July 2006

Volume 15 • Number 07

Smart Card News

Smart Cards, SIM, Biometrics, NFC and RFID

www.smartcard.co.uk

05 • SECCOS for German Market

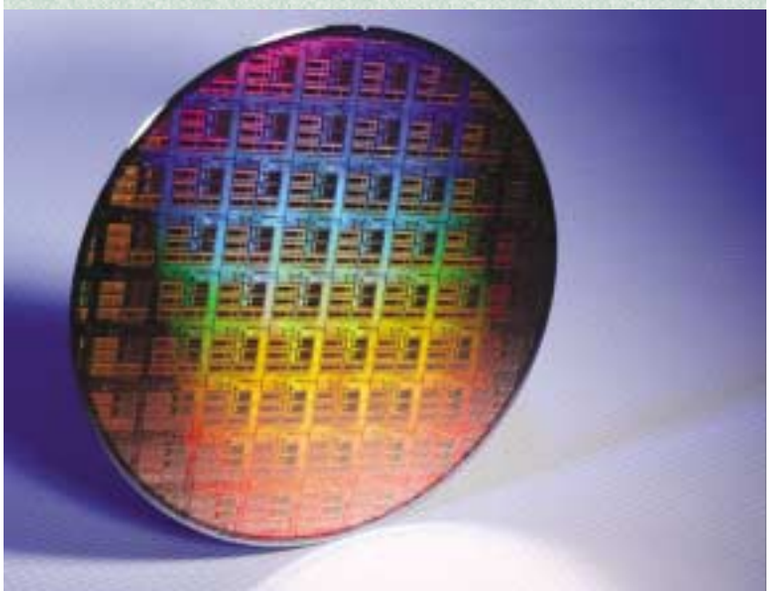
08 • GIE Certification for Gemalto

04 • Dudley Gets Smart

06 • The Brooklyn Pass for NY

This Month's Lead Story

Philips Reduce Share in Semiconductors



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 Subscriber,

We read once again of another loss of personal information this time by a police officer working for the Australian High Tech. Crime Centre (AHTCC) whilst on a trip to London in April. Apparently, according to The Australian newspaper, the officer misplaced a computer memory stick containing the personal banking details of 3500 customers. The memory stick contained information about an ongoing investigation into Russian mafia Internet fraud and their victims. Apparently it was deemed safe not to inform the bank customers whose details had been compromised as this would alert the criminals to the existence of the lost memory stick. If we know about the loss presumably so do the criminals!

I see that Paypal are going to roll out a virtual debit card to their 105 million account holders. The system is based on software from Orbiscom who are based in Dublin, Ireland. The system will generate a single use account number and a one time card verification code that is linked to the customers Paypal account. Customers will be able to use their virtual card at any e-merchant that accepts MasterCard cards.The system will first be trialed by Paypal employees and will hopefully be rolled out to customers by the end of the year. I am not surprised to see that eBay has banned Google's Check-out payment service, which was launched earlier this month, from its web-site by listing it as a prohibited payment option. Funny this was the action PayPal complained about of eBay when it was first launched.

It has been revealed in the New York Times that the US Bush administration was using emergency powers to access data on suspect wire transfers sent over the Swift network. Swift said they had responded to compulsory subpoenas and had kept Belgium's central bank and the European Central bank informed.

The Australian House of Representatives economics committee has called for the introduction of Chip & PIN to replace the current signature based cards.Looks like Australia is catching up with the rest of us.

Patsy

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**

Philips Reduce Share in Semiconductors

Royal Philips Electronics has announced the intention of the company to reduce its ownership share in its Semiconductors division in the course of the second half of 2006 to a minority stake through an initial public offering of shares (IPO) of the company and/or sale of shares to financial investors, while continuing to evaluate industry consolidation opportunities. .

In December 2005 Philips announced that its Semiconductors division would be legally separated in order to generate value to Philips' shareholders and to provide better ability to the division to achieve its business renewal objectives and become a stronger company. According to market researcher Gartner Inc., Philips Semiconductors failed to make its Top 10 list in 2005 after finishing ninth in 2004. Philips "was pushed out of the top 10 for only the fifth time in the last 25 years," said Andrew Norwood, Gartner's research vice president. Analysts valued the business at 5bn-6bn euros ($6.3bn-$7.6bn). It reported 2005 sales of 4.62bn euros, a sixth of Philips' total revenues.

In a letter e-mailed to employees Philips' President and CEO Mr. Gerard Kleisterlee, wrote: "In the course of these last few months hundreds of Philips people have been working long hours on issues relating to the disentanglement of Semiconductors, while a small top team has worked on the pursuit of the different strategic alternatives. Both projects are well on track and in the process we have been able to define more clearly the next steps we will make and the outcome that will result in, both for Philips as well as Semiconductors. This has led us to the decision to speed up the transformation of our Semiconductors division into a standalone company that is separate from Philips and will have a majority third parties ownership."

Gerard Kleisterlee

Mr. Kleisterlee further added: "The future deconsolidation of Semiconductors is a further step for Philips in moving away from a focus on high volume electronics and implementing a strategy to build a Healthcare, Lifestyle and Technology company with a strong market focus around the brand promise of Sense and Simplicity."This move away from semiconductors mirrors the strategy of Germany's Siemens, which spun off its chip business under a new name, Infineon, in 1999.

The new semiconductors company will strongly continue its business renewal strategy as well as consider additional measures to strengthen its portfolio in Mobile & Personal, Home, Automotive & Identification and Multi Market Semiconductors. Naming for the company will be announced in due course and preparations for a separate stock exchange listing have started. Philips is now seeking strategic options for its semiconductor division and there has been much speculation about which entities would make a good partner for Philips Semiconductor. Intel has been named alongside Infineon, Freescale and STMicroelectronics as potential partners. Industry observers see STMicroelectronics as Philips Semiconductors' likeliest merger partner since the Franco-Italian company shares research facilities in Crolles, France, with Philips. Frans Van Houten, Chief Executive Officer of Philips Semiconductors , however, called the Crolles partnership "a loose alliance

"We still do not know which the preferred option is. We have been discussing potential strategic partnerships over the past few months, and if the correct opportunity for this emerged, we would certainly not rule it out," said a Philips spokesman.The company has considered selling the business in its entirety but said that was "not a preferred option right now".

Preparatory to any one of those moves Philips has said it wants to create a subsidiary semiconductor company by the end of the third quarter of 2006 and that a name for the semiconductor company would be disclosed in "due course".

PHILIPS

Smart Cards

Smart Cards for Indian Sex Trade

Under a project facilitated by the Bill and Melinda Gates Foundation, about 500 sex workers in Mysore, India have been given Smart Cards, which when presented during retail transactions help them to get discounts at select shops and hotels and earn them loyalty points that can be redeemed for discounts on later purchases. The shopping basket can include provisions, food at restaurants and clothes. But the card serves another purpose. It has the medical record of the sex worker, who has to compulsorily get his or her health checked up at a clinic once every three months. The card becomes inactive if the holder fails to do this. The sex workers will be checked for sexually transmitted diseases (STD) and treatment provided if necessary.

Philips Chip for Franch e-Passport

France has selected secure contactless Smart Card chip technology from Royal Philips Electronics for integration into its new electronic passports. The e-passports were initially issued in Hauts-de-Seine, West of Paris and have now been rolled out across the country. The French government now produce 20,000 e-passports a day to meet its June 2006 deadline. The new passports have been issued to comply with US border regulations - or Visa Waiver Program (VWP) - which means that some countries' passports have to store biometric data and a digital image for visitors wishing to enjoy visa-free travel to the country.

Dudley Gets Smart

Dudley Metropolitan Borough Council, UK, has launched a new Smart Card pilot scheme to help citizens access services. The Dudley Smart Card is a 3-in-1 card which will allow individuals to borrow items from their library, log onto a PC at an adult learning centre or make online bookings at leisure centres. The pilot is currently rolling out to existing leisure centre members and to a small group of library users. They will be testing the system and reporting back before the full programme goes live in late 2006. The aim is for the Smart Card to eventually replace individual library and leisure cards, making it more convenient for local people and more cost-effective in the long term. The scheme will put Dudley Council on target to deliver a government set priority for all such data systems to be fully integrated.

