





**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 Townsend

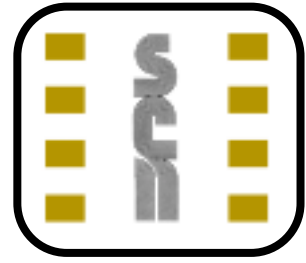
**This Issues Guest Contributors**

Martin Allen  
Cath Rawcliffe  
Dr David Everett  
Dr Peter Harrop  
Smart Card Alliance  
Jason Smith

**Printed by**

Hastings Printing Company  
Limited

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,

I have often wondered what savvy I am expected to display when dealing with point of sale terminals and web sites on the internet. Can I reasonably be expected to know whether the tamper resistance of a terminal has been broken and that it is now collecting fraudulent transactions? On the internet it just seems worse, you know that it is vulnerable to the trickery of the wily hacker but you really don't know if today is your lucky day. There is the old story of the man standing in a cardboard box in a shopping precinct pretending to be an ATM and asking for people's pin numbers, many of which were happily provided. But on the internet its really not that obvious. Privacy keeps raising its head and David Everett in this months letter has a go at some of the issues. He claims that privacy is an illusion in today's electronic world and that electronic tags, ePassports and eID cards just make it worse. So the question for me is do I care? The airports in the UK this month have been at best in a mess after the heightened security alerts but what was interesting is the reaction of the passengers who were quite unanimous in their reaction, 'if it gives me better security then I will put up with the inconvenience". Privacy is probably the same, I would trade some of my privacy for improved security. Then on another day we need to look at whether an electronic identity card gives me that trade off.

I see Nationwide are taking the moral ground on ATM charges to withdraw your own funds and teaming with BT to add free ATM's to phone kiosks particularly in those area's of deprecation and in rural communities. As the requirement is for more secure, tamper resistant terminals who, I wonder is going to pick up the bill for this?

Sophos, a UK software consulting house has raised concerns over PayPal and eBay customers being the top target for phishers because they are so popular around the world. Bank customers also suffer but they don't have the same global reach as PayPal and eBay according to Graham Cluley, senior technology consultant at Sophos. In November last year a UK criminal David Levi, 29, was able to steal nearly 200,000 pounds from eBay customers by tricking them to give away their passwords and account details. If I was criminally inclined and had the knowledge this is the area I would concentrate on, after I had set up a few false identities for myself.

Patsy

**Please Note**

From time to time, Smart Card News may include industry forecast and forward looking statements made by the companies concerned. Readers should be advised that Smart Card News Ltd cannot be held responsible 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.

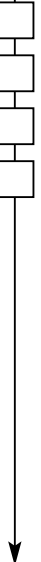
**Don't Forget!**

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](http://www.smartcardgroup.com)

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



# Gemalto Receives Order for US E-Passport



## ePassport

### WHAT HAPPENS AT PASSPORT CONTROL

1 The officer swipes the data page through a special reader to read the two lines of printed characters on the bottom of the data page. This provides a key that's unique to the passport and lets the process proceed.



2 The officer holds your open passport over another reader, then checks his view of you, with the photo in your passport, and all the data from your passport (including your photo) on the monitor.



The data on the monitor also verifies that your passport was issued by a legitimate authority, and that it has not been altered.

### DETAILS, DETAILS

3 A chip is embedded into the back cover. It contains data that cannot be read without the security key as shown in step one above.



4 When the passport is held over the reader (no contact is necessary), a radio field from the reader wakes up the chip, and the encrypted data is transferred to the reader, allowing the officer to conduct his visual check.



### PRIVACY PROTECTION

5 A thin radio shield can be sandwiched between the front cover and the first page. Whenever the passport is closed—for instance, in your pocket or briefcase—the digital information in the chip cannot be read. The shield will not set off airport metal detectors.



Source: Gemalto

The United States of America Government Printing Office (GPO) has placed its first order with Gemalto, following the company's electronic passport technology qualification completion. The GPO and US Department of State evaluated the Gemalto solution at their testing facilities and confirmed it fully satisfies the agency's requirements for privacy protection, security, durability, manufacturing yield, transaction speed and communications performance. The GPO, on behalf of the US Department of State, plans to incorporate the electronic capability in all new passports to be issued in 2007. The United States produced over ten million passports in 2005.

"This award comes at the end of Gemalto's successful completion of an extensive qualification process," commented Ernie Berger, president of Gemalto North America. "Winning this contract gives us enormous satisfaction and we look forward to delivering the first electronic passports to US citizens, as we fully support the GPO in this essential global security initiative. These new passports will greatly enhance the travel experience for US citizens by providing effective, efficient and rapid passage through border control points with an additional element of security."

The Gemalto electronic passport (e-passport) technology includes the company's highly secure operating system software running in a large capacity contactless micro-processor chip. The chip is embedded in a module that is highly resistant to damage and then is integrated into the passport booklet cover. The Gemalto e-passport solution has been designed to provide superior durability and performance over the passport's expected 10-year life span. Gemalto's e-passport references include the Czech Republic, Denmark, France, Norway, Portugal, Russia, Singapore, Slovenia and Sweden.

**Background information:** To better protect travellers, streamline immigration processes and improve the security of the passport booklet, the US Department of State and the GPO, which assembles all US passports, is issuing an electronic passport booklet in accordance with the standards developed by the International Civil Aviation Organization (ICAO), an agency of the United Nations. Last year, ICAO adopted the chip technology used in contactless smart cards as the standard for electronic passports in order to add a facial biometric and other security features to passport books. The computer chip in the passport will contain all the information that is now printed on the document's data page including a digitized photograph of the passport owner. The text data and the photograph can be read with a contactless reader at a border entry point and the electronically provided data can be compared to the information printed in the passport at issuance.

Not to be confused with RFID, secure personal identification devices using contactless smart card technology have built-in and active security and encryption capabilities to protect information access and communications. More than 30 nations worldwide have already pledged to adopt passport technology that conforms to an international standard for electronic identification data.



## Smart Cards

### **\$4.7b on e-Security**

The Middle East last year spent \$4.718 billion on e-security services, a 15.6% rate of increase placing it as the second largest spending region in the world. This is according to a report published by International Data Corporation (IDC), that expects this figure to reach \$5.620 billion this year and \$9.338 billion by 2009, with a compound annual growth rate (CAGR) of 18.6%. The report showed that the Americas region tops the list with \$8.065 billion reported in 2005 and 19.6% CAGR until year 2009.

### **OTI Selected for Polish e-Passport**

ASEC S.A., a wholly-owned subsidiary of On Track Innovations Ltd, (OTI) has announced that PWPW S.A. (Polish Public Printing Works) of Poland has placed its first order for electronic passport inlays for Polish citizens. Under the contract, ASEC S.A. will supply contactless inlays that will be adhered to the passport cover. Currently there are about 1.5 million passports issued in Poland annually and the government intends to roll out the first electronic passports starting this quarter. The first commercial order will be supplied this year.

### **3M to Buy British Passports Maker**

3M Co has acquired Security Printing and Systems Ltd., a British maker of passports and secure cards, from the German holding company authentos GmbH. Terms of the deal were not disclosed. Security Printing and Systems provides passports for the British government and is working with the Identity and Passport Service to shift from digital passports to biometric ones. The deal is expected to close by the end of the month.

### **Smart Cards for the Poor**

The government of Trinidad & Tobago is set to distribute around 20,000 Smart Cards to those citizens who are deemed as living below the poverty line to help them buy essential items. The value stored on the Smart Cards will be based on the size of the persons family. However there are growing concerns that these cards will be used to buy alcohol and cigarettes so to remedy this a Memorandum of Agreement has been drawn up between the government and shop owners to prevent this occurring.

### **Philips Sells Semiconductors Business**

Royal Philips Electronics has signed an agreement with Kohlberg Kravis Roberts & Co. (KKR), Silver Lake Partners and AlpInvest Partners NV, for this consortium to acquire an 80.1% stake in Philips' Semiconductors business, with Philips retaining a 19.9% stake in this business. The transaction will put the enterprise value for Philips' Semiconductors business at approximately 8.3 billion euros - consisting of 3.4 billion euros purchasing price, 4.0 billion euros for debt and other liabilities, and 0.9 billion euros for Philips' remaining stake.

Philips estimates it will receive cash proceeds after tax and transaction related costs of approximately 6.4 billion euros. The transaction is expected to close in the fourth quarter of 2006, subject to closing conditions, including governmental and regulatory approvals.

