

### Smart Card & Identity News

Is published monthly by  
Smart Card News Ltd

**Head Office:** Smart Card Group,  
Suite 3, Anchor Springs, Duke Street,  
Littlehampton, BN17 6BP

**Telephone:** +44 (0) 1903 734677

**Fax:** +44 (0) 1903 734318

**Website:** [www.smartcard.co.uk](http://www.smartcard.co.uk)

**Email:** [info@smartcard.co.uk](mailto:info@smartcard.co.uk)

### Editorial

**Managing Director** – Patsy Everett

**Technical Advisor** – Dr David Everett

**Production Team** - John Owen,  
Lesley Dann, Suparna Sen

**Contributors to this Issue** – Tom  
Tainton, Michael Trader, Suparna Sen,  
Stephen Price-Francis, Michelle  
Weatherhead

**Photographic Images** - Nejrion -  
Dreamstime.com

**Printers** – Hastings Printing Company  
Limited, UK

**ISSN** – 1755-1021

### Disclaimer

Smart Card News Ltd shall not be liable for inaccuracies in its published text. We would like to make it clear that views expressed in the articles are those of the individual authors and in no way reflect our views on a particular issue.

All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means – including photocopying – without prior written permission from Smart Card News Ltd.

© Smart Card News Ltd

## Our Comments

Dear Subscribers



*Patsy Everett*

Well we knew it was going to happen if the Tories got into power and yes in the Queens Speech this month the ID card is top of the list of things to go. Now of course, can you believe it, people are actually saying it won't save much money but human rights and all that will be preserved.

There are even plans to reduce the number of CCTV cameras around the land but I'm personally far more interested in those yellow boxes and more particularly the camera tripods operating out of the back of a van. Not for one minute would I suggest breaking speed limits but sometimes, change that too often, they are just in the wrong place. Sited to catch you unawares with little danger to others, in fact the last one I saw was literally 50 yards before the end of speed limit sign on a hill well past the occupied land. It was only 36 miles an hour but that was enough to get the summons and I'm sure my other half now appreciates better the dangers of speeding. He elected for the speed awareness course and did actually come back saying it was worth while albeit it took the best part of a day to get there and back.

But now there is no ID card or Identity Register what next? Well for some time we have preached about the humble driving licence, in the UK at least and probably still in America now that they have the counterfeits under better control, it is a pretty basic but none the less effective ID card. In fact I don't know about you but in general this is the document that I use the most when somebody asks for proof of identity and that is not just in the UK but also Europe more generally and North America. It's a convenient size and provides all the information the challenger requires and if you were to put a chip on it (sorry probably in it) then what else would you need? The last time I raised this at a dinner party there were screams from the non drivers around the table, am I unique in knowing so many people that like to be driven by others? Anyway sanity ruled even after a delicious bottle(s) of Chianti and eventually it was agreed that there was no difficulty in applying for a driving license whether you drive or not. I've notched that one up for posterity! And when it happens, not if, just remember you read it here first and just for the record my optimism is flavoured by the fact that the DVLA is in my view one of, if not the most effective service centre in the UK government! Perhaps it has something to do with living in Wales?

The other bit of interest this month was the excitement surrounding the Oyster card, which bit I can hear you saying. Well the BBC decided to do a Freedom of Information attack on Transport for London (TfL) and shock horror they discovered that TfL have £30 million stashed under the carpet every year from unclaimed or lost card value. Apparently a total of 16.5 million cards sat idle during the financial year 2009/2010 with an average amount on each card of £1.80. There's more, last year 31,000 Oyster Pay as you Go (PAYG) were issued and topped up but never used with a total value of £246,000. What would you do without the tourists?

Now the really interesting point here is that the wheel keeps going around, when the family and I first got involved with smart cards (yes





it was and still is a family affair) the electronic purse was all the rage and this was back in the late 70s and early 80s. The business case was all about the Float, that pot of gold accrued from the total prepaid and unspent value that the operator could invest to his financial advantage. This is of course true for any prepaid scheme Oyster card, iTunes card, etc. But the other thing we knew all those years ago is that not all the value would be taken back, people would lose the cards, tuck them under their pillow or do all those other things we can't mention. In fact we predicted back in those golden days that 2 – 4% might be an expected and that this escheat as it was called could be a lucrative business. However there is one little snag, unless you have an expiry date on the card you can't really claim it because the liability always exists. Guess what? There is no expiry date on an Oyster card, who on earth left that out?

Patsy

## Contents

### Regular Features

Lead Story - NHS scaring patients into accepting care summary record . . . . .	1
Events Diary . . . . .	3
World News In Brief . . . . .	7,10,13,16

### Industry Articles

Finger Biometrics - Not the one-size-fits-all Solution . . . . .	5
Chipmakers Face First Fine Over Price Fixing . . . . .	9
Man, Machine and Advanced ID Credentials . . . . .	11
Sagem Security announce launch of the latest in identification . . . . .	14
Prevention is better than cure - How banks can protect their customers against - the card fraud threat during big sporting events . . . . .	15
MasterCard Continues to Displace Cash. . . . .	19