Smart Cards for Oracle ID Ecosystem

Giesecke & Devrient's (G&D) multi-factor authentication services on Smart Card technology will now support Oracle Identity Management. Outfitted with a PIN and a Smart Card or token from the G&D StarSign product line, employees can present unique user credentials to Oracle Identity Management. This method (card and PIN) is called dual-factor authentication, and is far more secure than conventional user name/password systems.

Sagem Orga Doubles Production

Sagem Orga has doubled its Smart Card production in Brazil to 80 million cards a year, reported local newspaper Gazeta Mercantil. The expansion has come as a result of a 2.2 million euro investment in Brazil after Sagem took over local Smart Card firm Daruma. Daruma was a subsidiary of German card manufacturer Orga Kartensysteme, which merged with Sagem in September 2005. The merged companies now have 300 million euros in global revenues, with 30 million euros from Brazil.

Gemalto Receives GSM Certification

Gemalto has announced that its production facility in the United States is the first in the Americas to receive the prestigious Security Accreditation Scheme (SAS) certification from the GSM Association. This certification validates that Gemalto's production site and Subscriber Identity Module (SIM) card production processes meet the GSM Association's stringent standards for security and data protection. The GSM Association's SIM card Security Accreditation Scheme (SAS) is a stringent industry initiative that aims to further enhance the integrity of the SIM card. It is a voluntary certification whereby suppliers of SIM cards, like Gemalto, subject their production sites and processes to a comprehensive security audit.

TeamCard for Everton FC

Everton Football club, a UK Premiership team, has announced plans to introduce a Smart Card system at Goodison from the start of the new season. The Everton TeamCard allows supporters to simply swipe their card past a proximity reader to gain access to the stadium on a matchday. The card will provide Everton FC with information about the people coming in and the games they are attending. But the key point of the Smart Card from the perspective of supporters is the fact there will be a loyalty programme involved - providing value for season ticket holders.

SECCOS for German Market

Sagem Orga GmbH has received a landmark order for two million debit cards from Postbank. The order reaffirms the ongoing cooperation between the Smart Card expert in Paderborn and the Bonn-based bank, which is now committed to the highly secure SECCOS product from Sagem Orga. A decisive factor in awarding the contract to Sagem Orga was the recent certification of its SECCOS (Secure Chip Card Operating System) card to a CC certification level. The semiconductor and the operating system of the Smart Card have been successfully certified and thus guarantee maximum security for card-based payment transactions and in the use of add-on applications. Shipment of the ordered SECCOS Smart Cards and card bodies will begin in September 2006.

FIPS 201 Certified Tri-Interface Card

Oberthur Card Systems and HID Global have produced the first fully FIPS 201 certified card (FIPS 201 Certificate 1 and NIST FIPS 140-2 Certificate 668) with HID Prox Technology. "This specific Smart Card product will make a great addition to our TotalIDOne solution. It can be applied to a variety of identification needs such as First Responders, Transportation Workers and Registered Travellers, the Corporate Market, and with our vertical integration capabilities, we have a complete centralised ID management package, which is a critical need for many enterprises today." said Patrick W. Hearn, Director, Government and ID Markets of Oberthur Card Systems' American division.

35,000 Readers for Pension Fund

OMNIKEY is to provide the German Pension Fund (Deutsche Rentenversicherung Bund) with 35,000 Smart Card readers for their eGovernment project. The OMNIKEY CardMan 3121 Smart Card reader, in combination with the Pension Fund's employee ID card featuring digital signature function, will enable the government agency to implement efficient electronic processes utilising its new IT system.

Digital signatures will replace handwritten signatures for approximately 150,000 routine tasks a month, which will now be processed without media discontinuities and without paperwork. The Smart Card is the key to these secure and integrated electronic business processes, for instance to handle over 600,000 pension applications a year.

Smart Healthcare System for Algeria

Gemalto has announced that it has been selected by the Algerian national health insurance authority (Caisse Nationale de la Sécurité Sociale des Travailleurs Salariés, CNAS) to be its sole provider for the rollout of the first healthcare microprocessor cards in Algeria. As prime contractor, Gemalto will manage the entire project. Main roll out is to take place in 2007, including a total of 7 million Smart Cards.

New Xiring and Idealx Solution

Xiring and Idealx have pooled together their expertise to provide large corporate clients with a new Smart Card-based strong authentication solution in order to ensure a high level of security when accessing and manipulating sensitive data. With this partnership, Xiring and Idealx associate their know-how and experience in the banking, industrial and government sectors to provide a flexible, reliable secure solution.

$2 million Card Order for LaserCard

LaserCard Corporation has announced receipt of a $2 million order for a sports membership card project in the European Union. The project will be implemented by MCB Company, a long time LaserCard value added reseller based in Ljubljana, Slovenia. The card order was received from Prevent, a local Slovenian company supporting this program. Shipments are expected to begin this month and be completed in July.

£1m Contract for Ingenico in Norway

Ingenico is to introduce the security of Chip & PIN, along with the latest mobile payment solution, to post offices across Norway in deals totalling over £1 million. The new contract follows the Group's annual results, which announced a new exclusive distribution agreement with BBS and the sale of Ingenico Sweden to BBS.

As part of the new agreement Ingenico and BBS will secure economies of scale by jointly promoting and distributing products and services across the Scandinavian region. Thanks to the new partnership both organisations are now well placed to satisfy demands from retailers that operate across a number of countries.

Smart Cards For Video Lotto Market

Smart Card Marketing Systems has launched a pilot program with several of its co-branded card merchants to offer stored-value Smart Cards as a way to pay out lotto winnings in Florida, USA. The cards will be able to function like an ATM card. However, because of the company's Smart Card technology, the cards can restrict the purchase of tobacco or alcohol. Company officials say there are already more than 300 locations throughout the state that use gift cards to pay out lottery winnings.

Traveller Smart Cards for Qatar City

Mass Transit Director Anthony Tallant of the city of Mowasalat in Qatar has disclosed plans to introduce multi-purpose electronically-linked Smart Cards for travellers using the cities bus service. The new Smart Card scheme is planned for the first week of July.

Smart Cards for Israel's Transport

On Track Innovations Ltd, (OTI) has been awarded a contract for supplying Calypso compliant contactless Smart Cards for payment in public transportation in Israel. The contract was awarded by the Ministry of Transportation of the State of Israel and managed by Adalya Economic Consulting Ltd., a private economic consulting firm. Israel's Ministry of Transportation is launching a new card that allows travellers to use one card for payment on multiple public transportation operators -- buses, train and light rail.

Gemalto Receives Canadian ISO

Gemalto, has announced that it has achieved ISO/IEC 27001 certification for its advanced card personalisation center outside Toronto, Ontario, Canada. This is the first card personalisation center in Canada to receive the ISO designation.

The Brooklyn Pass for NY

Leisure Pass North America, in conjunction with Applied Card Technologies (ACT) have launched the all new "Brooklyn Pass". The increased success of the New York Pass, launched in 2003 means that Brooklyn is now able to offer visitors exclusive, discounted and priority entry to all its favourite sights through a single Smart Card.

Readers for Health Care Project

SCM Microsystems provided Smart Card readers for the European NETC@RDS project during the 2006 Football World Cup in Germany. SCM's SCR3311 Smart Card readers were used to read data from new European health cards as well as the national health cards of various countries, enabling World Cup athletes, staff and visitors from participating nations to gain rapid access to health care services while at the games. In addition to providing a common software platform to read cards from multiple European countries, the readers made it possible for national health cards, rather than cumbersome paper forms, to be used as the base for billing with insurance companies while travelling. During the 2006 World Cup, SCM's readers were implemented in about 20 hospitals near where the football matches took place.