### **\$1.5m European e-Passport Pilot**

SuperCom, Ltd, a provider of Smart Card and electronic identification solutions, has announced that it has signed a \$1.5 million agreement, with a European country, to supply its Magna end-to-end solution for the production, management and personalisation of biometric passports. The 16-month pilot program will produce a personalised passport that includes personal details, photo identification, digital signature and biometric data. The electronic passport will be compliant with European and International Civil Aviation Authority (ICAO) standards.

In addition, the passport will contain advanced security features including a high capacity contactless crypto processor chip with operating system for the secure storing of biometric data of the holder. In April this year, SuperCom was awarded a similar contract for the implementation of a biometric passport issuing and control system for a European country.

### **Smart Passports Tested in Hong Kong**

Asia-Pacific immigration officials have recently visited Hong Kong to test smart passport technology that the US government wants other countries to adopt. Hawaii tourism executives believe the growth of international visitor traffic in Hawaii has been impeded by bureaucratic obstacles to US travel in the wake of Sept. 11. Adoption of smart passports may help. The Asia-Pacific Economic Cooperation association organised a three-day "capacity-building exercise" in Hong Kong.





## Oberthur Acquires SetCard

Oberthur Card Systems has acquired SetCard, a Spanish company in the business of health care card personalisation. Thanks to this new step forward, Oberthur will be able to provide personalised Smart Cards to 12 provinces representing 40% of the Spanish population.

## MasterCard PayPass for Europe

MasterCard Worldwide has launched the first European MasterCard PayPass credit programme, in partnership with Garanti Bank in Turkey. Garanti bank will reissue 25,000 "Tap & Go" cards, which use MasterCard PayPass technology, to its Bonus cardholders. Starbucks, Burger King and Cinebonus, Turkey's largest cinema chain, have already signed up to accept MasterCard PayPass in Turkey. By using MasterCard PayPass, Turkish consumers can simply tap their new Garanti Bank MasterCard card on the PayPass reader at participating merchants and they are on their way.

## Smart Card Pilot for NY Subway

MasterCard Worldwide, the Metropolitan Transportation Authority, MTA New York City Transit, Citi Cards and Citibank have announced the beginning of a six-month contactless payment trial in select New York City subway stations with pre-selected Citi credit card and Citibank customers. The goal of the NYC Subway Trial is to evaluate the benefits of contactless payment technology in the busy NYC subway environment. The trial will take place at select Lexington Avenue Line 4, 5, 6 stations, between the 138th Street stations in the Bronx, two stations in Queens, and Borough Hall Station in Brooklyn.

## Beijing Goes Contactless

Thales has been chosen to undertake a radical refurbishment of the Beijing metro ticketing system based on the installation of a contactless ticketing solution. Capitalising on its systems integration expertise, Thales teamed up with local Chinese company Beikong and LG to win the contract from Beijing Mass Transit Railway Operation Corporation Ltd., for the supply of a new ticketing system for the network's three oldest lines. Ultimately, all of the Chinese capital's metro lines will be modernised. The integrated contactless ticketing system for lines 1, 2 and 8 ('Batong' line) comprises entry and exit ticket validation terminals on each line

## Security Upgrade for US Airport

Honeywell has announced that the Minneapolis-St. Paul Int'l Airport will upgrade its security system with Honeywell's Pro-Watch security management software platform, addressing new federal security guidelines and streamlining security management. The upgrade will include installation of head-end, intelligent controllers and a DESFire contactless Smart Card identification badge system for 17,000 badge holders. The card system is engineered to encode biometric information, such as fingerprints and hand geometry data, complying with rigorous federal standards.

## Additional ID Systems for Spain

The Mühlbauer Technology Group has been awarded another contract for delivering decentralised desktop personalisation solutions for the ID card project in Spain. As one of the strategic partners of the Indra system integrator, Mühlbauer supports the Spanish Ministry of the Interior in establishing the infrastructure for the first decentralised ID card project in the world. Mühlbauer's CLP54 system solution makes it possible for public authorities to electronically and optically personalise ID cards on site and to deliver them to the citizen. The Spanish public no longer needs to deal with long waiting times from the application to the reception of an ID card

## Japan Post Eye Up Smart Cards

Japan Post is talking with East Japan Railway Co. about a plan to issue a cash card with the electronic money and prepaid train ticket functions of JR East's Suica Smart Card. Japan Post, which operates the Yucho savings service, and the major railroad are considering launching the new card as early as next spring. By joining with JR East, Japan Post intends to make its Yucho service more attractive in the lead-up to the October 2007 start of its 10-year privatisation process. As the first step of the process, Japan Post will be split into four firms, including one for the Yucho service.

JR East is aiming to fortify its Suica-based electronic money business through the tieup, the sources said. The Suica card can now be used as electronic money at about 6,700 outlets in Japan, including station kiosks. Japan Post, meanwhile, will cautiously consider whether to allow holders of the Yucho-Suica card to charge their cards from their Yucho savings accounts using automated teller machines installed at post offices.





There are concerns mainly among regional banks that the envisaged tieup could lead the government-affiliated postal service firm into pressuring private-sector businesses. Among private-sector financial institutions, Mizuho Bank, the retail banking unit of Mizuho Financial Group Inc., launched a cash card with the Suica functions in March.

## NFC Forum Targets Wireless NFC

The NFC Forum has published its first four specifications. NFC operates in the 13.56 MHz frequency range, over a typical distance of a few centimeters. The underlying layers of NFC technology are ISO, ECMA, and ETSI standards. The new specifications make it possible for any manufacturer to create NFC-Forum-compliant devices that will be interoperable with other manufacturers' devices and compatible with the NFC-Forum-compliant offerings of service providers, ensuring successful communication between devices and tags.

The four specifications are: 1) NFC Data Exchange Format (NDEF) Technical Specification (specifies a common data format for NFC Forum-compliant devices and NFC Forum-compliant tags); 2) NFC Record Type Definition (RTD) Technical Specification (specifies standard record types used in messages between two NFC Forum-compliant devices or between NFC Forum-compliant devices and tags); 3) NFC Text RTD Technical Specification (for records containing plain text that can be read by NFC-enabled devices); 4) NFC URI RTD Technical Specification (for elements that refer to an Internet resource that can be read by NFC-enabled devices)

Europay, MasterCard & Visa

## VeriFone Buys Trintech Business

VeriFone Holdings, Inc. has agreed to acquire the payment systems business of Trintech Group PLC in an all-cash transaction. Trintech is divesting its payment systems business to concentrate on its transaction reconciliation software products and services, which allow customers to optimize enterprise funds management performance, including transaction verification, account reconciliation, process management and compliance. Under the terms of the Agreement, VeriFone will pay Trintech \$12.1 million cash for all of the outstanding shares of a newly-formed subsidiary which, prior to closing, will hold substantially all of the assets and liabilities of the payment systems business of Trintech.

## EMV Migration for Oman Arab Bank

AFS has announced an agreement with Oman Arab Bank in Oman. Under the agreement, AFS will provide Oman Arab Bank with EMV migration services which will ultimately enable the swift migration of its existing card portfolio as well as the issuance of EMV compliant credit cards for its customers. AFS will provide Oman Arab Bank with technical support as well as consulting services and will implement a series of chip migration services, which includes technical and business acceptance testing.

## NAB Rolls Out Chip Technology

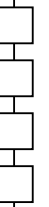
The National Australia Bank (NAB) has announced the successful completion of Australasia's first end-to-end chip card transaction pilot, paving the way for enhanced levels of electronic payment security. The EMV protocol sets the technological standards for the processing of the more secure chip card electronic payments.

NAB General Manager Acquiring, Peter Roeleven said: "We are the first acquirer in this market to be fully certified to process EMV chip card transactions. "We have completed a successful customer pilot, and we will begin processing up to 20,000 chip card transactions on a daily basis.

## FinecoBank Rolls Out EMV Cards

Giesecke & Devrient (G&D) recently began delivering EMV cards to Fineco, Italy's biggest online bank, following a successful pilot phase. Over the next several months, Fineco's 300,000 credit card and debit card customers will see their magnetic stripe cards gradually phased out in favour of secure EMV technology. The Smart Cards run on G&D's secure card operating system, Star DC I.

