless payments will enable vendors to streamline product development and testing, leading to reduced implementation costs and faster time to market for financial institutions and merchants. With a common protocol in place, merchants are expected to have the assurance that a single point of sale terminal may support multiple payment brands, and would require less time for terminal programming and testing.

Our analysis reveals that in 2004 the total unit shipment for the world contactless Smart Card market was 150.56 million units and expects to reach 1.17 billion units by 2010. As the dominant areas of use in contactless Smart Cards become more established areas such as banking, government, telecommunications and security, people will start to realise that the benefits of contactless are far reaching. Other areas like medical, gaming (betting) and emergency services are starting to look into the use of Smart Cards to fill the need for security, volume and speed in their sectors. For example, in healthcare and emergency services, medical personnel need to be identified in an instant to ensure that the efficient flow of medical services is provided." National IDs and passports are areas of massive implementations, where places like United States, China and Europe have sufficiently large populations to generate demand for contactless technology. Where mandates are imposed, the pressure to comply is significant.

Other agencies relating to defence, transit and government services are pushing for contactless rollouts to cope with security and efficiency needs. Progress in National IDs and passports in countries which were previously not as technologically superior as first world countries are showing that the educational barriers have come down significantly in many places, like projects in China, Brazil, Macedonia, Malaysia and Thailand. Unlike other technological advances, some of the more advanced countries are learning from the experiences and successes of these countries before they take the leap themselves. Consumers are starting to integrate contactless technology into their way of life without the apprehension and anxiety previously seen. Consumer rights groups and privacy concerns in more advanced countries continue to slow down the growth in some areas. Especially with national ID cards involving the government and the use of biometric features for security needs, this area needs to be addressed to prevent potential lawsuits and human/consumer rights violations.

Reading, Writing and Security

By Nathan Cummings, Director of Product Line Management, HID Corporation

Contactless Smart Cards precisely balance security and user-friendliness, but they're not all created alike. If you've ever waved a contactless Smart Card in front of a door lock, metro turnstile or store checkout, you know that it's fast and convenient. If you haven't, chances are good that you will soon. Contactless technology is already widely used in Asia, Europe and North America. Train and subway systems around the world use contactless Smart Cards for transit payment. Major U.S. cities such as Boston, Chicago, Washington D.C. and San Francisco are implementing contactless Smart Card-based Automatic Fare Collection (AFC) systems.

In the United States, contactless payment systems are used for a wide variety of applications. For example, Chase Bank U.S.A. recently announced a broad roll-out of "blink"-branded credit cards, and KeyBank is offering debit cards branded with MasterCard's PayPass. Both products include contactless payment technology. Another important application for contactless Smart Cards is physical access control, where contactless S0mart Cards are increasingly accepted as the credential of choice. Just as proximity technology brought advantages over magnetic stripe and weigand card technology 20 years ago, contactless Smart Card technology today is bringing new advantages over proximity. Contactless Smart Cards are both robust and flexible, giving security professionals the ability to reduce maintenance costs, improve employee productivity and increase security. As this technology takes hold in the security industry, it is important to understand the standards that have emerged for contactless Smart Cards. Following, we will review the technology options, discuss the differences and review which standards are best for different applications.

About Contactless Smart Card Technology: Contactless Smart Cards use electromagnetic induction to transfer information between the card and a reader that is located at a few inches or feet away. Contactless Smart Cards don't require a battery, so the card will not stop working after a few years. The lack of physical contact eliminates to wear and tear, so the contactless Smart Card does not have to be replaced often.

For example, a credit card that uses a magnetic strip (also known as "magstripe") stops operating correctly much earlier when compared to a contactless Smart Card. Another key difference between today's contactless Smart Cards and cards that use magstripes, proximity Radio Frequency Identification (RFID) or older technologies is the flow of information. Although the latter can be loaded with information - such as an account number - they are "read-only" because that's a one-time programming process. By comparison, today's contactless Smart Cards are "read-write" because they can be programmed and reprogrammed - although only by authorised sources and then in a tightly secured process.