1st Full HOPS ITSO Certification

Applied Card Technologies Ltd (ACT) have successfully been awarded the first and only Full HOPS (AMS) certificate by ITSO, as confirmed by the independent Belgium-based testing house: Integri. Mike Eastham, General Manager for ITSO said "We are pleased to award the first full HOPS (AMS) certificate to ACT. In doing so we independently verify that ACT has passed all the required tests for a Full HOPS (AMS); this is a significant milestone empowering scheme operators further and also demonstrating the continued commitment and support of ACT to ITSO". Chris Forrester, ACT ITSO Project Leader said "It has been a significant undertaking to achieve full certification for our HOPS (AMS) and we are delighted to have reached this significant milestone for our customers and our business. There can be no more ambiguity; we have passed all the tests and can now focus on progressing our ITSO product roadmap plans.'

EDS Delivers 10 Millionth Smart Card

Responding to the global security needs of the American military, EDS has announced it has delivered the 10 millionth Smart Card to the U.S. Department of Defense (DoD) under an aggressive five-year-old global security program managed by the Defense Manpower Data Center. It is the largest federal government advanced Smart Card program. EDS also announced it has been awarded a new contract by the General Services Administration to provide additional Smart Cards to DoD and has received an initial delivery order for 1.25 million cards.

New ExpressCard Reader

OMNIKEY has launched CardMan 4321 featuring the new ExpressCard interface. The ExpressCard standard enabling smaller and faster PC card solutions has already been implemented in the latest laptops in addition to or as a replacement for traditional PC Card expansion slots. The CardMan 4321 uses the USB 2.0 interface as defined by the ExpressCard standard for simple and fast integration within a mobile device. Due to its small size, it is also ideal for mass distribution by mail, bundled in an envelope or small package together with accompanying Smart Cards and/or software.

First Data Acquire GZS in Germany

First Data International has completed the acquisition of GZS Gesellschaft fur Zahlungssysteme mbH, a German processor of cashless, card-based payment transactions. The shares of GZS that were previously held by savings banks organisations, private banks and the co-operative banking sector have been fully transferred to First Data. The Federal Cartel Office approved the GZS acquisition on this condition, as First Data already owns TeleCash, a strong supplier of network solutions in Germany.

2nd Smart Parking City in the US

Truckee, California, has announced that it is integrating Parcxmart Technologies' parking and local merchant Smart Card payment system throughout its Downtown area. This means that people coming to and living in Truckee can load up to $100 onto a Parcxmart Card and use it to pay for parking on-street and in parking lots, and for retail purchases at participating local merchants. Truckee is the second city in California, following San Jose, to adopt the interoperable Parcxmart payment solution.

SCM Readers Pass e-Passport Test

SCM Microsystems, Inc has announced that its radio frequency readers were among the most successful reader entries in the June international e-Passport testing in Berlin, where electronic passport samples were tested against readers from multiple manufacturers for interoperability. SCM Microsystems' reader successfully read 89 of 90 electronic passports -- a success rate of almost 99%. The company was one of the top performers out of 47 reader vendors at the event, improving on its results at the previous interoperability test in Singapore held last November.

Among the ten most successful manufacturers of e-Passport readers at the June test were also several whose readers included SCM radio frequency technology. The interoperability test took place from May 29th to June 1st in Berlin, Germany, with more than 450 participants from 38 nations representing both industry and government. The test was organized by the German Institute for Standardization (DIN) and was held under the auspices of the European Commission.

Yorkshire Secures £4m for Smart Card

The UK Department for Transport (DfT) has responded to regional advice about the transport priorities for the Yorkshire and Humberside region. The Government has approved a grant of £4m towards the cost of the introduction of a Smart Card ticket system, but have not approved proposals to extend the existing Supertram network. The Smart Card scheme will be known as 'Yorcard' and will be given a 12-month trial on key bus routes in the city and on trains between Sheffield and Doncaster. The 12-month trial is due to commence in spring next year.

Europay, MasterCard & Visa

McDonald's Netherlands Goes EMV

VeriFone Holdings, Inc has announced that McDonald's Netherlands is upgrading its entire electronic cash register network with VeriFone's SC 5000 secure consumer-facing payment system, enabling fast PIN-based payment throughout McDonald's restaurants in Holland. VeriFone Partner CCV Holland B.V. has deployed the smart programmable devices across 100 stores, enabling faster transaction times and increased security and convenience for restaurant customers and staff. As part of the national upgrade programme, CCV Holland worked directly with MDIS, the cash register supplier, to provide complete implementation, installation and maintenance.

EMV DDA for the French Market

The French Groupement des Cartes Bancaires (GCB) is granting approval for the immediate release of Visa and MasterCard cards equipped with the EMV DDA mask developed by Sagem Orga. This approval marks the conclusion of the GCB, Visa and MasterCard certification sequence. Sagem Orga now has two DDA platforms developed and deployed in Europe and is well positioned for the challenges of the future Single European Payment Area (SEPA).

EMV Service in the Middle East

Sagem Orga continues to expand its banking business in the Middle East. After providing the first PayPass Dual Interface card on EMV basis to the region, the Smart Card company has now signed a strategic partnership with Arab Financial Service Company (AFS) in the Kingdom of Bahrain. Through its partner AFS, Sagem Orga now enables banks in the Middle East with EMV personalisation and EMV migration consulting

GIE Certification for Gemalto

Gemalto has announced that the French payment card consortium GIE Cartes Bancaires has approved its DDA (Dynamic Data Authentication) EMV card known as Multima Protect. Four major French banks have already chosen Multima Protect to migrate to DDA as required by the French central bank to adopt this standard beginning in July. Gemalto has already started deliveries of the certified Multima Protect card in volumes and several hundred thousand units will be deployed by the end of this month.

ERG Losses Software Technology

ERG has given up the fight to protect its core software, having agreed to drop its action against Octopus Cards in Hong Kong for infringement of its technology. Although investors actually boosted ERG's share price, it looks as though the deal will result in ERG having to compete against its own technology around the world. This is a major concession which means Octopus will be free to offer the clearing-house system in any fare collection contract it tenders for around the world.

Westminster Gets Parking Solutions

Thales is working with the City of Westminster to introduce the latest payment solutions for the UK parking industry - Chip and PIN payment systems for both off-street parking and on-street parking. The pilot schemes, which have gone live over the past 10 days, are the UK's first examples of certified EMV parking solutions.

As Chip and PIN transactions become the de facto choice of payment, the unattended payment sector is set to expand rapidly. The enhanced card payment services provided by Chip and PIN offers the 550,000 people who work and shop in the City of Westminster a secure and convenient way to pay for their parking.

Near Field Communication

NFC Mobile Payment Pilot

JCB together with seven players in payment systems, terminals, NFC and mobile technology, have announced the launch of a pilot project using an NFC contactless credit payment scheme to start this autumn in Amsterdam. This project is being run by a joint cooperation with JCB, CCV Holland B.V., Gemplus, KPN, Nokia, PaySquare, Philips and ViVOtech. With the contactless credit payment scheme, consumers will benefit from the convenience of using their mobile phone to make small payments in the Amsterdam area.

Selected cardmembers will be supplied with a Nokia mobile phone equipped with Philips' NFC chips, loaded with the JCB payment application. Cardmembers will be able to pay at merchants by just waving their mobile phone at the contactless payment terminal. In the first stage of the pilot, JCB will be targeting approximately 100 cardmembers located in Amsterdam and merchants in and around the city's World Trade Center.

On this scale, the pilot is primarily designed to evaluate the technological aspects and operational feasibility including customer ease-of-use. The companies involved in this project are hoping to expand both the cardmember base and merchant locations as the project evolves. This pilot will mark the very first implementation in Europe of a contactless credit payment scheme using a mobile phone with an NFC chip.

G&D and Nokia Team in NFC

Giesecke & Devrient (G&D) and Nokia have announced an agreement with intent to form a joint venture. Giesecke & Devrient will own 57% and Nokia 43% of the new company. The joint venture will provide services to the NFC ecosystem by enabling consumer applications, such as credit cards or transport tickets, to be securely and easily downloaded over-the-air to NFC enabled mobile devices.