In the project, G&D will be providing the full range of services, from initialisation, card design and production right up to personalisation and fulfillment. For its EMV cards, Fineco decided to use Star DC I, G&D's secure EMV solution for issuing banks in Italy. It meets all the requirements put down by ABI (Italian Banking Association) in its EMV specification for debit and credit Smart Cards in Italy. Being an online bank, Fineco felt it essential to offer its customers innovative, high-quality card products. This includes transparent cards, which will be sourced from G&D.





## Account Wins £1.2m EMV Contract

The Saudi Arabian Monetary Agency (SAMA) has awarded Account a contract worth £1.2 million for the provision of a Programme Management Office responsible for the design and management of the Kingdom's deployment of chip cards, using the international EMV standard. Account, which has extensive experience within the financial sector, will work in partnership with Saudi Business Machines (SBM), the general marketing and services representative for IBM World Trade Corporation in the Kingdom of Saudi Arabia, to deliver the 18 month programme.

## DBS to Use VeriFone's EMV Solution

VeriFone Holdings, Inc has announced that DBS Bank (Hong Kong) has chosen and has begun implementing the VeriFone Vx 510 payment solution for the enhanced ComPass Visa card, a co-branded credit card jointly offered with Hutchison Whampoa Ltd. The ComPass Visa card program, which celebrated its 10th anniversary last year, engaged VeriFone to enhance its acceptance infrastructure to provide EMV and multi-application features. The new ComPass Smart Card, launched last month, carries an embedded microchip to stop counterfeit fraud, thus offering cardholders greater security than conventional magnetic stripe cards.

It also offers a powerful loyalty program that rewards cardholders based on their buying preferences. The system allows merchants to customise marketing initiatives to target cardholders. Five thousand VeriFone Vx 510 payment systems will be deployed across the Hong Kong SAR, including in mega-retail chains such as Park N Shop. This is part of DBS Bank (Hong Kong)'s phased program to upgrade ComPass Visa cards - believed to be the largest EMV Smart Card transformation exercise in Hong Kong.

## Rahaxi Market Terminals in Finland

FreeStar Technology Corp has announced that its Finnish-based, wholly owned subsidiary, Rahaxi Processing Oy, has received the Finnish EMV certification required to sell Hypercom's Optimum T2100 card payment terminal in Finland, and is commencing product sales immediately. Rahaxi Processing will be the first distributor of the T2100 in Finland, giving local merchants access to a high-speed terminal capable of supporting traditional magnetic stripe cards, more secure chip and PIN transactions, and value-added applications such as gift and loyalty cards in the same device

## Financial Results

### Oberthur 2nd Quarter Results

Oberthur Card Systems has reported second quarter 2006 revenues of 122.9 million euros, topping the record-breaking 121.1 million euros Q2 2005 sales. Sales as of the end of June 2006 reached 244.7 million euros, showing 2.3% growth at current exchange rates over the 239.2 million euros revenue recorded in the first half of 2005. In a delicate environment under highly competitive conditions, Oberthur Card Systems delivered strong sales. During the second quarter of the year, Oberthur Card Systems delivered 58.7 million microprocessor cards, breaking the record of 58.2 million cards sold in Q4 2005, a period, which is traditionally characterised by strong seasonality. This performance was highlighted by a 30.5% increase in volume compared to Q2 2005. The microprocessor card top line reached 77.3 million euros.

### Gemalto 2nd Quarter 2006 Results

Gemalto has reported its revenue for the second quarter 2006, the first to consolidate Gemalto and Gemplus activity following the execution on June 2, 2006 of the first step of the combination between the two companies. The revenue reported includes Gemplus' June revenue of \$127 million. During the period, Gemalto recorded revenues of \$368 million, 2% lower than last year's comparable revenue, which includes Gemplus' June 2005 revenue of \$116 million. Olivier Piou, Gemalto's Chief Executive Officer commented: "The combination between Axalto and Gemplus is now effective. Since its announcement eight months ago, we have very steadily delivered on all the operational objectives we had set for Gemalto, ahead of schedule, and the integrated organisation is in place. Gemalto confirms its objective of 85 million euros annual net synergies in 2009.

### NDS Reports Fiscal 2006 Results

NDS Group plc has reported their revenue for the fiscal year 2006 were \$600.1 million, an increase of 8% compared to the previous fiscal year. Conditional access revenue increased; higher security fees resulting from growth in the number of authorised cards using NDS technologies were offset in part by lower deliveries of Smart Cards. NDS delivered 65.0 million active digital TV Smart Cards in their fiscal year 2006.





## Strong First Half Result for Ingenico

Ingenico has announced a record performance in the company's history, with revenue 22% higher than in the first half of 2005 (207.4 million euros). On a like-for-like basis, this translates into 27.5% growth for the six-month period, and 24% growth on a like-for-like basis and at constant exchange rates. This remarkable achievement was driven in particular by extremely strong business growth in Latin America, North America, Australia and Italy. "We are extremely pleased with our performance in this six-month period, especially with the sharp increase in revenue in North America (+ 47%), a top-priority growth region for Ingenico," said Amedeo d'Angelo, the Group's Chief Executive Officer.

## ActivIdentity 3rd Quarter Results

ActivIdentity Corporation has announced revenue for the third quarter ended June 30, 2006 was \$12.9 million compared to \$12.0 million for the quarter ended June 30, 2005, and \$11.1 million for the previous quarter ended March 31, 2006. Gross margin for the three months ended June 30, 2006 was 55% compared to 73% for the quarter ended June 30, 2005. Net loss for the quarter ended June 30, 2006 was \$5.3 million compared to \$5.6 million for the three months ended June 30, 2005. Net loss for the previous quarter ended March 31, 2006, was \$8.3 million.

## SCM 2nd Quarter Results

SCM Microsystems, Inc has announced revenues from continuing operations in the second quarter of 2006 were \$9.4 million, above previous management guidance of \$7 million to \$8 million and up 63% from revenues of \$5.7 million in the second quarter of 2005. By product segment, second quarter 2006 revenues included \$6.8 million from sales of Smart Card readers and other products for secure network and physical access, and \$2.6 million from sales of OEM digital media reader technology. SCM benefited in the second quarter from stronger than expected sales of Smart Card readers to support German e-passport programs and US government security projects. Sales of the Company's Smart Card reader products are subject to significant variability based on the size and timing of customer orders.

## VASCO 2nd Quarter Results

VASCO Data Security International, Inc has reported financial results for the second quarter and six-months ended June 30, 2006.

Revenues for the second quarter of 2006 increased 50% to \$18.5 million from \$12.3 million in 2005 and, for the first six months of 2006, increased 35% to \$32.2 million from \$23.8 million in 2005.

## Radio Frequency Identification

### RFID Reader Shipments Up 14%

The global market for RFID readers and reader modules grew to more than 35,500 unit shipments in 2005, according to new metrics released by ABI Research. In addition, the analysis reveals that reader unit volumes grew nearly 14% in Q1 2006 compared to Q1 2005. "By aggregating quarterly RFID reader shipment data from the industry's top suppliers, we are pleased to be the first in the industry to provide a truly accurate quantification of this fast-growing market," says Michael Liard, ABI Research's practice director for RFID and Contactless. Liard adds that the new database has a core focus on passive supply chain technologies, particularly those employing UHF technologies.

### 3-Year RFID Research Project

A three year initiative dedicated to research, development, training and demonstration in the effective use of RFID based on EPCglobal standards, launched in Brussels. The Building Radio frequency IDentification solutions for the Global Environment (BRIDGE) project is being supported by the European Union's Sixth Framework Programme for Research and Technological Development (FP6) with 7,5 million euros funding. Co-ordinated by global data standards body, GS1, the BRIDGE project brings together a consortium of 31 global organisations. Participants in the programme comprise universities in Europe and China, including three of the Auto-ID Labs, solutions providers, both large and small, together with large scale retailers, manufacturers and SMEs.

### Top Auditor Selects AXCESS' RFID

AXCESS International Inc has announced that PricewaterhouseCoopers has selected their ActiveTag RFID physical computer asset protection solution for use in their Mexico City office. Under the terms of the rollout, PricewaterhouseCoopers in Mexico will utilise AXCESS' Dual-Active RFID solution for its custodial asset management capabilities; allowing for real-time detection when a valuable asset such as a laptop is in or out of a secured area.