## Events Diary

### June 2010

- 2-4 Debit and Prepaid Conference 2010, Budapest, Hungary
- 6-8 Mobile Banking and Emerging Applications Summit, Las Vegas, NV, USA -  
<http://www.americanbanker.com/conferences/mobile10/>
- 7-9 Smart Cards + RFID China 2010, Beijing, China - <http://www.scsl-china.com/enindex.asp>
- 9-10 European e-Identity Management Conference, Cardinal Place, London -  
<http://www.revolutionevents.plus.com/eema/index.htm>
- 14-16 Prepaid Conference & Expo, London - [www.prepaid-conference.com](http://www.prepaid-conference.com)
- 16-18 Payments Panorama 2010, Vancouver, Canada -  
<http://www.cdnpay.ca/conference/english/homepage.html>

Source: [www.smartcard.co.uk/calendar/](http://www.smartcard.co.uk/calendar/)





21-22 Contactless Cards & Payments, Marriott Hotel Regents Park, London –

<http://www.smi-online.co.uk/events/overview.asp?is=8&ref=3407>

22-23 Cardware 2010, Ontario, Canada –

<http://www.actcda.com/calendar.html>

### July 2010

7-8 The Future of Cards and Payments, Le Méridien Piccadilly, London, UK -

<http://www.marketforce.eu.com/Conferences/cards10/>

*Source: [www.smartcard.co.uk/calendar/](http://www.smartcard.co.uk/calendar/)*

## NHS scaring patients into accepting care summary record.... Continued from page 1

At the Infosecurity Europe conference this month, Deputy Information Commissioner David Smith said that the NHS currently hold the undesirable title as the biggest single UK organisation that loses data. Since November 2007, a staggering 287 out of 962 serious data loss incidents have been made by the NHS.

You'd expect any organisation which processes personal information to at least ensure that the information is secure. Not so, with the NHS. The most recent episode was the loss of a data stick containing information on psychiatric patients in Forth Valley, Scotland. The Information Commissioner's Office (ICO) has announced that they'll be investigating the matter. The ICO recently gained the power to fine organisations up to £500,000 for serious data breaches, but they said it was 'too early' to say whether they would consider using its powers in this instance.

But if ever the ICO needed a reason to wield their authority, surely the NHS (and their debacle of a track record) provides the perfect incentive for tougher sanctions?

Despite the latest data loss errors, the NHS Connecting for Health agency posted a document on their website listing the dangers to patients if they continued to have their medical information stored in paper form. Warnings have been placed on the site saying that failure to sign up could lead to further lost records and operating errors. Visitors to the website are warned that if they choose to opt out of the computerised scheme, they could suffer 'adverse consequences' or a 'delay for correct treatment.'

The document states, that if a patient chooses to opt out, then:

- "Health-care staff treating you may not be aware of your current medications in order to treat you safely and effectively."
- "Health-care staff treating you may not be made aware of current conditions and/or diagnoses leading to a delay or missed opportunity for correct treatment."
- "Health-care staff may not be aware of any allergies/adverse reactions to medications and may prescribe or administer a drug/treatment with adverse consequences."

Critics have panned Connecting for Health's controversial tactics; a strategy which highlights the risks of the current paper-based records system whilst brushing aside concerns about the care summary record. Experts argue that the dangers are not as severe as the NHS is suggesting. A department of Health spokesman said the problem of lost records was not a major concern, prompting further speculation that the government is frightening patients into joining the scheme.

By Tom Tainton, Smartcard & Identity News



# *Finger Biometrics - Not the one-size-fits-all Solution*

*By Michael Trader, President and Co-Founder of M2SYS Technology*



*Michael Trader*

The world is changing, and with every moment comes a new, emerging technology that makes our lives easier, more efficient, and provides us with the tools that we need to be more productive and secure. Many businesses are openly embracing these advances as a way to gain a competitive edge and provide unparalleled customer service. For instance, biometric technology has surfaced as a perfect example of a trusted resource.

Biometrics is the science of using unique human characteristics such as fingerprints or iris images to positively identify individuals. The technology is gaining widespread popularity in many different markets, such as banking, healthcare, public safety, workforce management, point-of-sale, and membership management.

As with many modern technologies, biometrics has rapidly evolved. Inevitably; however, a by-product of innovation is the process of determining a technology's strengths and weaknesses. For instance, some are finding that fingerprint recognition may work well for a particular demographic, but worse for another because of varying issues such as population diversity and environmental conditions.

The advancement of Hybrid Biometrics™ promises to mitigate these weaknesses and offer unprecedented flexibility in the adoption and application of biometric technology. This article brings this concept to light by summarizing a case where multiple biometric modalities were seamlessly coalesced through the use of a new biometrics solution from M2SYS Technology to achieve higher accuracy and reliability rates.

## Case Study – Workforce Management Deployment

In recent years, thousands of companies have turned to biometric technology to streamline the employee identification process. To the surprise of many, the implementation of fingerprint recognition technology has been unreliable and often falls short of identifying users at consistent and acceptable rates. In fact, many people worldwide are finding that fingerprint biometrics is not the one-size-fits-all solution they once thought.

Take a popular property management company in the United States. The company has an employee base of 1,500 people across more than 250 locations. Prior to installing a fingerprint authentication system, the workforce management process was susceptible to “buddy-punching”, or one employee clocking in for another. The American Payroll Association estimates that businesses can lose between 2-5% of gross annual payroll expenditures from buddy-punching.

Seeking to completely eliminate the hassle and expense of buddy-punching and forgotten ID cards, passwords, or PINs, and to bolster employee accountability, the property management company integrated a low-level fingerprint Software Development Kit (SDK) into its workforce management system and enrolled biometric information of their employees.