Over-the-air management of the consumer applications is a critical part for the emerging NFC ecosystem, and the joint venture will work closely together with other stakeholders when bringing these services to the market. The joint venture is expected to commence operations in the fourth quarter 2006.

Radio Frequency Indentification

RFID Tags for World Cup Tickets

Philips have supplied RFID technology to FIFA for the 2006 World Cup. Every single World Cup ticket (3.2 million) issued for the tournament in Germany was embedded with an RFID tag to eliminate counterfeiting. Each ticket was personalised with the holders name in an effort to stop touting and prevent hooligans from getting access to World Cup matches. The tickets were checked and scanned when fans arrived at any of the 12 stadiums the World Cup matches were being played in. Other uses for this Smart Card style technology were rejected for being too complex. These included fans being able to use their tickets for contactless payments for such things as refreshments and parking.

Integrating RFID into the Enterprise

According to a new Aberdeen Group research report, 50% of enterprises report that they will have anywhere between 2 and 10 of their manufacturing sites RFID-enabled by 2008. The planned growth is forcing companies to create strategies to better integrate RFID technologies into their overall Enterprise technical infrastructure. The report finds that over half of the manufacturers surveyed have automated or will automate their RFID tagging processes in the next 24 months by integrating with manufacturing execution and material handling systems, as well as Programmable Logic Controllers (PLC). "For the first time, reliability of RFID technology trumped cost as the leading consideration in RFID technology selection," says John Fontanella, Sr. VP of Research. Key findings in the research, underwritten by BEA Systems, Odin Technologies, Reva Systems, and Xterprise, Inc., demonstrate the challenges of scaling up RFID implementations and also how companies overcome them.

RFID to Exceed $500m in South Korea

In a report to an IT forum hosted by the Ministry of Information and Communication, the Korea Association of RFID/USN said the country's RFID-related equipment and device shipments would reach $551.8 million this year, compared with $305.11 million last year and $160.97 million in 2004.The association forecast the volume to grow up to $1.26 billion by 2010. Overseas RFID shipments will grow from $34.72 million in 2005 to $55.23 million this year, according to the association.

On the Move

HEI CFO to Resign

HEI, Inc, a supplier of RFID technology, has announced that Timothy Clayton, the Chief Financial Officer (CFO), has informed the Company of his intention to resign effective June 30, 2006. Mr. Clayton is resigning to pursue other opportunities through his firm Emerging Capital, LLC. Mark Thomas will become the new CFO.

Zebra Expands Regional Office

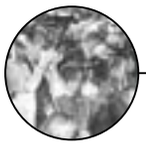
Zebra Technologies Corporation has appointed Dara McKenna as Media Supplies Specialist based in Zebra's regional head office in Dubai's Jebel Ali Freezone. This appointment is to further cement Dubai's position as the regional sales centre servicing the Middle East, Indian-Subcontinent and African Region.

Management Change at NBS

NBS Technologies Inc has reorganised its Smart Solutions Division. The division has been reorganised into four product business units focused on product and service technical excellence. The four business units are - UbiQ personalisation software in Minneapolis, Minnesota, Card Technologies embossed card equipment in Paramus, New Jersey, Javelin desktop card printers in Surrey, UK, and Cybernetix Smart Card equipment in Rousset, France. One global Sales, Marketing and Customer Service operation based in Toronto, Canada will represent these products to customers. The leaders of these business units will report directly to Kirk Hamilton, President & CEO of NBS Technologies. Simon Ormerod, Executive Vice President & General Manager of the Smart Solutions Division, is leaving NBS Technologies to pursue other interests.

New Unit President at ASSA ABLOY

Juan Carlos García has been appointed President of ASSA ABLOY Identification Technology (ITG), a manufacturer and supplier of identification and RFID products. Juan García will have worldwide responsibility for ITG, reporting directly to Joe Grillo, Executive Vice President of ASSA ABLOY and President of the Global Technologies Division.



Increasing Security and Establishing Trust at Ports

By Walter Hamilton, Vice President & General Manager - Biometric Systems, Saflink

Walter Hamilton

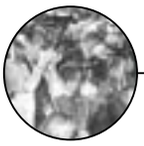
Since the terrorist attacks of 9/11, the federal government has begun implementing new security procedures at US ports. Designed to fill in security gaps and prevent acts of terrorism, these new regulations have accelerated the development of revolutionary physical access control (PAC) strategies and technology. The new approach replaces isolated physical access control systems, or systems limited to one facility, with a comprehensive and interoperable framework that can scale to support many sites. New Smart Card technology has enabled the development of a single, common credential and thus, a consistent level of trust among disparate ports. In order to maximize Smart Card investments, ports must ensure deployed card readers can support rapidly changing Smart Card requirements.

To address potential security weaknesses in US transportation modes, the Transportation Security Administration (TSA) began testing a system-wide credential for transportation workers requiring unescorted physical and/or logical access to secure areas of the US transportation system. The program and credential, known as the Transportation Workers Identification Credential (TWIC), was tested during the prototype phase at 28 sites in three geographic areas between late 2004 and June 2005. TWIC is a non-transferable smart card that contains biometric information unique to the cardholder. The TWIC card enables port facilities to verify the identity of a worker and prevent unauthorized individuals from gaining access to restricted areas. Moreover, the TWIC program requires ports and other transportation sites to standardise on a common credential and eliminate the need for port workers to carry multiple identification cards. In the eventual nationwide rollout, more than 12 million workers across all transportation modes, including seaports, ships, airports, rail, bus and pipelines will possess a TWIC card.

By definition, a credential entitles an individual to confidence, credit or authority. Historically, ports have relied on a guard simply looking at a driver's license to verify a worker's identity. In more sophisticated environments, proximity cards or badges have been used as an automated method for verifying an employee's identity and access privileges. A proximity card functions in a read-only mode, supplying a static, factory-loaded identity number. User registration requires entering the card's serial number into a PAC system's access control list, linking a particular card number to an employee and determining that employee's access rights to the facility. Proximity cards can be transferred to another employee by changing the name and access rights in the central system.

While a proximity card system is easy to manage and implement, it is a particularly weak and flawed approach to security as proximity cards can easily be lost, borrowed or stolen. More importantly, proximity cards do not require strong authentication for identity verification of the card holder. This means that anyone can pick up another employee's proximity card and use it to access secured sites and sensitive data. Many facilities issue their own proximity cards, making the card useless at other facilities because there is no "chain of trust" that can be linked back to the card issuer. If a worker needs unescorted access at another port or terminal, he or she will likely need to be issued a separate card specific to the second location, oftentimes with the same set of access rights as his or her previously issued card. This sort of redundancy wastes time and money and negatively impacts worker productivity.

System configurations for proximity card-based access control systems are straightforward; readers connect to a physical access controller that receives and processes all reader requests including the granting of access and unlocking of doors or opening of gates. In more advanced configurations, the PAC system's controller is subordinate to a security management server that also monitors alarms and video surveillance. The TWIC approach provides a way to leverage existing physical access control and security infrastructures while replacing weak proximity card-based systems with interoperable Smart Card-based credentials. Biometrically enabled Smart Cards, such as the TWIC card, can be used to irrefutably prove that the cardholder is the person to whom the card was issued.



To gain access to a secured site, a TWIC cardholder passes their biometric Smart Card near a contactless reader and touches a sensor that scans his or her fingerprint. If the submitted fingerprint matches the fingerprint data stored on the Smart Card, the worker is confirmed to be the legitimate cardholder. Next, an access request for this unique card is sent to the PAC system. The PAC system can determine if the card is still valid by checking the unique cardholder number against a list of revoked or expired credentials. Finally, the PAC system will then determine if this person has privileges to enter the facility through this particular gate or door and at this particular time and date. If each of these steps is confirmed, the door will then automatically unlock, or the gate will raise, to permit unescorted entry to the facility. While the process sounds very complex, it is actually very fast - taking less than two seconds - and it's easy for the port worker to use. By implementing a common standards-based biometrically-enabled Smart Card for all workers requiring unescorted access to sensitive transportation facilities across US transportation modes, businesses can achieve interoperability between facilities, much higher levels of security and eliminate multiple badging systems that are redundant and costly.