## RFID Revenue Forecasts Down 15%

ABI Research has announced that it has reduced its 2007 market forecast for RFID software and services revenue to \$3.1 billion, which represents a downward adjustment of approximately 15% from the firm's previous estimates. According to RFID practice director Michael Liard, the lowered revenue expectations result from the current direction of RFID's evolution, not from any decline in the industry. "Four interrelated factors, particularly within asset-management and supply-chain-management RFID markets, have led us to revise our forecasts," he says. "They are: market consolidation; collaborative solutions; the growing availability of off-the-shelf commercial RFID software packages; and the improving level of skills in RFID project planning."

## RFID to Track Aircraft Equipment

QinetiQ and the Harrier IPT have just started a one-year 'Proof of Concept' evaluation of an active Radio Frequency Identification (RFID) system that automatically tracks critical aircraft equipment between designated zones. The Forward Maintenance Asset Tracking (ForMAT) proof of concept underlines the IPT's drive for efficient assurance of operational capability and through enhanced visibility of assets, will improve aircraft turnaround, reduce stock holdings resulting in financial savings and minimise the effort spent looking for them.

## RFID To Track US Army Medical Files

3M Co has won a three year contract worth \$3.76 million from the US Army to develop and install a system that uses RFID technology to track medical files at Fort Hood Installation in Texas. The company feels that the proposed system would make a positive impact on operational efficiencies in health care delivery, the troop deployment process and the management of medical data collection. The proposed use of a RFID system to track medical files will substantially reduce errors and inefficiencies associated with manual tracking, retrieval, filing and file merging methods, the company noted.

### On the Move

## New CFO at Oberthur

Oberthur Card Systems has appointed François Rivière as Chief Financial Officer (CFO) of Oberthur Card Systems.

A graduate of the French Business School ESCP, François Rivière, 53, was formerly CEO of WILSON GESTION. Previously, François was CFO within PROUVOST / V.E.V. Group. He started his career in SCHLUMBERGER Group as controller of the subsidiaries in France and the UK. François Rivière replaces Cyril Malher who, after 6 years with Oberthur Card Systems, is leaving the Company.

## PubliCARD Appoints New CEO

The Board of Directors at PubliCARD, Inc have appointed Joseph Sarachek as its next Chief Executive Officer effective July 31, 2006. He succeeds Tony DeLise, who is leaving PubliCARD to pursue other opportunities. Mr. Sarachek has also been elected to the Company's Board of Directors.

## HID Appoints New Sales Manager

HID Global has appointed of Rob Pattiwaël as regional sales manager. Pattiwaël will be based in the Netherlands, with sales responsibilities for the Benelux territory, comprising Belgium, Netherlands and Luxembourg

## New CEO at Assa Abloy

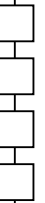
Juan Carlos García has been appointed Chief Executive Officer (CEO) of Assa Abloy ITG. The new CEO's chief task is the strategic repositioning of the brands ACG Identification Technologies, Soky-mat, VisionCard and Omnikey under the umbrella of Assa Abloy ITG. Based in Germany, García is responsible for ITG's global business, and reports to Joe Grillo, Executive Vice President of Assa Abloy's Global Technologies Division (GTD).

## Ingenico Reinforces its Team

Boosted by the preliminary results and successes of the recovery plan, Ingenico announced in September 2005, Ingenico has decided to bolster its management team by recruiting Didier Sérodon and Cyril Malher, as Chief Marketing Officer and Chief Financial Officer, respectively. Both new arrivals will also sit on the Executive Committee.

## ID Data to Bolster its Marketing Team

ID Data Systems has appointed Julie Roughton as Marketing Communications Executive, a new role within its Petersfield based marketing team. Julie's main role at ID Data will be to grow the scope and frequency of both ID Data's internal and external communications.





# NHS Failing to Secure Data on Mobile Devices

By Martin Allen, Managing Director, Pointsec Mobile Technologies



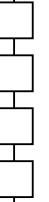
Martin Allen

A survey we have carried out of the healthcare sector on the use of portable data storage devices has found that almost two thirds use no or inadequate security and that half of those in the NHS use their own equipment to store data - a basic breach of security practice. This survey entitled "Mobile device usage in the healthcare sector" which was carried out by Pointsec Mobile Technologies and the British Journal of Healthcare Computing & Information Management has revealed that one fifth of the devices used to store data have no security on them at all and a further two fifths have only password-controlled access - which does not guarantee security from hackers.

Using basic hacker software downloaded from the Internet it would take a few seconds to bypass a basic password. Just a quarter of respondents used passwords with another form of security, including encryption, biometrics, Smart Card and two-factor authentication. Respondents included information managers, IT managers, medical professionals and a range of other job titles. Two thirds of the 117 who responded to the survey were in the NHS and a quarter were suppliers to the sector. USB memory sticks/memory cards (76%) were the most popular mobile device to be used to download data in the healthcare sector followed by laptop/tablet PC (69%), PDA/Blackberry (51%), smartphone (9%) and mobile phone (2%). Advances in technology have resulted in the ability to store gigabytes of information not just in these devices but also MP3 music players, cameras, voice recorders etc. The easy availability of tiny, high capacity storage devices such as USB memory sticks and memory cards makes it very easy for a person to carry unnoticed large amounts of data such as patient records or sensitive corporate data.

Overall, 42% of respondents owned at least one of the devices they used, but half of the NHS respondents were using their own devices to aid them in their everyday work. The most common type of data stored was personal contact details (80%), while three quarters stored work contact details. Nearly two thirds stored corporate data and an amazing fifth of the healthcare workers who were interviewed held security details - which could include passwords, PIN numbers and bank account details. About half of the medical professionals carried patient records on a mobile device. The majority of medical professionals used a password alone for security. One Doctor commented that his security was okay because he used "the initials of one of his patients as his password". Two-fifths used higher levels of security, but a small number had no security at all. Comments from respondents included a claim that there was minimal chance of loss or theft and a minimal chance of misuse. Another wrote "my patients couldn't afford to pay for blackmail and they probably wouldn't care if others knew" [about their medical records]. A couple thought that the risk to security was no worse than having information on paper.

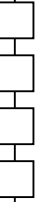
Over half expressed anxiety that patient details are being held on mobile devices. The biggest concerns were that if a device is lost or stolen it would breach patient confidentiality (57%) and that the information "could get into the wrong hands and be abused" (50%). This still leaves, however, a large number who didn't show any concern and thought that security was adequate. The survey shows that a large number of people are using their own devices for carrying data such as work contacts, corporate data and even medical records, which is a basic failure of security policy. Two thirds of the devices have no or inadequate security and there appears to be a lack of appreciation of the security risks among a large number of users. About 80% said that there was a security policy in their organisation, but the results of the survey show clearly that there is widespread and serious failure in the way that security policies deal with the risks of mobile devices and are enforced. There is much documented evidence of patients who are worried about the safe-keeping of electronic medical records, but this survey shows the medical sector themselves are worried about medical information being held on mobile devices which are not being secured by their NHS Trust. It will only be a matter of time before these weaknesses are exploited as it is very easy to steal or pick up a mobile device and access the information for ill-purposes. Mobile devices seem to be falling through the security net and our advice is that any NHS trust or organisation downloading sensitive or patient records should automatically encrypt the information. That way security no longer becomes an issue it becomes second nature and works in the background.





# Living With Smart ID

By Cath Rawcliffe, Head of eID, ACI Worldwide



*Cath Rawcliffe*

Implementing a national ID scheme is one of the most complex Smart Card deployments possible. A myriad of political, social, technical and data protection challenges have to be overcome. A typical example of this is the proposed National ID card scheme in the UK where debate still rages over so many aspects of the scheme. Curiously, however, very little of the discussion focuses on use and management of the card after it has been issued. It would seem that while politicians, professors, pundits and technologists spend considerable amounts of time and money deliberating and examining the challenges of issuing the Smart ID cards, no-one places any consideration on the enormous challenges and potential pitfalls that will be faced when citizens are actually living with Smart ID.

The most fundamental issue at stake here is whether or not it is possible for a Smart ID card to remain static from issuance through to the necessary replacement of the card - typically estimated at 10 years. If the cards can remain frozen in time, without any need to change then there need not be any concern. However, evidence from other Smart ID projects around the world strongly suggests that the cards will have to change to meet future demands. As such, the success of any ID scheme must lie as much in the flexibility of the card to adapt to change as it must around other important challenges such as the database. Failure to mitigate against the risk of change will inevitably mean that the initial investment has not been safeguarded and the citizen benefits will be low.