What they failed to realize is that near-perfect conditions have to consistently exist to reliably identify employees. For example, the company did not know that Harold, the 60 year-old maintenance manager who has worked heavily with his hands over the past 40 years, had severely degraded fingerprint ridges from a lifetime of working with chemicals and tools. They failed to take into account that Lisa, a leasing manager who gets very chapped skin during the winter season, will have dry fingerprints, making for a very poor and often unrecognizable fingerprint scan.

Shortly after setting up the fingerprint recognition workforce management system, many employees notified management that they had difficulty or could not clock-in at all. The company suddenly realized that fingerprint technology wasn't the fix-all that they had sought. While some employees, such as Maria the office manager, had no issues, Paul, the electrician, was not even able to enroll in the system.

The crux of the company's problem was that they failed to include the physiological diversity of their employee population as a deciding factor in which biometric technology would be the most efficient for their workforce management needs. After one month of exclusively using fingerprint recognition, their biometric technology implementation was not producing ideal results. Incorrect scanning procedures, skin surface



issues, and overhead costs signalled a needed change. Since management was adamantly focused on increasing profits by eliminating buddy punching, the company had to make some quick decisions about how to solve their problems.

Upper management took time to assess the situation. Although user errors existed, there were also several success stories. Eliminating a biometric component altogether would re-introduce the previous and flawed mechanism of workforce management at the expense of employees who could be reliably authenticated. Sticking with the fingerprint-only biometric solution would prevent them from achieving their goal of 100% biometric read rates and maximized cost reduction.

The company heard about other forms of biometric authentication such as finger vein, palm vein, and iris biometrics, but did not have an easy mechanism to implement these modalities. Originally, they paid thousands of dollars for the low-level fingerprint SDK and biometric readers. From development to rollout it took about four months to get the system up and running. They could spend the time to research and find a new SDK, pay for development, and deploy the system with the hope that it would resolve their issues.

Through internet research and a referral from their workforce management software company, the property management firm identified a solution called Hybrid Biometric Platform™ that uses a unique integration methodology called Bio-Plugin™ to facilitate the rapid integration of four leading forms of biometric technology from a single software installation.

After several referrals and a free trial, they implemented Hybrid Biometric Platform™ from M2SYS Technology. They learned that vein technology, such as palm or finger vein, completely eliminated skin surface issues by reading beneath the surface of the skin, providing near 100% read rates every time. The solution still provided the option to implement fingerprint recognition at locations where it was effective, which lowered their total cost of ownership.

Several months after the switch to Hybrid Biometrics™ the property management company's employees were reliably clocking into work by following the quick scan of a palm vein, finger vein, or fingerprint. Harold the mechanic, Maria the office manager, Lisa the leasing manager, and Paul the electrician now clock into work without scanning inconsistencies, providing a greater return on investment and maximized employee satisfaction.

After trial and error this property management company found that the ideal biometrics solution was not solely fingerprint recognition, but rather a Hybrid Biometric Platform™ that allowed them to experience higher accuracy and reliability rates.

## Advertising with Smart Card News

Let the power of advertising with Smart Card News ([www.smartcard.co.uk](http://www.smartcard.co.uk)) bring customers direct to your website. Smart Card News is the number one source for Cards, Payments, Cryptography, Biometrics, RFID, EMV and Security relating to the Smartcard industry.

Just type smart card into Google, our second place ranking attracts thousands of visitors to our website, from Smartcard companies, Government agencies, Research companies and Universities. One of the best ways of increasing your website ranking is to be linked by other established industry websites.

If you require any additional information or would like to discuss your requirements, please contact Lesley on +44 (0) 1903 734 677 or email: [lesley.dann@smartcard.co.uk](mailto:lesley.dann@smartcard.co.uk)



## World News In Brief

### **Educated iTunes Fraudsters Jailed**

A gang of highly educated fraudsters turned their talent to crime in a sophisticated iTunes fraud which was set to make them all millionaires. The swindlers included a PhD student - Kibriya Ahmad, two IT experts - Mohammed Rasool and Suhail Tufail, a scientist - Ketanbhai Kantubhai Patel and a former business school student. They used stolen credit card details to generate cash through the sale of iTunes cards on social media websites. Detectives believe the fraud had the potential to rake in more than £4m. One of them used computers at the University of Manchester to take part in the money-making scheme.

The eight-strong gang, from Rochdale, carried out £777,278 of unauthorised purchases from Apple before the scam was exposed. The fraudsters used the credit card numbers, understood to have been hacked from an online retailer, to buy £100 gift certificates in bulk from Apple. They were then sold on eBay and through websites for a fraction of their face value, netting them around £200,000 in cash. It is estimated the scam cost Apple up to £800,000. However, the company declined to comment.

### **LaserCard supplies Next Generation RFID 'Green Cards'**

LaserCard Corporation, a leading provider of secure ID solutions, has announced the introduction of the next-generation U.S. Permanent Resident Card ("Green Card") featuring advanced optical security media and, for the first time, a Radio Frequency Identity (RFID) tag for compliance with the Western Hemisphere Travel Initiative (WHTI).

Mailing of the new card by the U.S. Department of Homeland Security (DHS) to legal permanent residents began May 10. Designed and manufactured by LaserCard, the Green Card is issued to lawful permanent residents as evidence of their authorisation to live and work in the United States. LaserCard has been shipping quantities of the new card to DHS for several months under a previously announced contract.