It may take many months for all port facility workers to be issued a TWIC card. However, many ports and terminal operators would like to take advantage of advanced Smart Card and biometric technology immediately to better secure facilities now and prepare to quickly transition to the TWIC card when it becomes available. But the data models and software may be different between the two implementations. To accommodate such a transition, ports and terminals should consider more sophisticated Smart Card/biometric readers that support a flexible data and software model. Some Smart Card readers are designed to support a single card data format and application software, and any change requires a major system overhaul. In fact, updating a reader to support new card data formats and software can be very expensive, requiring an on-site technician visit with component swap and re-attach. To further maximize port technology investments, readers should be easy to upgrade remotely using standard network communication protocols, such as TCP/IP. Such an advanced reader can even be programmed dynamically to require additional authentication factors, such as biometric plus a personal identification number (PIN) in times of elevated threat levels.

In addition to remote administration and enhanced security capabilities, physical access Smart Card/biometric readers should also be flexible enough to be used in both indoor and outdoor environments. Many entry points in port facilities are outdoors and exposed to the extremes of heat, cold, dust, moisture, salt and vibration. Due to these demanding environmental conditions at most seaports, TWIC technology providers developed a Smart Card/biometric reader that is capable of withstanding extreme weather, including dust and moisture.

In a cutting-edge deployment for the State of Florida Seaport Gate Control Project, Saflink Corporation has begun implementing a TWIC-compliant Smart Card/biometric reader to enhance physical access security at the state's 12 deepwater seaports. The initial installation included more than 1,000 fixed-mount Smart Card biometric readers at port vehicle and pedestrian entry gates and doors. To date, Saflink and technology partner, Datastrip, have deployed an additional 200 wireless readers to enable port authorities to verify a worker's identity anywhere at any time. This flexible approach allows critical facilities to respond to heightened security events more efficiently.

Advances in Smart Cards and supporting readers have made it easy for ports to increase security quickly and further refine security practices. Large-scale Smart Card implementations, such as TWIC and the Florida Seaport initiative, have proven to be a highly efficient method for quickly verifying the identity of a worker and establishing a consistent level of trust among disparate but related sites. To ensure the flexibility and cost-effectiveness of a Smart Card deployment, organisations must ensure that card readers match the flexibility of the Smart Cards themselves. Smart Card deployments with insufficiently flexible readers may require significant and costly system overhauls to accommodate future routine Smart Card upgrades.

www.saflink.com

Convergence of IT and Smart Cards will Develop the Potential of Smart Cards Market

By George C. Paul, Frost & Sullivan, Research Analyst

FROST & SULLIVAN

Smart Cards are in the middle of an expansion phase and are exhibiting double-digit growth rates. As Smart Cards grow, there is a parallel development of the applications and technologies depending on it. A major boost to this advancement is the convergence of IT and Smart Cards. Our Smart Cards Platform Market report reveals that unit shipment in this market totalled more than 940 million in 2005 and estimates to reach more than 4.6 billion in 2011. The growth of the Smart Cards platform depends on the convergence of IT and Smart Cards. The integration of Smart Cards with the IT infrastructure will become a necessity and only the most secure and interoperable platform is likely to succeed in the future.

Currently, Smart Cards are linked to a computer network only through a reader or terminal-side application that has Transmission Control Protocol/Internet Protocol (TCP/IP) support. As newer platform specifications support TCP/IP, vendors will be able to integrate Smart Cards directly into the computer network and negate the need for complex terminal-side infrastructure. The specificity of their functions often deters the uptake of Smart Cards. Overcoming technological barriers and becoming interoperable are mounting challenges for Smart Cards. Vendors have to standardise Smart Cards to make them eligible across all applications.

The platform in this market will either be flexible and open or proprietary and secure.The flexible platform will be suitable for applications such as global system for mobile communication (GSM) and transit applications, whereas the secure platform is likely to be utilised for payment and identification applications. Participants in the Smart Cards platform market are coming under increasing pressure to bring out specifications targeting particular applications with the right balance of flexibility, security and cost. Smart Card manufacturers need to scrutinise business opportunities and take into account the cost of changes in technology before entering the market. Smart Cards are likely to deliver huge value to end users and manufacturers as they converge with IT.

Events Diary

September 2006

06-08	2nd ICAO-Standard MRTD Symposium with Exhibition - *Montreal, Canada - www.icao.int/mrtd*
06-08	SmartCards Expo 2006 - *New Delhi, India - www.electronicstoday.org/smartcardsexpo.htm*
06-08	Inter Airport China 2006 - *Beijing, China - www.interairport.com*
12 - 14	Cardex & IT Security 2006 - *Moscow, Russia - www.cardexpo.ru*
13-14	Air & Port Security Expo - *Brussels, Belgium - www.aps-expo.com*
18-20	Cards and Payments Conference & Expo 2006 - *Paris, France - www.efma.com*
19-22	*World e-ID- Sophia-Antipolis, French Riviera - www.strategiestm.com*
20 - 22	e-Smart Conference 2006 - *Sophia-Antipolis, France - www.e-smart.eu/*
20-22	Smart University 2006 - *Sophia-Antipolis, France*

October 2006

03 - 06	2006 Smart Card Alliance Annual Conference - *San Diego, US - www.smartcardalliance.org*
08 - 11	ICMA Expo - *Athens, Greece - www.icma.com*
25 - 26	Linux World 2006 - *Olympia 2, London - www.linuxworldexpo.co.uk/*
09 - 12	Cards Africa 2006 - *Johannesburg (South Africa) - www.terrapinn.com/2006/cardsza*
18 - 20	Biometrics 2006 - *London, United Kingdom*

RFID: Security, Privacy, and Public Policy

By Matthew Kazmierczak & Josh James, American Electronics Association

Radio Frequency Identification (RFID) is an emerging technology that is often misunderstood. Critics often downplay the benefits of RFID while exaggerating its risks to personal privacy and security. While privacy and security concerns are understandable, they are also addressable.

In December 2005, AeA published a paper outlining the basics of RFID technology: how it worked and what benefits it offered. This current article aims to drill down a bit deeper. The technology industry is as concerned as anyone about securing the integrity of personal information. Without a secure system, RFID technology garners mistrust, and that is bad for business. RFID already meets the stringent requirements of securing personal information, and in many ways can do so much more efficiently than other technologies. Concerns vary depending on how the technology is used. RFID can be broken down into two main types of use: *1)* Supply Chain Management; and *2)* Secure ID/Smart Cards.

The specific use determines the level of security and privacy concerns. Tags used in supply chain management want to be found. To do their jobs, these tags need to convey their location and information effectively and efficiently. On the other hand, Secure IDs or Smart Cards need to hide themselves from unauthorised use. The information contained on a Smart Card is valuable and uses strong security measures to protect and restrict the release of its information. Recognising the end goal of the RFID tag helps determine the security, privacy, and policy goals associated with it.

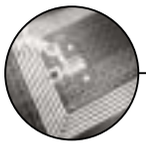
There are many different ways to address these issues, and the concerns raised in these cases are often not specific to RFID technology. Furthermore, AeA strongly believes that while technology can provide solutions for protecting privacy, bad behavior also needs to be punished, and as such we support strong criminal and civil penalties against those who seek to undermine RFID systems. Security and Privacy: Concerns about RFID technology fall into four categories: **1)** Location/Privacy with Supply Chain RFID Tags; **2)** Duplication of RFID-Enabled Secure ID/Smart Cards; **3)** Unauthorised Database Access; and **4)** Compiling/Selling of Personal Buying Habits. Before diving into the specifics of each category, let's briefly explore the security involved in a supply chain management RFID tag.

Most of these tags do not contain actual information about the product. They usually contain only a unique Electronic Product Code (EPC) identifier, which must be crossreferenced with a database to link the information. For example, a library book does not typically contain the name of the book, but contains an EPC identifier that corresponds to the library that the book came from and the Dewey Decimal Classification System code that identifies the book. The link between the RFID-enabled library book and the patron of the library is contained in a separate database.