A simple example of the change within a Smart ID programme is certain details of the cardholder such as entitlement to citizen services. In practical terms this means the cards may need to be regularly updated and it is the way in which this information is updated that will be essential to making Smart ID cost-effective and attractive to other ID Service users. It is inconvenient for the citizen, impractical for the Government and expensive to produce entirely new cards every time the information on the chip needs to be updated. The Government must ensure that the chip has the capacity to be updated if it is to safeguard its initial investment and that it has the flexibility to choose new chip technology as needed to address future requirements whilst remaining in tune with European and other standards. At the same time, it is extremely beneficial for the system to be designed and built incrementally on existing legacy systems so that initial implementation costs can be minimised and rollout times kept to a minimum.

Smart ID in Hong Kong has demonstrated how this can work in practice. Hong Kong deployed a Smart ID card that can be updated post-issuance through its chip management solution. Data stored in the back-office databases is updated as necessary by authenticated users through a robust interface that provides a secure mechanism for changing the data to be held on the chip of a card. Of course, the legislation passed within the UK defines the data that the Government can hold on the national identity register and that may be held on ID Card and it is essential to protect this sensitive personal ID data. Initially the UK Smart ID cards will contain similar data to that held on e-passports. Indeed it is envisioned that Smart ID cards will replace the function of the e-passport for travel within European boundaries.

However, management of the core personal ID data on the card is just one part of the issuance and post-issuance debate. Even as the specifications of the Smart ID cards are being drawn up, a wider scope for the use of the cards is envisaged to provide extended ID services and secure other 'business users'. This is most likely to involve the use of the cards for more than the single ID function. Smart ID cards can potentially store a large number of applications from leisure and library cards, to 'Oyster' style transport cards and electronic cash functions through the use of an e-purse. In general, division of these functions into segments will occur, however a core infrastructure can be deployed as evidenced for the Hong Kong ePassport implementation currently in rollout. UK ID cards likewise need to be future-proofed. The card issuer must have a means of updating or adding new applications easily and at low cost. The freedom to manage new cards and other ID tokens such as ePassports must also be provided.





Hong Kong has faced a similar challenge - the need to be able to selectively load new applications onto a number of the cards after issuance. Hong Kong uses ACI Smart Chip Manager to meet this challenge. In addition to the mandatory application parameters mandated by the Hong Kong Special Administrative Region (HKSAR), it also offers its citizens the opportunity to add voluntary applications at will. For example, Hong Kong residents wishing to shop online can download a Digital Certificate onto their ID card. This allows the citizen to log on to online shopping sites and secure their transactions through the Smart ID card. The rollout of this application has seen a rise in secure online transactions in the region due to improved citizen confidence. When deploying Smart ID cards in the UK, the Government should maximise the uptake and benefits by consideration of such services and the ability to offer new applications to those who want them without having to update the whole ID programme. There is an enormous opportunity to extract cost and usability benefits from the scheme by adopting this approach.

By having full control of the card lifecycle the Government will be able to address future challenges such as managing multiple applications on a chip or supporting different cards/tokens and data sources for varying departments, agencies or local/regional government entities. Should a card be lost or stolen, the card management system will be able to handle the complexity of interacting with each department/database for the reissuance of the card. Similarly, should a change be required to an application - e.g. expiry or rescinding its use - then the card management system can ensure smooth interaction between the database and the card without the need for the citizen to be involved or any other application to be affected. It is functions such as these that will significantly enhance the end user's day-to-day experience of the ID card. Indeed, the ability to highlight the flexibility of the scheme through the use of cost-effective proven technology that can minimise future expense, will be a benefit for citizen acceptance.

It would be highly unusual for post-issuance requirements not to be considered within the UK ID scheme. What is clear from other Smart ID programmes around the world, such as in Hong Kong, is that such card management considerations have to be at the heart of the programme. The software needs to be able to manage the cards both pre- and post-issuance and work with multiple departments, agencies and other government bodies, as well as a variety of channels and functions to handle the workflow effectively. Failure to take lifecycle management and the need for a flexible card scheme into account could lead to costly and ultimately unnecessary changes in the future.

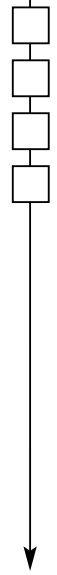
## Events Diary

### September 2006

- 06-08 2nd ICAO-Standard MRTD Symposium with Exhibition - *Montreal, Canada* - [www.icao.int/mrtd](http://www.icao.int/mrtd)
- 06-08 SmartCards Expo 2006 - *New Delhi, India* - [www.electronicstoday.org/smartcardsexpo.htm](http://www.electronicstoday.org/smartcardsexpo.htm)
- 06-08 Inter Airport China 2006 - *Beijing, China* - [www.interairport.com](http://www.interairport.com)
- 12-14 Cardex - *Moscow* - [www.cardexpo.ru](http://www.cardexpo.ru)
- 13-14 Air & Port Security Expo - *Brussels, Belgium* - [www.aps-expo.com](http://www.aps-expo.com)
- 18-20 Cards and Payments Conference & Expo 2006 - *Paris, France* - [www.efma.com](http://www.efma.com)
- 19-22 World e-ID- *Sophia-Antipolis, French Riviera* - [www.strategiestm.com](http://www.strategiestm.com)
- 20-22 e-Smart Conference 2006 - *Sophia-Antipolis, France* - [www.e-smart.eu](http://www.e-smart.eu)
- 20-22 Smart University 2006 - *Sophia-Antipolis, France*
- 25-26 Identity Theft & Fraud Symposium - *San Francisco, USA* - <http://list.sourcemediacom.com>

### October - 2006

- 9-12 Cards Africa - *Johannesberg* - [www.terrapinn.com/2006/cardsza](http://www.terrapinn.com/2006/cardsza)
- 11-12 Infosecurity (Netherlands) - *Utrecht* - [www.infosecurity.nl](http://www.infosecurity.nl)
- 13 Maximizing Software Security & Sales - *Orange County, CA* - [www.aladdin.com](http://www.aladdin.com)
- 18-19 Gartner IT Security Summits 2006 - *London* - [www.gartner.com](http://www.gartner.com)
- 26-27 Corporate Identity Mngement in Financial Services - *Barcelona* - [www.jacobfleming.com](http://www.jacobfleming.com)





# Privacy and Security



By Dr David Everett, Principal Consultant, Microexpert Ltd



*Dr David Everett*

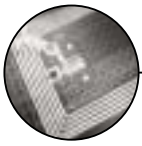
This month we hear of a new organisation, the Secure ID Coalition set up to alleviate the confusion among politicians and the public over the privacy and security of RFID. Just to make it clear the Coalition wants to make sure that we can distinguish between RFID and Smart Cards which while related are not the same technology. Feeling confused yet? Don't worry the Coalition is made up of Gemalto, Infineon, Oberthur Card Systems, Philips Semiconductors and Texas Instruments. Tres Wiley, manager of eDocuments for Texas Instruments is reported as saying that the conclusions of many of the security analyses often mix apples and oranges by lumping Smart Cards in with RFID.

Smart Card technology is not particularly new and its security capabilities have only come under the spotlight as security specialists have recently turned their focus to RFID. At this stage I would be feeling totally confused and this is clearly what happened to the particular journalist reporting above. Other journalists have cited Tres Wiley I suspect more accurately as saying that there is confusion between radio frequency identification tags used for tracking and tracing and contactless Smart Card chips as might be used for ePassports and eID cards. Perhaps all will become clear from the mission statement on the Secure ID Coalition website <http://www.secureidcoalition.org/>. The Secure ID Coalition is an affiliation of companies providing digital security solutions for identification documents, including contactless smart cards. Our mission is to promote the understanding and appropriate use of Smart Card technology to achieve enhanced security for ID management systems while maintaining user privacy. Such ID management systems include physical and/or logical access to facilities and networks. Coalition members support specific citizen privacy rights, which clearly this is just following the line of the data protection regulations. The motivation for the Coalition was to address the numerous pronouncements about RFID and Smart Card security vulnerabilities. Perhaps I'm missing something here but is there anything really new about this? Recently we have heard about attacks on the ePassport, the Belgium eID card, RFID viruses and worms, the Texas Instruments Speedpass payments tag, and a list that goes back for as long as I can remember.