### **2010 SC Magazine Europe Award given to Imprivata**

Imprivata Inc., the company that simplifies and secures user access, has been awarded the prestigious 2010 SC Magazine Europe Award for Best Biometric Solution. The ceremony, held alongside the Infosecurity Europe 2010 Conference, saw Imprivata's trademark OneSign solution named the inaugural winner in this new category award. OneSign was acclaimed for its flexible support for a

broad range of biometric devices, enabling organisations to enforce strong security policies across the enterprise while increasing user satisfaction and improving workflow. Imprivata was also named as a finalist for Best Information & Access Management Solution, as well as Information Security Project of the Year for its implementation at Invensys Rail.

### **First Biometric Cash Machine arrived in Europe**

A Polish bank has become the first in Europe to offer the use of biometrics instead of PINs at cash machines. Customers of BPS visiting one of its ATM in Warsaw have the option of using placing their fingerprints on readers, instead inputting a four digit code, to authorise withdrawals or other transactions following the introduction of new technology this week.

The system is based on the recognition of the pattern of veins in an enrolled customer's finger, a form of biometric technology developed by Hitachi. The technology is already widely used in Japan but new to Europe.

### **Turkey offers World's First NFC-enabled SIM Cards**

Garanti Bank, the second largest private bank in Turkey and Avea, Turkey's sole GSM 1800 mobile operator, have teamed up to provide Turkish mobile phone users with NFC-enabled SIM cards that remove the need to buy NFC-enabled handsets.

Developed in conjunction with MasterCard and Gemalto, this new offering is a world first and will be available from July 2010. It enables users to conduct mobile contactless payments at numerous compatible payment terminals in Turkey and around the world. Users convert their existing mobile phone to become compatible with NFC technology simply by installing the new SIM card. This will enable them to immediately benefit from the convenience of the new payment method without having to replace their existing handset.

### **Gemalto selected for Austria's First Picture Card Program**

Gemalto, has announced that RZB (Raiffeisen Zentralbank Österreich), the central institution of Austria's largest banking group - the Raiffeisen Banking Group, has begun deploying its innovative, end-to-end solution for customising payment card designs securely over the internet. Central to the program is Gemalto's user-friendly web-based interface that lets users customise their EMV



payment card with a picture of their own choice. This is the first picture card program in Austria and its commercial rollout started in early 2010.

## **Kratos awarded \$4.4 Million in New Homeland Security System Contract Work**

Kratos Defense & Security Solutions, Inc., a leading National and Public Security Solutions provider, announced that its Public Safety and Security segment has recently received new security system deployment and integration contract work of approximately \$4.4 million, including options. The contract awards include security system design, deployment and integration work for a large, international petroleum and natural resources, a large regional hospital and a public museum of natural science. All of Kratos' work will be performed at locations in U.S.

## **Finally Smart Credit Cards arrive in U.S**

In middle of May, the United Nations Federal Credit Union (UNFCU) became the first financial institution in the U.S. to unveil plans to issue credit cards that comply with the Europay MasterCard Visa (EMV) smartcard standard. The credit union's new Platinum Visa EMV cards will be issued to about 5,000 of its most high-value customers and can be used anywhere EMV cards are accepted.

## **Expansion of European Contactless Smart Card Schemes**

Of the two major European service station companies, fuel giant Orlen Germany will deploy cashless payment terminals across its entire 511 service station network by the end of 2010 and has already introduced the technology in 120 locations.

French company Carrefour will also implement a similar project at its 210 hypermarkets and 1,200 service stations in France.

## **Cubic Telecom launches Europe's First iPad 3G SIM Card**

Europe's first SIM card for the new iPad 3G has been launched by Cubic Telecom, an Ireland-based mobile network operator. The newly introduced SIM card went on sale in the US on April 30. This clearly shows that the iPad 3G users, without racking up expensive roaming charges, will be able to travel and access the web anywhere in Europe.

Sold under the brand name MaxRoam, the first Cubic Telecom iPad 3G SIM cards are available for sale. Available at €75, the SIM card comes preloaded with 50MB data.

## **Industry-Leading Mobile Banking Technology finally reached Caribbean**

Sybase 365, a subsidiary of Sybase, the global leader in mobile messaging and mobile commerce services, announced a partnership with FirstCaribbean International Bank (largest regionally-listed bank in the English and Dutch-speaking Caribbean) to provide customers with mobile banking services enabling them the flexibility and convenience of managing finances over their mobile phones, without needing to visit a branch.

## **Watchdata and Institute of Microelectronics to Develop Contactless ASIC**

The Institute of Microelectronics (IME), a research institute of the Agency for Science, Technology and Research and Watchdata Technologies Pte. Ltd., a pioneer in data security and smart card technology solutions, has announced their partnership to develop a contactless ASIC solution for use in SIM card along with SIM IC and microcontroller for contactless payment application. The research development will leverage on IME's innovative ASIC solution and Watchdata's expertise in system implementation.

Through the contact interface, the SIM acts as a standard SIM card to execute subscriber's identity authentication to the mobile phone. The contactless feature can be used for services such as transportation, movie ticketing, mobile banking, access control and even retail outlets.

## **Verizon partners with U.S. Secret Service on Data Breach Report**

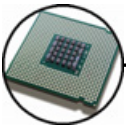
Verizon's Data Breach Investigations Report (DBIR) will now include data from hundreds of computer crime cases investigated by the U.S. Secret Service, the company announced last week. The report, which tracks data loss incidents, is based on a framework called VERIS that allows the comparison of data sets.

According to Verizon's Wade Baker, the 2010 report which is slated for release this summer will feature findings from Verizon's own caseload and hundreds of computer crime cases investigated by the Secret Service.