Location/Privacy with Supply Chain RFID Tags

PERCEPTION - **A)** RFID tags will allow unauthorised people to inventory the personal property of individuals. **B)** The purchaser of an item with an RFID tag will be unaware of the technology and/or unable to remove it. Because RFID tags are tiny, broadcast information over radio waves, and often remain functional after a product is purchased, privacy advocates wrongly contend that RFID makes it easier to monitor individuals without their consent. They argue that this allows for malicious or unintended uses outside the scope of the logistics and security functions. Many critics are concerned about "skimming," - unauthorised eavesdropping of RFID tags. They claim that by using an RFID reader, someone could inventory the possessions of people as they walk down the street.

REALITY - **A)** RFID tags only send information after there is a "handshake" between tag and reader. Tags do not respond to every reader, only to those with the proper authorisation. **B)** The industry supports transparency in the use of RFID tags.



Establishments using these tags should post reasonable disclosure of this use to consumers. **C)** When feasible, the industry supports the ability of the consumer to decide whether to leave enabled or to disable an RFID tag. A consumer may want to leave the tag enabled to facilitate receiptless returns and warranties. **D)** The industry categorically supports legislation that makes skimming illegal. **E)** No case has been documented of a person's personal identifying information being stolen as a result of skimming a Secure ID or Smart Card.

Security is of the utmost concern for the industry, as it guarantees trust in the system itself. All information must be protected at all times, from the moment of collection, while being stored, and when in use. Protecting an individual's privacy involves more than simply selecting a particular technology. The entire system must be designed with privacy and security in mind. Appropriate policies and procedures that support these privacy and security requirements must be strictly implemented.

Duplication of RFID-Enabled Secure IDs/Smart Cards

PERCEPTION - Many people wrongly believe that if the RFID tag in a Secure ID or Smart Card is skimmed and the information contained on that tag is captured, someone could use the information to duplicate or clone that RFID tag.

REALITY - This would be a concern not only for consumers but also for the industry. If duplicating or cloning were a viable option, companies that have invested heavily into RFID-enabled credit cards would stand to lose a tremendous amount of money. Given current encryption technology, however, companies can make the cost of cloning prohibitively expensive. The industry supports reasonable levels of security for ensuring that cloning is not viable. The level of security should vary based on the type of information being protected. As such, RFID-enabled credit cards and identification cards have a much higher levels of security than a supply chain tag.

The best defense against cloning is that the Smart Card industry has made it not worth the trouble. While researchers at some universities have been able to clone weakly encrypted RFID tags, the ability to clone a strongly encrypted card is so difficult as to be nearly impossible. Cloning a strongly encrypted RFID-enabled Secure ID or Smart Card is significantly more difficult and costly than cloning a conventional credit card or ID. In fact, RFID constitutes a more secure technology than other systems currently available.

Unauthorised Database Access

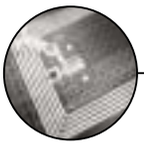
PERCEPTION - Typical RFID systems use a database to tie everything together, linking the EPC identifier with the information associated with it. Because the database tracks and stores every transaction, it holds a large amount of information. As a result, some critics wrongly argue that RFID technology increases the likelihood of a database breach.

REALITY - Privacy and security concerns exist in any database holding vital information, but these concerns are separate and apart from RFID technology. Nothing inherent in RFID technology makes a database more vulnerable.

Compiling/Selling of Personal Buying Habits

PERCEPTION - Another concern is the linking of an individual with his or her personal buying habits. As these databases can track every transaction, they allow for large compilations of data about individuals' buying habits. Linking this information with other databases or allowing it to be sold to third parties would violate a consumer's privacy.

REALITY - This concern is also not specifically related to RFID technology. Businesses can already compile information on consumer buying habits from loyalty cards or credit cards. Also the technology industry supports open disclosure of privacy policies from companies that compile this data. The policy should describe what information is collected, how it is stored, who has access to it, and how it is protected.



The Link to US Competitiveness

As the Internet went from being a fringe technology for academics to becoming the ubiquitous medium for commerce and communication, policymakers struggled with how to deal with such a revolutionary innovation. For the most part, policymakers resisted the urge to step in prematurely to regulate the Internet. This hands-off approach helped the United States build some of the largest and most innovative online companies in the world. Similarly, most of the leading manufacturers of RFID technology are US firms. And, a number of the foreign firms have production and research facilities in the United States.

All these firms have benefited from a business culture that embraces new technology and views intrusive legislation as a last resort. In 2005, the RFID market was estimated to have generated $1.7 billion in products and services. America stands at a critical juncture. The ability of the rest of the world to challenge our technological preeminence is at an unprecedented high.

To maintain our competitiveness and spur wealth and job creation in the United States, we need to promote innovation, especially in fields where US companies hold a competitive advantage, such as RFID technology. RFID helps companies improve logistics and supply chain management. This not only leads to lower prices for American consumers, it makes US companies more competitive. The United States does not compete globally on wage rates. Our advantage derives from productivity, know-how, and innovation, all of which RFID enhances.

Good Public Policy Bans Bad Behavior, Not Technology

RFID is in the nascent stages of development and will continue to face challenges. To become truly effective it must be widespread; to be widespread it must come down in cost. Such is the history of any new technology. The day when RFID is utilised to its full potential is years away. The tech industry is highly concerned with protecting privacy. Successful development of RFID in its myriad uses hinges on consumer confidence in the technology. But RFID is not the culprit. Identity theft is wrong whether accomplished by breaching a database, stealing discarded personal information from the trash, or mugging a person's wallet on the street. The technology is not to blame for the bad behavior - the criminal is. And the criminal should be punished to the full extent of the law.

In March 2005, the Federal Trade Commission (FTC) drew similar conclusions. After studying the technology and conducting a workshop with advocates on all sides of the issue, the FTC decided to allow retailers and industry to self-regulate. The FTC continues to monitor development of the technology. We believe much of the debate is being shaped by the wrong question. It is not: "Should personal information be protected from illicit use?" Of course it should.

The more useful question is: "Who is in the best position to decide the level of protection needed given the range of uses for RFID technology?"We argue that these decisions should be made by those closest to the technology; they have the most to lose if the system becomes compromised. We support working with all stakeholders on these decisions - technology experts, policymakers, and privacy advocates. We do not support legislation that imposes arbitrary technology standards or levels of protection. US State Department officials, in concert with privacy advocates, determined the level of encryption needed on passports. In the private sector, major credit card companies have worked to ensure that their cardholders' information is secure, as these companies have much to lose in reputation and revenue if something goes wrong.

RFID is not a monolithic technology. It has many uses, each requiring different levels of privacy and security protection. The chip embedded on the entry card for a nuclear facility will require a much higher level of encryption than a mass transit card. RFID chips carrying personal information require higher security than those in a supply chain. New technologies are often greeted with fear and misinformation. Fortunately, the technology tends to survive because its benefits far outweigh its costs. With barcodes, consumers came to appreciate the speedier checkout lanes and lower prices. These lower prices were most notable for food and clothing, which most directly impact lower income individuals. The same will prove true with RFID if it is not stifled in the early stages by well intentioned but shortsighted legislation.

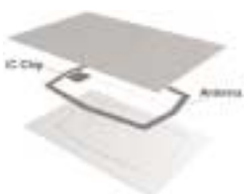
Deploying RFID for WHTI PASS Card

By Randy Vanderhoof, Executive Director, Smart Card Alliance

Randy Vanderhoof

Contactless Smart Card technology best meets the objectives set forth by the Department of Homeland Security (DHS) for high throughput and the protection of individual privacy at the nation's border crossings for its People Access Security Service (PASS) card program supporting legislation directed by the Western Hemisphere Travel Initiative (WHTI). PASS cards will be required by 2008 for all US citizens who cross the northern and southern borders of the United States without passports.