Trying to educate the user that RFID and contactless Smart Cards are different technology seems fraught. In fact I would want to argue that contactless Smart Cards are a part of RFID, a view shared by Klaus Finkenzeller author of the RFID handbook. In the future I would be expecting to see very secure RFID tags used for payments and simple physical access control devices in the form of ISO ID-1 cards. The form factor has nothing to do with security. As for the radio communications, well some of the standards are common across a whole range of applications (e.g. ISO 15693). In fact at the current time the 13.56 MHz frequency band is used for ePassports, eID, contactless low value payments and most of the RFID (HF) article tags. At the end of the day a car is a car whether a Mini or a Rolls Royce. I have another problem and that is I do not believe you can expect lay users to understand the detail of what is going on under the bonnet (hood to my friends across the water). I sit and marvel at the magic of SSL that is the ubiquitous security infrastructure for web transactions. It is usually applied on a mono directional basis and relies on the user checking the authenticity of certificates (this really isn't going to happen). Without Smart Cards (there was going to be a plug here somewhere) all you achieve with SSL is a secure channel between two anonymous entities.

And then there is privacy which I want to define as, "Privacy is restricting public knowledge of the association of an individual's attributes and behaviour to their unique handle". If you look at the main concerns raised previously they are over the confidentiality of data which is a security service (also data integrity, authentication and non-repudiation). What is really required for privacy is restricting knowledge of behaviour in an identifiable way and that is what people really worry about. The use of any form of electronic tag, eID, Smart Card, ePassport is inherently a contradiction. There is a world of difference between showing credentials and recording them. And just for the record if you offer an electronic RFID card or token to a reader system you really don't know what is going on behind the scenes unless you can categorically vouch for the authenticity, correctness and integrity of that particular device. Technology helps us in every walk of life but in terms of personal privacy we might argue that it is already an illusion. What is for sure is that creating confusion between RFID and contactless Smart Cards and attempting to dismiss the academic security attacks as they arise is not going to produce a solution.

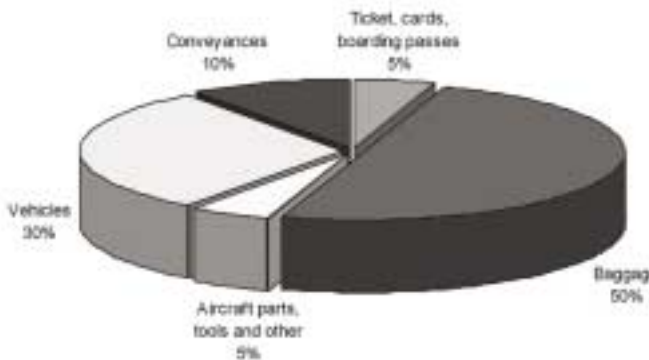




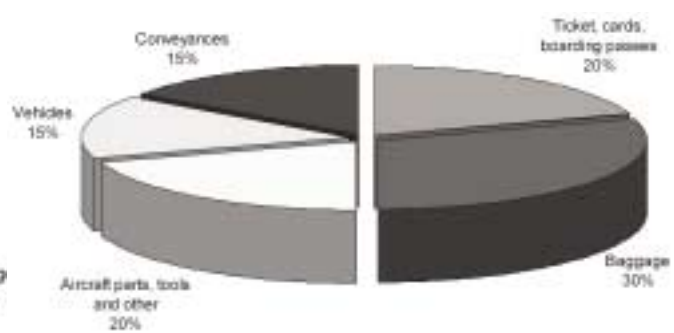
# RFID in the Air Industry and Land Transport

By Dr Peter Harrop, IDTechEx

As the RFID business grows strongly from \$2.8 billion in 2006 to \$26 billion in 2016, transport will be taking its fair share. Indeed, RFID in civil air transport alone will rise from \$42 million in 2006 to \$667 million in 2016, a major component being baggage tagging systems and tags at \$20 million in 2006 rising to \$100 million in 2016. Here a seminal decision was the unanimous vote of IATA, in October 2005, to settle on only one specification for the world's baggage tags, this being based on the UHF frequency band. This was courageous, because UHF works well with dry, non-metallic environments such as retail apparel in the UK and books in shops in the Netherlands, where there are few readers to interfere with each other but air baggage is none of these things. The technologists are wrestling with that one but in Europe and East Asia it is largely a waiting game as they hope for easing of UHF radio regulations to something nearer to the power levels, signalling protocols and bandwidth enjoyed in the US. However, few countries are willing to match the US regulations. Work rounds are on the way and the seven million or so airline bags that are lost yearly in the world, at a retrieval cost of about \$100 a time, must surely reduce some time soon. The split of value sales of RFID systems including tags in the air industry is shown below.



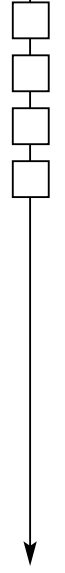
**Figure 1:** Percentage spend on RFID systems including tags exclusively for the civil air industry by application in 2006



**Figure 2:** Percentage spend on RFID systems including tags exclusively for the civil air industry by application in 2016

Boeing and Airbus are energetically introducing RFID on parts and equipment to reduce counterfeiting, automate status checks and make the supply chain more efficient. Virgin Atlantic, FedEx and others are deeply involved. UHF is preferred but there is interest in HF where appropriate. In transport in general, there is a boom in RFID tickets and cards to improve security and speed of transaction and some are increasingly usable for general purchases. Twenty million of the new e-passports are being issued this year, with their RFID labels for security and automated recording of movements. That figure will soon reach 40 million yearly as over 50 countries adopt them. Over eight million ExxonMobil Speedpass key fobs are in use for purchases at gasoline stations. The 4.5 billion credit, debit and account cards from Visa, MasterCard, American Express, JCB and others are gradually being issued in RFID form so they transact faster and are more reliable and longer lived. The first 20 million were issued last year. Well proven HF is used for RFID for ticketing, bank cards and passports.

However, nothing stands still for long in the RFID business and there is now great interest in locating people and things with RFID. For example, one major airport is trying to figure out how to make all people in the airport carry something that lets them be located at all times, the better to eliminate queues and improve evacuations and security. Tracking freight and baggage with the off electronic reader here and there and making heroic assumptions about what happens in between is all well and good but we need Real Time Locating Systems RTLS. These usually consist of RFID at 2.45 GHz because, at this license free frequency, you can locate things using time of arrival from interrogatory beams or be parasitic off pre-existing WiFi networks or use peer to peer ZigBee RFID. However, this is a very busy frequency like UHF and there are a lot of interference issues. The good news is that the cost of RTLS systems and tags is tumbling down. The tag no longer drains its battery in a short time, it is smaller and other impediments are largely overcome. RTLS on vehicles, assets, freight and even people - when they volunteer for queue elimination and other delights - is on its way.





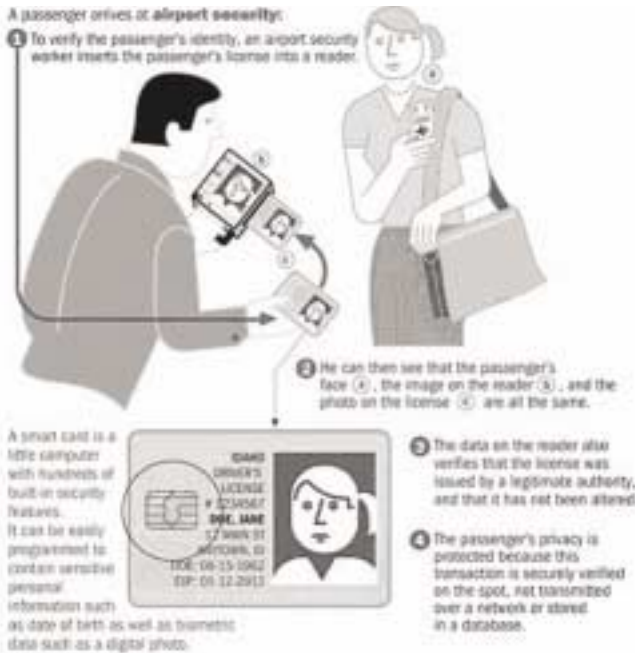
# The Real ID Card Act

By the Smart Card Alliance



In the United States, driver's licenses are issued by individual states. States also issue identification cards for use by non-drivers. States set the rules for what data is on a license or card and what documents must be provided to obtain a license or card. States also maintain databases of licensed drivers and cardholders. The REAL ID Act of 2005 stipulates that after May 11, 2008, "a Federal agency may not accept, for any official purpose, a driver's license or identification card issued by a State to any person unless the State is meeting the requirements" specified in the REAL ID Act.