## **Symantec's \$1.28 Billion Cash Deal**

Symantec Corp. has decided to pay \$1.28 billion to buy a division of VeriSign Inc. that sells security technology to websites. The \$1.28 billion cash deal - the third encryption-related purchase for Symantec in three weeks, would seem to be a natural extension of its desktop and server security offerings.





## ***Chipmakers Face First Fine Over Price Fixing***

***By Suparna Sen, Smartcard & Identity News***



***Suparna Sen***

The European Union fined 9 chipmakers who were found guilty of illegally fixing prices of the DRAMS chips or dynamic random access memory. The fines could be the first of many to come. The companies - Samsung, Hynix, Infineon, NEC, Hitachi, Mitsubishi, Toshiba, Elpida and Nanya are set to pay a record-breaking total of £283.1m (331m euros, \$404.2m) for operating a cartel.

Samsung received the biggest single fine of 146m euros. The second in the league is Germany's Infineon<sup>1</sup> who had to shell off 57m euros. However, all the fines were reduced by 10% since the companies co-operated with the investigators. As per July 2008, the European Commission introduced a new settlement procedure which allows companies to receive a 10% reduction in fines if they admit to taking part in a cartel. Receiving a 10% cut in penalties in return for admitting involvement in price fixing scam is first in the history of a cartel case.

Going back, on 21st October 2008, European Union antitrust officials carried out surprise inspections at the premises of several chip manufacturers in different member states. Officers went to STMicroelectronics, Infineon Technologies, NXP and Renesas Technology as part of their unannounced checks. EU had prior knowledge that the companies concerned may have violated European Commission treaty rules prohibiting practices such as price fixing, customer allocation and the exchange of commercially sensitive information.

In the year 2002, the United States Department of Justice, under the Sherman Antitrust Act<sup>2</sup> began a probe into the activities of DRAM manufacturers. US computer makers Dell and Gateway raised their voices against over-rated DRAM pricing that was causing them lost profits and hindering their effectiveness in the world chip market.

In December 2003, the Department charged Alfred P. Censullo, a Regional Sales Manager for Micron Technology Inc., with obstruction of justice in violation of 18 U.S.C. § 1503. Censullo pleaded guilty to the charge and admitted to having withheld and altered documents responsive to a grand jury subpoena served on Micron in June 2002.

On December 2, 2004, Infineon also pled guilty. Four biggies of this popular German based memory vendor were arrested for involvement in international dram price-fixing conspiracy. Each of the executives had to pay \$250,000 criminal fine and serve prison terms ranging from four to six months. The Korean company, Hynix agreed to plead guilty to price fixing and likewise rewarded a reduced fine of \$185 million.

In October 2005, three Samsung executives - Sun Woo Lee, Yeongho Kang, and Young Woo Lee were also charged of cartel involvement and they were fined \$250,000 each in addition to serving seven to eight months in a US prison.

The settlement discussions started during 2009 only after the chip companies agreed on their infringement of EU laws. The end of this ongoing cartel investigation maybe coming to a close when the EU finally issued fines this month on the 19th May.

According to Commission Vice President and Competition Commissioner Joaquín Almunia, "This first settlement decision is another milestone in the Commission's anti-cartel enforcement. By acknowledging their participation in a cartel the companies have allowed the Commission to bring this long-running investigation to a close and to free up resources to investigate other suspected cartels. As the procedure is applied to new cases it is expected to speed up investigations significantly".

A new settlement procedure has allowed the Commission to settle this case in the simpler manner, with an objective to reduce the length of administrative proceedings. Of course, quick clearance of cartel cases is good for both consumers and taxpayers, as it trims down investigative costs. It also acts as a blessing for the antitrust enforcement, since it provides room to tackle other suspected cases.

<sup>1</sup> Except Infineon Technologies of Germany, all the other companies are non-European. But since they sell their products in the European Economic Area (EEA) they are abide by the EU's cartel ban law.

<sup>2</sup> The Sherman Antitrust Act, passed in 1890, has given power to the US Federal government to investigate and pursue trusts, companies and organisations suspected of violating the Act, by engaging in cartel.





## World News In Brief

### **Inside Contactless shipping 200 Million MicroPass Units**

Inside Contactless, a provider of open-standard contactless chip technologies announced that shipments of its MicroPass intelligent payment platform have surpassed the 200 million-unit mark, with production volume doubling in the 18 months since reaching 100 million units in November 2008.

Since its introduction at Cartes 2005 in Paris, the MicroPass platform has been regarded as the gold standard for contactless payments. MicroPass is available from all bankcard brand certified manufacturers in North America and now powers more contactless bankcards than any other core technology available in the market.

### **Panasonic releases Mobile Identity Checking Solution**

The new identity checking solution from Panasonic, the Person Identification Mini Dock (PIMD), was introduced into the border control and security market as a comprehensive policing solution. The Toughbook CF-U1 PIMD includes an optical character recognition (OCR) and contactless smart card reader as well as fingerprint scanner that connects to the corresponding mobile device. The PIMD is marketed toward the border control market, specifically the security personnel on the move who are required to constantly check identities. Its mobile capabilities include the components of DESKO, Dermalog and HID Global. The PIMD is said to be released officially for use in September 2010.

### **Comviva bags Awards for Virtual SIM Solution**

Comviva, the Gurgaon (an Indian city)-based provider of value added services to operators, announced that it has bagged two awards at the World Vendor Awards 2010 held at London. While the Best Outsourcing Initiative award was received for its managed VAS offering, the company won the Best Software Solution award for its virtual SIM solution.