The Smart Card Alliance disagrees with the current DHS technology choice for the PASS cards. The DHS are using EPC Gen 2, a type of radio frequency identification (RFID) technology based on the Electronic Product Code Generation 2 (EPC Gen 2) specification. This technology allows cards to be read at a distance of up to 30 feet, which raises security and privacy concerns for the Alliance members as well as other organisations.



Contactless Smart Card technology is different from radio frequency identification (RFID) technology. Contactless Smart Cards are designed for secure applications such as payment and secure identification of people. They contain a small but fully functioning microcomputer that can deliver the highest levels of security, and include built-in features that protect the contactless smart chip from a wide variety of attacks.

In contrast, RFID technology is used in applications such as identifying animals, tracking goods through the supply chain, tracking assets such as gas bottles and beer kegs, and controlling access into buildings. RFID tags include a chip that typically stores only a static number (an ID) and an antenna that enables the chip to transmit the stored number to a reader. There is little to no security on the RFID tag or during communication with the reader.

RFID chips are not designed for human identity applications, but are optimised for supply chain and other applications that need low-cost, electronic identifiers that serve as a replacement for barcodes. In contrast, contactless Smart Card technology is widely used in secure identification cards and travel documents, supporting the level of security functionality required for protecting individual privacy. There are many advantages to using contactless Smart Card technology for the WHTI PASS card program, including the ability to support electronic verification of authenticity to prevent counterfeiting and to use secure, encrypted communications to thwart eavesdropping and replay attacks, and ensure privacy protection for cardholders. A WHTI PASS card based on contactless smart chip technology can also leverage the infrastructure that is being put in place by DHS and the Department of State to support the new ePassport. Using the same secure contactless technology for the PASS card and ePassport could potentially decrease the implementation time and lower the cost of the program.

The Alliance strongly recommends a technology trial to evaluate the performance of ISO/IEC 14443-based contactless technology -- the same technology used in the new ePassport -- versus the EPC Gen 2 RFID technology being considered by DHS, before the final implementation decision for the WHTI PASS card program. In our ongoing efforts to educate the industry about the differences between secure smart chip technology and RFID, as well as other technologies like barcode, optical stripe and magnetic stripe we have produced a white paper entitled "Western Hemisphere Travel Initiative PASS Card: Recommendations for Using Secure Contactless Technology vs. RFID".

www.smartcardalliance.org

Why ePassports Need to be Multi-Application Ready…

STEPNEXUS MULTOS

By Tim France-Massey, VP Smart Card Marketing & Business Development, StepNexus

Tim France-Massey

The Migration to ePassports: If you've already received a new "biometric" or "e-Passport", then you're still one of the lucky few. But over the next 2 years, citizens in over 40 states around the world will also begin to receive passports containing contactless smart card chips that electronically store and transmit their passport details, a facial image and an optional additional biometric of fingerprint or iris, as defined by the International Civil Aviation Organisation (ICAO).

Apart from making it easier to detect forged travel documents, one of the primary benefits of the ePassport is that it will enable automated passenger clearance at border control points. By presenting the travel document to an automated reader device, the passenger's passport information and biometric can be read from the contactless chip. Then when the passenger has their facial, fingerprint or iris image captured in the reading system, the stored biometric image can be compared to the one presented, and if there is a successful match, the traveller can pass through immigration, without needing to interact with an immigration officer. This whole process takes just a few seconds, and in the countries where automated passenger clearance with biometrics has already been implemented, such as the Hong Kong Special Administrative Region of China, it has vastly reduced queues at immigration control points.

What does the ePassport Chip Do? The chip in the ePassport is supposed to perform 4 key functions: *(i)* Securely store the biometric data - mandatory facial image, and optional fingerprint or iris image; *(ii)* Securely store the holder's passport data or "Logical Data Structure (LDS)"; *(iii)* Transmit the data over distances of a few centimetres to a contactless reader based on ISO 14443 proximity standards, whilst encrypting the data according to Basic or Enhanced Access Control requirements to prevent skimming or eavesdropping.; *(iv)* Enable verification of authenticity and integrity of ePassport data (LDS and biometric images). This is achieved by the establishment of an ICAO managed Public key Infrastructure (PKI). Each issuing government will generate its own public / private key pair, and use their private key to digitally sign the data that is stored in the ePassports it issues. The ePassport data will also be appended with a signed Hash of the data. ePassport readers will be able to access the public key of each issuing government by accessing the ICAO public key directory, and use that key to verify that the data is genuine and has not been tampered with.

Single Application or Multi-Application? The above 4 functions can be achieved by developing a single integrated piece of software running inside a contactless micro-processor chip. So in theory, a "single-application" or "fixed function" contactless chip supporting the ICAO specification will do. But what happens when the issuing government wants to update the ePassport in the field to support a new version of the ICAO standard - perhaps requiring new functionality in the ICAO application? Or what if a new standard for eVisas is released, whereby the passport issuing government may permit a Visa issuing country to download an eVisa into its citizens' ePassports?

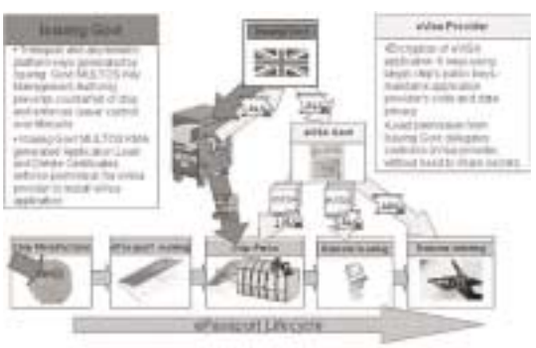
The one thing that is for certain with new technologies, is that things change. So if the ePassport is to remain valid, trusted and functional for the full 10 years of its life, then it should be flexible enough to handle these changes, whilst being secure enough to ensure that only the issuing government can permit changes to the ePassport's functionality. In order to achieve the levels of speed and performance necessary, the ICAO application software running on the contactless chip is often developed in so called "native" code - i.e. low level assembly code that is targeted at a specific hardware device and fixed in its Read Only Memory - analogous to the embedded software that drives handheld or custom built devices. These "native" or "single-application" chips are being issued by most countries that are implementing ePassports, but they have no capacity to allow changes to the functionality of the chip to be made after it has been issued, or for new applications such as eVisas to be supplied by third party governments.

Is there a flexible alternative to native OS ICAO chips? The answer is of course yes - and it is called "MULTOS". MULTOS is an open standard specification for multi-application smart chips that can be implemented on any contact or contactless silicon chip. MULTOS is already used as a flexible open standard platform on over 50 million Smart Cards in the payment and national identity card sectors, is available on 4 different contactless silicon chip families (Infineon, Renesas, Samsung and Philips), and is now also being used as a platform for ePassports.

MULTOS defines an API that allows Smart Card application programmers to develop their own applications such as ICAO, Match on chip biometrics, Payment, Digital signature, eVisa etc, in C, Java or Assembler, and compile them to run on any MULTOS chip. Despite the fact that the application code is "interpreted" by the MULTOS virtual machine, the efficiency and simplicity of MULTOS means that at the recent ICAO interoperability tests in Berlin at the start of June, an ICAO application developed to run on a MULTOS chip can execute at least as fast, and in some cases faster than many native OS ePassport chips.

Maintaining a "Secure Trusted Environment" inside the ePassport Finally, ePassport's using MULTOS chips enable the issuing Government to permit third party application providers to supply additional functions to the ePassport - such as an eVisa application supplied by another Government, or an electronic Boarding pass application from an airline - WITHOUT compromising the security of the Issuing Government's ePassport application. This is achieved thanks to the ON-CHIP firewalls between applications that are enforced by the MULTOS operating system, and by the MULTOS mechanism for "Secure Trusted Environment Provisioning" (or "STEP" for short). "STEP", as described in the diagram below, essentially enables the issuing Government to maintain complete control over the issuance of ePassport chips, and over the software that can be installed into them.