The Act includes the following requirements: (A) A driver's license or identification card must include certain specific information and features. (B) A driver's license or identification card cannot be issued unless certain specific documentation is presented. (C) The state must verify all documentation presented with an application. (D) Driver's licenses or identification cards issued to persons who are present in the United States only temporarily can be valid only for the amount of time for which the persons are authorised to be in the United States. (E) Controls and processes must be established to ensure the security of the issuance process. (F) Each state must maintain a motor vehicle database and provide all other states with electronic access to the database. The REAL ID Act also stipulates that the technology incorporated into the driver's license or identification card must meet the following requirements: (1) It must support physical security features designed to prevent tampering, counterfeiting, or duplication of the credential for fraudulent purposes. (2) It must be a common, machine-readable technology, with defined minimum data elements. The Department of Homeland Security has the authority to issue regulations and set standards for compliance with the REAL ID Act.



**Smart Card Technology and Identity Applications** - Smart Card technology is currently recognised as the most appropriate technology for identity applications that must meet certain critical security requirements, including: Authenticating the bearer of an identity credential when used in conjunction with personal identification numbers (PINs) or biometric technologies, protecting privacy, increasing the security of an identity credential and implementing identity management controls. Countries around the world (such as Germany, France, Malaysia, and Hong Kong) use Smart Cards for secure identity, payment, and healthcare applications. In addition, public corporations (including Microsoft, Sun Microsystems, Chevron, and Boeing) use smart employee ID cards to secure access to physical facilities and computer systems and networks.

In response to Homeland Security Presidential Directive-12, the National Institute of Standards and Technology (NIST) has published the Federal Information Processing Standard 201 (FIPS 201), providing specifications for an interoperable Federal PIV card. The standard calls for a combined contact/contactless Smart Card that can authenticate the cardholder for both physical and logical access. The FIPS 201 standard not only applies to Federal employee and contractor IDs; it is also being used to specify the underlying requirements for the TWIC, Registered Traveller and FRAC credentials. States could incorporate the same proven PIV card technology into a state-issued Real ID (i.e., a driver's license or identification card issued to comply with the REAL ID Act). The PIV-based Real ID could then be used to authenticate the bearer in a "federal" situation, such as checking in at an airport. This Real ID card could also incorporate biometric factors to help verify the cardholder's identity. States that want to issue a Real ID card that uses the FIPS 201 standard would need to incorporate Smart Card technology into the card.





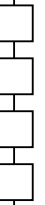
However, the states would not necessarily have to deploy any significant new infrastructure to use the Smart Card features. Each state individually could decide whether and how to use the personal identity verification applications in situations unrelated to Federal use. Examples of how state divisions of motor vehicles (DMVs) and law enforcement agencies could use and benefit from the use of Smart Cards are listed below. These and other applications could be phased in over time as the opportunity and economics of the applications evolve for each state: (A) Driver's license renewal - Renewal of driver's licenses could be expedited by an applicant coming to a DMV office or kiosk, inserting the Smart Card and getting a new card automatically; (B) Driving privileges - A DMV could revoke driving privileges for various infractions (for example, DUI, tickets) and still allow the individual to use the card for identification purposes. (C) Ticketing - Law enforcement officers could issue tickets by reading the Smart Card chip and getting all driver demographic data from the card automatically. (D) Driver histories - Driver history could be kept on the card enabling improved safety on highways where access to backend systems may not be available.

**The Benefits of Smart Card Technology** - Unlike alternative, less secure ID card technologies (such as magnetic stripe, printed bar code, optical, or RFID), Smart Card technology supports numerous unique features that can strengthen the security and privacy of any ID system.

**1) Strong Identity Authentication** - One essential characteristic of a secure ID system is the ability to link the individual possessing an identity document securely to the document, thus providing strong authentication of the individual's identity. Smart Card technology supports PINs, biometric factors, and visual identity verification. For example, the REAL ID Act requires that each person applying for a driver's license or identification card be subjected to a facial image capture. This facial biometric factor can be stored directly in the secure chip in the Smart Card and used to verify that the individual presenting the card is the individual to whom the card was issued. If states want to implement other biometric factors (for example, fingerprints), the biometric that is captured when the cardholder applies for the card (or is enrolled in the identification system) can be stored securely on the card. It can then be matched either on or off the card (in a reader or against a database) to verify the cardholder's identity. In addition, states can establish databases to achieve the goal of "one credential, one record, and one identity."

**2) Strong Card Security** - When compared to other tamper-resistant ID cards, Smart Cards represent the best balance between security and cost. When used with technologies such as public key cryptography and biometrics, Smart Cards are almost impossible to duplicate or forge. Data stored in the chip cannot be modified without proper authorization (a password, biometric template, or cryptographic access key). Smart Cards also help deter counterfeiting and thwart tampering. Smart Cards include a wide variety of hardware and software capabilities that can be used to detect and react to tampering attempts and counter possible attacks. When smart ID cards will also be used for manual identity verification, visual security features can be added to a Smart Card body. Adding a Smart Card chip to a Real ID would exponentially increase the difficulty of making a fraudulent ID card. The vulnerabilities of printed plastic ID cards are well known-fake state IDs are readily available for purchase over the Internet or in rogue ID card facilities. Smart Cards deter forgers and can ensure that only the person to whom the card is issued will be able to verify themselves when the card is presented. No other technology can offer such secure, trusted, and cost-effective identification capabilities.

**3) Strong Support for Privacy** - The use of Smart Cards strengthens the ability of a system to protect individual privacy. Unlike other identification technologies, Smart Cards can implement a personal firewall for an individual's data, releasing only the information required and only when it is required. The card's unique ability to verify the authority of the information requestor and the card's strong security at both the card and data level make Smart Cards an excellent guardian of a cardholder's personal information. Unlike other forms of identification (such as a printed driver's license), a Smart Card does not reveal all of an individual's personal information (including potentially irrelevant information) when it is presented. Information embedded on the chip can be protected so that it cannot be surreptitiously scanned or skimmed, or otherwise obtained without the knowledge of the user. Personal information stored on the Smart Card can be accessed only through user-presented PINs and passwords or by biometric matches at the place of use. By allowing authorized, authenticated access to only the information required for a transaction, a Smart Card-based ID system can protect an individual's privacy while ensuring that the individual is properly identified.





5) *Flexibility as a Secure Multi-Use Credential* - The driver's license is currently a multi-use credential. It not only indicates that the cardholder has driving privileges, it also serves as the default credential for establishing that the cardholder can board an aircraft, engage in age-related retail purchases, establish banking relationships, complete retail point-of-sale transactions, and apply for employment. Smart Card technology can support these current uses along with any additional applications that enhance citizen convenience and/or government service efficiency. For example, Smart Cards provide the unique capability to easily combine identification and authentication in both the physical and digital worlds. This capability can generate significant savings for states. A Smart Card-based driver's license or ID card could not only indicate privileges and allow physical access to services, it could also allow individuals to file taxes, request official papers (e.g., birth certificates) online, or access secure networks. Multiple applications (with their required data elements) can be stored securely on the smart ID card at issuance or added after the card is issued, allowing functionality to be added over the life of the driver's license or ID card.

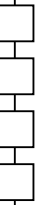
6) *Standards-Based Technology* - Smart Card technology is based on mature international standards (ISO/IEC 7816 for contact Smart Cards and ISO/IEC 14443 for contactless Smart Cards). Cards complying with standards are developed commercially and have an established market presence. Multiple vendors can supply the standards-based components necessary to implement a Smart Card-based ID system, providing buyers with interoperable equipment and technology at competitive prices.

7) *Cost-Effective and Flexible Offline Verification* - In addition to the privacy and security benefits afforded by Smart Cards, the technology also delivers features that support cost-effective offline verification and efficient use of the ID card once the card has been issued.

Verification of a cardholder's identity is often required at multiple locations or at points that do not have online connections. A Smart Card-based ID system can be deployed cost-effectively at multiple locations by using small, secure, and low-cost portable readers that take advantage of the Smart Card's ability to provide offline identity verification. For example, verifying a cardholder's identity with biometrics would not require access to an online database: the Smart Card can securely hold the necessary biometric identifier, with the secure chip on the card comparing it to the live biometric. The credential on a card can be authenticated by a reader using digital signatures contained on the ID card, making it a trusted credential-online or off. One key issue that has been raised by different states and by the American Association of Motor Vehicle Administrators (AAMVA) is the cost of Smart Card technology. While a smart ID card or driver's license may cost a little more than a plastic card, the cost of the card itself is a small fraction of the total cost of implementing an identity system that complies with the REAL ID Act.