### **First Indian Bank to issue EMV Credit Cards**

HDFC Bank has become one of the first Indian banks to supply credit cards compliant with the global EMV standard to its premium-segment customers nationwide. The 500,000 smart cards for the commercial launch phase that will run until

March 2011 are being supplied by the Indian subsidiary of security technology specialists Giesecke & Devrient (G&D). This initiative is said to significantly boost the Indian subcontinent's migration to EMV, from standard magnetic stripe formats to chip-based smart cards. HDFC Bank has already prepared a considerable amount of its deployed POS terminals to accept EMV smart cards in India.

### **Sagem Sécurité renamed Morpho**

Sagem Sécurité (Safran group) has changed its name to "Morpho". This new name reflects the company's dynamic performance and objective of consolidating all security businesses within the Safran group under a single name.

The new name embodies the company's core values, namely innovation as the basis of trust and technological excellence dedicated to its customers. The new identity will be gradually deployed across the company's many subsidiaries operating worldwide. Sagem Orga will also have the brand-name Morpho.

### **Borders broken by Octopus Dual Card**

The Octopus Company has set a December launch for a new smart card for use in both Hong Kong and Shenzhen Tong networks. The cutting-edge card integrates the functions of both smart cards but works in separate accounts for Hong Kong dollar and Yuan. The card will contain no personal information like names of cardholders, said Octopus chief executive director Prudence Chan Bik-wah. The Octopus Company said talks are still underway with Shenzhen Tong on card repairs and deposit amounts.

### **Myki Fails Yet Another Test!**

The \$1.35 billion Myki (contactless smartcard ticketing system introduced on public transport in Victoria, Australia) has once again failed a test, forcing its operators to manually adjust the accounts of nearly 90,000 senior cardholders.

Staff at the firm making Myki has had to manually add one cent to 87,261 cards so that they can be used on Sundays, when seniors are entitled to free travel. The Myki system requires all users, even those getting a free ride, to have a positive balance on their card.



## *Man, Machine and Advanced ID Credentials: Why Layering Human and Electronic Authentication Capabilities Provides Optimum Security in ID Credential Programs*

*By Stephen Price-Francis, Vice President of Marketing, LaserCard Corporation*



*Stephen Price-Francis*

Hope it should not be a strategy when it comes to identification systems, especially those employed for sensitive areas such as border control or access to secure facilities. And yet, some seemingly failsafe technologies turn out, on closer examination, to supply only a partial solution.

For example, electronic readers offer highly effective methods of authenticating and cross-referencing credentials, so surely machine-driven authentication is the wave of the future for ID programs?

True, but also not true. No matter how advanced the technology in a reader, database or credential, real life practices get in the way. The authentication method most commonly used to examine credentials is the human eye. ID documents are inspected by people, rather than by electronic readers more than 95% of the time, whether at borders, police checkpoints, airport security or building entrances.

Furthermore, readers are not as yet standardized to work with all ID technologies, but there is a high degree of variability in the selection and implementation of machine-readable technologies by governments and agencies. Take chips as an example, whatever the type – contact chip, contactless chip, a hybrid of both, or RFID: they are all in use, but there is no initiative – more importantly, there is no central budget - to place multi-functional readers at key points where they might be needed, such as Departments of Motor Vehicles, airports, or at the border.

While the attention of the ID credential industry frequently focuses on which machine-readable technology to select, we often lose sight of a fundamental reality – automatic ID readers are not always available or functional. Machine-readable credential programs encounter more stumbling blocks than program managers and their suppliers ever anticipate. Furthermore, readers tend to be very expensive. For this reason, they are usually deployed at the last possible phase of any ID project, and then only in a fraction of checkpoints.

The effectiveness of an ID credential is not just a function of its sophistication, but is dependent on its ability to be used in a variety of real life situations. Any credential authentication system based purely on electronic readers is in danger of being unusable for at least some of its life.

### **Biometrics: the panacea?**

If readers are not the answer, it might appear that a credential containing a securely stored biometric using any of the available secure storage technologies is the solution to document fraud. Moreover, there would be little need for additional security features on such a document. Perhaps, if a document reader checked every credential that contained a biometric and a live “one to one” verification was conducted then that might be the case. As it is, however, biometrics alone is not the silver bullet, although they play an important role in improving the security of a credential.

The International Civil Aviation Organization (ICAO) has established standards for biometrics in documents used for international travel that are accepted by the more than 190 ICAO-participating States and are intended to facilitate global interoperability. ICAO chose facial recognition as the mandatory biometric for machine readable travel documents, with fingerprints and iris as approved optional biometrics. In documents used for international travel there is also an ICAO standard machine readable zone containing the biographical and document details that can be “swiped” or “read” and checked against watch list databases.

ICAO, however, has never considered biometrics as the panacea for identity verification, but simply as an additional security measure that complements existing secured image and biographical data held in credentials. Additionally, there is serious concern that, because these new secure biometric documents are now in widespread circulation, some examining officers may develop a false sense of security when examining them. It is precisely because these documents are deemed so secure and reliable that they may be accepted at face value without being closely examined. Therefore, although the “biometric” credential is a more secure document, if it is not read and doesn't have front line verifiable features it maybe actually be less secure than non-biometric documents.





Experts agree there is no absolutely perfect biometric system. Each has its own strengths, weaknesses, and vulnerabilities. However, using truly transportable biometrics on a high data capacity, counterfeit-resistant, secure identification card will lead to the creation and implementation of the ‘trusted identity’ card.