At the centre of "STEP" is a so called "StepNexus Server" (also known as a "MULTOS Key Management Authority"), that generates chip specific transport keys, asymmetric key pairs, and application load and delete permission certificates. The transport keys lock the MULTOS chips until the chip is "enabled" with encrypted data containing chip configuration parameters, and a public / private key pair used to encrypt and decrypt new applications. The permission certificates ensure that only applications that are "approved" by the ePassport issuer can be installed.



Users of MULTOS for ePassport and National ID - More and more governments around the world are coming to recognise the advantages of security and flexibility that MULTOS and the "STEP" scheme provides for ePassport and National ID card issuance. *1)* The most advanced deployment of smart card technology in the world - as voted by Card Technology, an independent industry publication - is in Hong Kong, where the Immigration Department of Hong Kong Special Administrative Region has deployed a single identity document infrastructure for managing the issuance and usage of 7 million Smart Identity Cards supporting biometrics and Digital certificates since August 2003, and 4 million ePassports starting from the end of this year. Although the Hong Kong ePassport will be issued as a single application chip, by using MULTOS, the Hong Kong Government has complete control over the lifecycle of the chip, has the flexibility to update the chip with new versions of software or new applications in the field, and has the ability to multi-source the silicon that is used inside the ePassport. ANY passport manufacturer can source the contactless MULTOS chip inlays, so every Government can continue to buy from its existing passport manufacturer. *2)* The largest national ID project in the Middle East - the Saudi National ID project - is also deploying MULTOS to its citizens. Following a successful pilot, a combined National Identity, Healthcare, Driving License card will be issued to all 17 million residents from later this year. *3)* The second largest military force in NATO - the Turkish Armed Forces - is issuing MULTOS Smart Cards containing biometrics, healthcare, physical and logical access control to all 2.2m servicemen and family members since Dec 2005.

HSPD-12 - The US Smart Card Initiative

By Jason Smith, Staff Reporter, Smart Card News Limited

Jason Smith

As the business world struggles with data-security lapses and intrusions, US federal agencies are preparing for strict new standards to protect their facilities and information systems. On August 27, 2004 the US government took an important step toward standardising the form and level of security by which employees and contractors are identified for access to federal facilities and information systems. According to the Homeland Security Presidential Directive (HSPD) 12 US federal government agencies must begin issuing secure and reliable forms of Personal Identity Verification (PIV) to its 1.8 million employees and contractors by the governments October 27, 2006 deadline that has been set.

Smart Cards will be used as the vehicle that carries the physical and digital components that form the user's PIV credentials laid out in HSPD-12. The Smart Cards will use two-finger biometric and digital certificate technology. The digital components stored on the card will support a variety of electronic authentication mechanisms and are composed of a series of cryptographic and non-cryptographic elements. Each card will also contain a user's identification credentials as well a PKI digital certificate for authentication.

The primary goals of HSPD-12 are clearly defined by US President George Bush in regards to this new Policy for a Common Identification Standard for Federal Employees and Contractors. He stated "It is the policy of the United States to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees)."

He then went on to say "Secure and reliable forms of identification for purposes of this directive means identification that (a) is issued based on sound criteria for verifying an individual employee's identity; (b) is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; (c) can be rapidly authenticated electronically; and (d) is issued only by providers whose reliability has been established by an official accreditation process.

The National Institute of Standards and Technology (NIST) has responded to HSPD 12's mandate for the Secretary of Commerce to officially promulgate a Federal standard to meet the goals of the Presidential Directive by issuing the Federal Information Processing Standard (FIPS) 201 on February 25th, 2005. This new standard specifies the architecture and technical requirements for a common identification standard for Federal employees and contractors. The overall goal reflects that of HSPD 12 and seeks to achieve appropriate security assurance for multiple applications by efficiently verifying the claimed identity of individuals asking for physical access to Federally controlled government facilities and electronic access to government information systems.

The standard is composed of two major sections outlining the details of the proposed PIV system. The first, PIV-I, focuses on the minimum requirements to meet the control and security objectives of HSPD 12, including personal identity proofing, registration and issuance. PIV-II delivers the detailed technical specifications aimed at achieving interoperability between the PIV systems of all Federal departments and agencies. FIPS 201 is the standard which specifies that Smart Cards should contain a photograph, cryptographic keys, and biometric data so that a cardholder's identity can be verified either by security personnel or an automated card reader. According to the recent Federal Market Study on HSPD-12 Readiness, proper steps to prepare for this initiative have not yet been taken by the majority of the Federal agencies affected by this mandate. The Federal IT community believes that current identity management and access control processes are not adequate in their current form, and place a high priority on HSPD-12 goals and objectives.

However, despite the Federal IT community buying in on these priorities and contending with a looming compliance-related deadline, HSPD-12 awareness levels are low. While HSPD-12 represents an opportunity for progress, only 22% of survey respondents believe their agency will meet the initial October 27 deadline and just 16% report their agency has a plan in place to meet the requirements. 50% of Federal IT professionals report that they have not heard of HSPD-12 and of that 50%, 58% cannot state the objectives of the first level of compliance.

An independent survey by INPUT, which was released in June 2006 at the HSPD-12 and Identity and Access Management Symposium also found that nearly half of federal IT security executives do not have an integrated plan to help their agency meet the Office of Management and Budget (OMB) imposed October 27, 2006 deadline for compliance with HSPD-12. "There appears to be considerable confusion in the industry as 46% of survey respondents do not feel that OMB is providing enough clarity for HSPD-12 compliance," said Bruce Brody, vice president, information security at INPUT. "Federal IT security executives cite a noticeable lack of guidance as to how to actually define success with the compliance efforts and how funding and budgetary issues would be addressed. There is even more grey area with regards to the deadline itself since 37% of respondents either do not believe or are unsure that OMB will hold fast to the HSPD-12 compliance deadline."

When asked if their organisation had implemented an Identity and Access Management (IAM) solution, 56% of respondents reported having not implemented one or just being in the initial stages of implementation. Of those organisations that have implemented IAM, most are leveraging either Smart Cards or ID badges as the primary means to authenticate users. 56% of respondents indicated that they had seven or more Physical Access Control (PAC) systems and 58% indicated that there had been no decision made on whether or not to standardise these systems.

Because HSPD-12 involves utilising a single Smart Card for authentication and authorisation of both physical and logical access, PAC systems must be integrated into a single identity and access solution. The research indicates that the vast majority of agencies are not in a position to be compliant by the October 2006 deadline because of the proliferation of PAC systems and their lack of progress on deciding to standardise on a system. While these findings may be a cause for concern, the survey showed that 74% of respondents indicated that they have established an HSPD-12 task force, suggesting that agencies have realised the impact and complexity that HSPD-12 will have on their security infrastructures. Christopher Michael, federal technology strategist at CA, the IT management software vendor who commissioned and released the INPUT survey comments, "Agencies are clearly struggling with HSPD-12 compliance. This compliance deadline, however, does present an opportunity for agencies to address their larger identity management issues and thereby improve the speed and efficiency with which they manage their growing user base and their access to an increasingly complex portfolio of IT services."

We can clearly see from these findings that a majority of US Federal agencies have not identified a path toward achieving HSPD-12 compliance, and realised improving access control and identity management. In order to better facilitate this initiative, the Office of Management and Budget will need to work more closely with agencies and the vendor community to increase awareness, establish plans, resolve technical issues, and address budget/resource challenges. "Compliance with the directive will be a significant test as to how well Smart Card systems scale, and the measure of its success will be important to both the public sector and the business world," says Bob Wilberger, senior executive for Northrop Grumman and a board member of the Smart Card Alliance.

Also just by using a standardised Smart Card will not eliminate security challenges altogether. The weakest link in the Smart Card security chain for the US may very well be in issuing them. Birth certificates, driver's licenses, and other key documents used to verify a person's identity differ from state to state, and that lack of consistency creates opportunities for tampering. As the deadline rapidly approach's to issue the interoperable Smart Cards under HSPD-12, and with the Office of Management and Budget Administrator saying there is no option but to comply by this date, it will be interesting to see what happens if the US federal agencies that are still unprepared miss it.