When considering costs, it is important to understand the advantage of an ID that is strongly tied to the bearer and enforces citizen privacy. By incorporating Smart Card technology into a Real ID, states can place a portable security agent in the hands of the cardholder, ensuring that the state's security policy is enforced and that only an authorized cardholder can be authenticated before specific identity information is released. Any additional costs associated with the technology are a small price to pay for such robust security. Moreover, the ability of Smart Card technology to support additional applications can generate both cost savings and potential new revenue sources. In addition, Smart Card technology is flexible. Unlike today's printed plastic cards, Smart Cards can be updated and managed throughout the life of the card.

**Conclusion** - The Smart Card Alliance strongly recommends that Smart Card technology be adopted as the underlying infrastructure for state driver's licenses issued to comply with the requirements of the REAL ID Act of 2005. Smart Cards have been proven to be the most cost effective and secure identity authentication and verification technology. They are already widely used for secure identification in both the public and private sectors, are based on international standards, can provide all of the features required to meet the security requirements of the REAL ID Act, and can deliver strong privacy protection for the cardholder's personal information. Once states have adopted Smart Card identification technology, they can then decide whether to use the trusted Real ID credential for other applications beyond the Federal points of use according to their needs, budgets, and timeframes. Failure to embrace Smart Card technology will undermine the fundamental goal of the REAL ID Act-ensuring that the Real ID is not fake and that it is being used by the intended bearer.





# The US Western Hemisphere Travel Initiative

By Jason Smith, Staff Reporter, Smart Card News Limited



Jason Smith

Smart Card News touched on the WHTI in our July issue with Randy Vanderhoof of the Smart Card Alliance strongly recommending that 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 the Department of Homeland Security (DHS), before the final implementation decision for the WHTI PASS card program is made.

The Western Hemisphere Travel Initiative (WHTI) is one element of a much larger bill - the Intelligence Reform and Terrorism Prevention Act - approved by US Congress and signed by the President of the US in late 2004. Following up on a recommendation of the 9/11 Commission, Congress acted to remove what was known as the Western Hemisphere Exception - a rule that permitted returning US travellers and some foreign nationals to present driver's licenses and/or birth certificates upon entering the United States. Once implemented, the WHTI will require all travellers, including US citizens, to and from the Americas, Canada, the Caribbean, and Bermuda to have a passport or other accepted document that establishes identity and citizenship to enter or re-enter the United States.

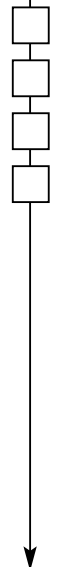
"In the aftermath of September 11, the Department of State's Bureau of Consular Affairs conducted a comprehensive review of our procedures for adjudicating the travel documents that we have the legislative authority to issue: US passports, and immigrant and nonimmigrant visas. The US passport is arguably the most valuable travel and identity document in the world. As the report of 9/11 Commission noted, travel documents are as valuable to terrorists as weapons, and we have taken steps to improve both the security features of the passport, as well as the underlying adjudicatory process that determines who is entitled to one." Remarked Frank E. Moss, Deputy Assistant Secretary for Consular Affairs at a US Senate Foreign Relations Committee Subcommittee on Western Hemisphere.



"Our goal is to strengthen border security and expedite entry into the United States for US citizens and legitimate foreign visitors," Homeland Security Acting Under Secretary for Border and Transportation Security, Randy Beardsworth stated. "By ensuring that travellers possess secure documents, such as the passport, Homeland Security will be able to conduct more effective and efficient interviews at our borders." Given the enormity of this change in practice, the Department of Homeland Security (DHS) and the Department of State (DoS), in consultation with other government agencies, agreed to adopt a phased implementation plan for the WHTI. The current proposal is to roll out the WHTI in two phases, with the timeline as follows:

- ❑ **December 31, 2006** - Requirement applied to all air and sea travel to or from Canada, Mexico, Central and South America, the Caribbean and Bermuda.
- ❑ **December 31, 2007** - Requirement extended to all land border crossings with Canada and Mexico.

The most recent major development in the US to-date has been the introduction of the People Access Security Service (PASS) card, or passport card, as part of the Rice-Chertoff Vision in January 2006. The PASS card is proposed as an inexpensive and secure biometric passport card that will serve as an alternative to a traditional passport and would be made available to US citizens for use in land-border crossings. As previously noted, the passport (US or Foreign) will be the document of choice for entry or re-entry into the US. However, another document that may be acceptable under the travel initiative is the Border Crossing Card, (BCC - or "laser visa"). Currently, the BCC serves in lieu of a passport and a visa for citizens of Mexico travelling to the US from a contiguous territory. Other documents that may be acceptable under this initiative are the Customs and Border Protection Secure Electronic Network for Travellers Rapid Inspection (SENTRI), NEXUS and Free and Secure Trade (FAST) program cards.





Additional documents are also being examined to determine their acceptability for travel. The government would expect that acceptable documents must establish the citizenship and identity of the bearer, enable electronic data verification and checking, and include significant security features. Ultimately, all documents used for travel to the US are expected to include biometrics that can be used to authenticate the document and verify identity.

So what effect will the WHTI potentially have on the US? Well obviously this initiative will strengthen their border security, safeguard identify documents against counterfeiting and facilitate secure entry into the United States for US citizens and legitimate foreign visitors. But what are the unforeseen problems with this new tiger control over its border.

Lets just take the Canada-US border for example! Many people on both sides of the border fear WHTI will severely curtail social and economic relations between the two countries. Currently Canada and the US have a unique relationship, characterised by the world's longest undefended border. This initiative threatens to undermine that relationship by blocking the free flow of legitimate goods and people. The greatest harm will be to the cross-border communities that span the border from coast to coast.



More than 300,000 people from both countries cross the border every day to work, shop and visit family and friends, but they don't rely on passports. In fact, only 23% of US citizens and 40% of Canadians hold valid passports. To this measure, when WHTI is fully implemented, we could see a multitude of community and family relations grind to a halt, from birthday celebrations to school trips to business and professional events. In addition to stifling community-to-community relations, the US WHTI will come with a steep economic price tag. Canada's trading relationship is the largest in the world, worth more than \$1.2 billion a day. More than 5.2 million US jobs rely on trade with Canada. After 2008, when WHTI is adopted, projections show that the Canadian tourism industry stands to lose up to \$1 billion a year. The US will be similarly affected, with a projected \$750-million decline in tourism receipts in US communities from 2005 to 2008.

But those are just the effects of Canada alone; the US also has to consider the effects of the travellers to and from Mexico, the Caribbean, Bermuda and the Americas. The State Department estimates that some 2.0 million Americans travel each year to the Caribbean without a passport. And, American citizens make about 100 million land border crossings each year. But to add salt to the wound, the proposal to stagger implementation of the new requirements, starting with air and sea travellers in 2007 and moving to land travellers in 2008, will increase uncertainty and further discourage cross-border travel and trade.

Both the DoS and the DHS recognise that there are a host of issues that must be addressed thoroughly to implement the WHTI smoothly and successfully. A critical part of successful implementation is public participation in the regulatory process. With this in mind, they will solicit public comments as a way to refine the implementation of the WHTI. The Departments have prepared an Advance Notice of Proposed Rule-making (ANPRM) and expect that the comments they receive after it is published will have a material effect on what they develop.

The ANPRM process is an important step in informing the public of this important change in travel requirements. In addition to explaining the new requirements to the American public, the DoS will also work with their hemispheric neighbours to make sure that they are aware of the requirements of the WHTI and that they have adequate notice to take the necessary steps to comply with them without hindering the legitimate flow of people and goods between the nations. To also help assess the land border implications of this program, the State Department has contracted with outside experts who will survey land border crossers at 16 ports of entry to help them develop more accurate data on the scope of this aspect of WHTI.



"We recognise the implications WHTI may have for industry, business and the general public, as well as our neighbouring countries, and they are important partners in this initiative. The advanced notice of proposed rule making will allow these affected publics to voice concern and provide ideas for alternate documents acceptable under the law," explained Assistant Secretary of State for Consular Affairs, Maura Harty. "The overarching need is to implement this legal requirement in a way that strengthens security while facilitating the movement of persons and goods."