This latter is the approach used in the optical media-based Costa Rica Foreign Resident Card program, where the overriding objective was to develop the most counterfeit-resistant document possible while implementing machine-readable biometric elements, tamperproof data storage and interoperability with the U.S. Green Card program.

The most effective approach to using biometrics requires an integrated approach combining visual and digital verification of identity based on biometric data. Such an approach would include implementing more than one type of biometric; providing storage capacity on the card to enable the addition of new data; assuring secure off-line verification ability; and providing the ability to select the appropriate biometric depending on the application.

### At-a-glance authentication

Given the prevalence of human, rather than machine-read, inspections, usable ID credentials require strong counterfeit resistance to enable confident authentication, and distinctive visual security features for validation without the aid of tools or devices. A key element is consistency and quality of manufacture - if inspection agents are accustomed to seeing variations, it becomes more difficult to detect fraudulent documents with the human eye.

One of the most effective security technologies, delivering fully on this requirement, is optical security media, a stripe of optical recording medium encapsulated into a laminated polycarbonate card structure. Digital data is encoded into the optical stripe using a laser beam (somewhat analogous to the writing of data onto a CD-R) and, since the process is destructive, the data cannot be fraudulently altered or erased, making it literally tamperproof. The optical security media is frequently combined with contact or contactless chips and RFID technology to deliver advanced functionality as well as security, as in the new U.S. Green Card. Introduced in May this year, this credential combines RFID antennae, optical security media, biometrics and a host of visual authentication as well as covert verification features, delivering optimal functionality and security in a single card.

The optical security media exhibits very distinctive visual characteristics which are extremely difficult to simulate. Add to this the ability to permanently mark the optical stripe with very high resolution images (up to 25,000 dots per inch) and security printing features, such as guilloche patterns, plus binary optical variable devices, and we now have a strong additional layer of tamper and counterfeit resistance. Experience shows that relatively inexpert “examiners” can make a sound judgment about the card’s authenticity based on these characteristics.

### Unalterable images

Among the most popular forms of fraudulent ID tampering is image substitution, despite advances in preventive technologies. One way of countering such attempts is to laser “etch” the cardholder’s facial portrait into the optical stripe itself. The result is a feature called “Personalized Embedded Hologram HDTM, a high resolution, high contrast, photo-like image which cannot be altered. The combination of inherent visual characteristics, high resolution security images and the Personalized Embedded Hologram builds a third, blended layer of tamper and counterfeit resistance and gives optical memory what one industry expert has called ‘self referential authentication’.





This forgery countermeasure is used in the Saudi Arabia National ID Card, among many others, and serves to support visual inspection of the card in a wide variety of settings where readers are unlikely to be present.

Layered technologies and multiple authentication methods provide a real world solution where human eyes can be deployed as effectively as machine readers to verify a credential. Combined technologies plus the capability of confident visual identity checking will deliver a robust, effective and secure ID program that is highly functional in almost all situations where ID authentication is required. This approach offers a strong and effective transition from today's reality of visual inspection to the world of tomorrow based on a widely available e-id infrastructure delivering convenience, interoperability, security, better service levels and ID fraud protection.

## World News In Brief

### 2010 Élan Award Winners Announced at ICMA's 20th Anniversary

The International Card Manufacturers Association (ICMA) announced the winners of its annual Élan Awards for Card Manufacturing Excellence at a 20th anniversary gala celebration and awards ceremony on May 4, 2010 as part of its four day Card Manufacturing and Personalization EXPO at the Camelback Inn, a JW Marriott Resort in Scottsdale, Arizona.

The ICMA Élan Awards honour card manufacturers and vendors for their excellent card design and innovative products. Past recipients include leading card manufacturers from around the globe. Entries were judged solely on the card's features as entries were not identified by company. Winners and finalists were chosen in each of the following categories:

To know more on this, visit <http://www.icma.com/>

### Weneo Pass now available for easy Online Reloading of Transport Tickets

Semitag has selected the Weneo Pass from Neowave to offer a secure and user-friendly solution for transportation. Now TAG customers just have to connect their Weneo Pass on the USB port of their computer. Within a few clicks, they can purchase their transport tickets and reload them on their USB key format Weneo Pass, at home or from any location with an internet access point, all round the clock. Using the Weneo Pass to travel on TAG public transportation network is as easy as using a contactless card.

### Comtech receives \$26.3 Million Movement Tracking System Orders

Comtech Telecommunications Corp. announced that its Maryland-based subsidiary, Comtech Mobile Datacom Corporation, received orders totalling \$26.3 million under its Movement Tracking System

or MTS contract with the U.S. Army. Total orders received to date against the \$672.4 million MTS contract increased to \$621.3 million. This order follows Comtech's May 5, 2010 announcement that it received a \$67.3 million ceiling increase to its MTS contract.

### iPhone to feature Contactless Payment

iPhone users will soon be able to use their handsets for contactless payment. Visa and DeviceFidelity have developed a protective iPhone case that will allow users to pay for goods and services "by simply waving their iPhone in front of a contactless payment terminal".

### Ice Cream with RFID Chips!

Izzy's Ice Cream Cafe in St. Paul, Minn has started using RFID technology to give customers real-time updates on all the available flavours. Each time one tub of ice cream is replaced with a new flavour, an employee swaps the RFID tag in front of the tub with the one corresponding to the new flavour. RFID readers in the dipping cabinet scan the tags 22 times every second and send the information to a system which then projects a series of dots representing different flavours onto a wall in the store. Customers glance at the coloured dots projected on the wall, or on the plasma TV behind the counter, to find out what flavours the store is serving.