The Power of Flexibility: Here is why contactless Smart Cards provide power with flexibility: Although contactless Smart Cards look like their magstripe and proximity cousins, they contain a small integrated circuit with on-board storage space and far more security. As a result, not only are contactless Smart Cards capable of storing more information, they are also able to interact with card readers and accessory systems, rather than merely serving as mute subordinates. These abilities directly affect the return on investment (ROI) and total cost of ownership (TCO) for the companies that use or issue contactless Smart Cards.

For example, a contactless Smart Card can host multiple applications, so the cost can be spread over multiple initiatives. In the case of an enterprise, a single Smart Card could be used for purposes such as identification, access to buildings and IT systems, or paying for lunch in the company cafeteria. Contactless Smart Cards improve ROI and lower TCO by providing flexibility to host multiple applications, including those that weren't envisioned when the cards were initially deployed. That flexibility is particularly important for contactless Smart Cards used initially for access control, but gradually enhanced to support revenue-generating applications.

ISO 15693 and 14443: Although contactless Smart Cards are ideal for a wide variety of applications in areas such as retail, government, security, transit and financial services, choosing the right contactless Smart Card is key for ensuring a successful deployment. That's why it's important to understand the major standards and how they determine the differences between one contactless Smart Card and another.

The two major contactless Smart Card standards today are International Organisation for Standardisation (ISO) 15693 and 14443. Both standards define the protocols, data formats and other features necessary to ensure that contactless Smart Cards can communicate with readers and applications that adhere to the same standard. However, it's important to note that as far as reader-writer devices are concerned, supporting one standard does not lock out other options.

For example, HID's iCLASS contactless Smart Card readers work with cards based on 14443A, 14443B2 and 15693, as well as related protocols such as MIFARE. ISO 15693 is the basis for contactless Smart Cards designed for use over distances of up to one meter (3.28 feet). This range makes them a good fit for applications such as physical access or controlling entry to a parking garage, where it's inconvenient for users to open their door or roll down a window just to get a contactless Smart Card close enough to the reader to work. By comparison, contactless Smart Cards based on ISO 14443 are designed for a range of about 10 centimeters (3.94 inches), so they are a good fit for applications such as vending machines.

Another advantage to contactless Smart Cards is data speeds: Because an ISO 15693 contactless Smart Card can transfer data over a longer distance, its throughput is about one-quarter the speed of ISO 14443's rate. However, contactless Smart Cards usually transfer small amounts of data, so throughput isn't a deciding or noticeable factor. ISO 15693 has helped contactless Smart Cards' cost structure: The ISO 15693 standard serves as the foundation for a wide variety of applications outside of contactless Smart Cards, such as airline baggage tracking and supply chain management. Such an extensive adoption means more ISO 15693 components, which will reduce prices as their volumes increase, a plus for contactless smart card vendors and their customers. That is why contactless Smart Card solutions based on ISO 15693 typically cost less than models based on technologies such as MIFARE.

MIFARE: A widely used technology isn't the same as a standard. For example, although MIFARE technology is used in many contactless Smart Cards, it's not a standard, nor is it the only read-write technique available. The current trend is toward using ISO 14443 for transit applications and ISO 15693 for tasks such as access control. For example, when HID introduced a contactless technology that was optimised for access control called iCLASS, the company selected the ISO 15693 standard because of its advantages.

Although ISO 15693 uses the same 13.56 MHz band as MIFARE and offers the same features, there are some key differences. For example, ISO 15693 supports a read range of up to five times longer than MIFARE. That extra distance lets ISO 15693-based contactless Smart Cards tap into a wider range of applications. iCLASS also has tougher security, thanks to its 64-bit key. By comparison, MIFARE uses only a 48-bit key.

In conclusion, the bottom line is that although contactless Smart Cards are ideal for a wide variety of security and non-security applications, picking the right contactless Smart Card is critical for a successful implementation. That's possible only with an understanding of the standards and how they affect factors such as ease-of-use and security. For physical access control in particular, choosing a more secure, simpler, diversified and multi-faceted Smart Card technology based on 15693, such as HID's iCLASS, provides a competitive edge with endless possibilities.