### MasterCard to Launch New Open API Developer Portal

MasterCard Worldwide announced that later this year it will release Open Application Programming Interfaces (Open APIs) for third-party and independent software developers around the world. By opening up previously proprietary payments and data services, developers will be able to create a new wave of e-commerce and mobile payment applications. The new Open API program is the first initiative from the newly created MasterCard Labs.



# *Sagem Security announce launch of the latest in identification: The Multi-Purpose Card, IDEal Citiz*

*By Tom Tainton, Smartcard & Identity News*

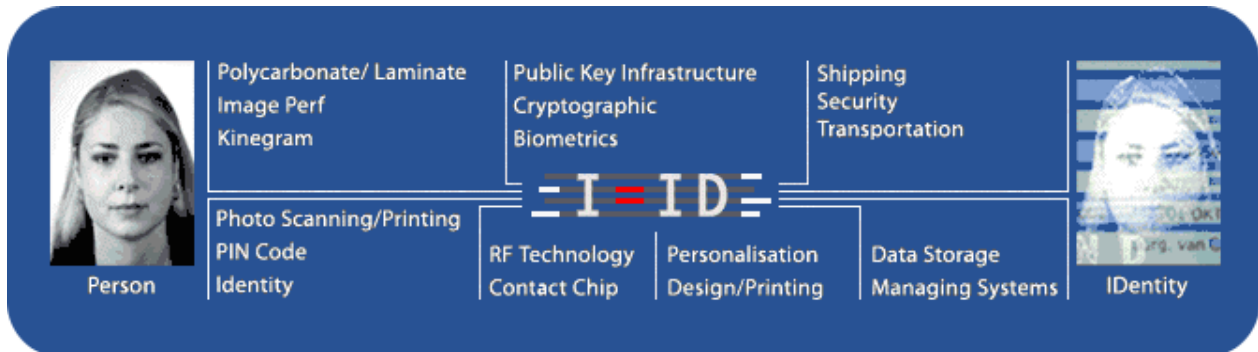


*Tom Tainton*

In today's shady world of ID fraud and online theft, there's a increasing demand for higher security and stringent identity controls. Government agencies are striving to improve their services for citizens, demanding fast and efficient products which are capable of meeting a series of requirements including e-services, digital signature and travel applications.

Now, they need not look any further. Sagem Security, one of the world's leading suppliers of identity systems, has launched an all-in-one solution that addresses the full range of government ID needs. The IDEal Citiz is the first multi-Match On Card product to incorporate facial, iris and fingerprint recognition technology – multi-biometry that has significant benefits to the end-user. The card can play a variety of roles: a healthcare card, a driving license, a residency permit and even a qualified signature.

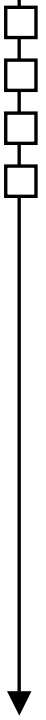
The combination of all three recognition technologies enhances the matching accuracy and provides an increased level of reliability. However, holder privacy remains of utmost importance, and so all biometric references remain secret and exclusively on the card. Philippe Bertiaux, Sagem's Vice President of ID products, said: "This is the latest product that we have developed for the ID market. IDEal Citiz also functions in the identity and driving license markets. We're confident that we have developed a product which is state of the art in terms of specification, security and performance. Essentially, it's all the elements required for the ID market in one product."



IDEal Citiz boasts a multitude of standards including ICAO/EAC standards which provide citizen identification, transforming the card into a travel document. Bertiaux describes it as a 'secure performance, open product which complies with the required European standards.' Extended Access Control technology is a vital component in epassport solutions, which allows storage of fingerprint biometrics on microprocessor. The product also draws from the smartcard expertise of sister company Sagem Orga, utilizing MINEX II (Minutia Interoperability Exchange Test) certification to enable strong multi-biometric authentication. The ID document is also fully interoperable with IAS ECC ecosystems, the international standard that's defined by the French smartcard association, Gixel.

Furthermore, it provides customers with an open product which can be personalized to the user, thanks to a standard published by Global Platform. In fact, it's so flexible that applets can be loaded without jeopardizing the product's security certification. Bertiaux said: "We've taken a lot of effort to ensure the product is efficient in terms of performance. For example, in the e-passport application we can perform full transactions in fewer than three seconds. That's the quickest application that you will find in the market."

On the 27<sup>th</sup> May Sagem Sécurité (Safran group) announced it is changing its name to "Morpho". The new name change come in an effort to consolidate all of security businesses within the Safran group under a single name.





## ***Prevention is better than cure: how banks can protect their customers against the card fraud threat during big sporting events***

***By Michelle Weatherhead, ACI Worldwide Fraud Consultancy***



***Michelle Weatherhead***

In preparation for this year's world cup in South Africa, the country is putting extra measures in place to protect tourists from the anticipated rise in criminal activity. The government is even introducing a fast-track legal system that will enable visitors to give evidence while still in the country following a crime, so that foreigners' cases - whether they are victims or perpetrators - will receive priority.

From a banking point of view, financial institutions are particularly concerned about the increased potential for card fraud during the world cup. Card fraud is already a problem in South Africa. According to the South African Banking Risk Information Centre, counterfeit card fraud was the most costly type of fraud in 2009, increasing by 22 per cent to R144 million<sup>1</sup>. With the influx of foreign visitors to South African soil over the coming weeks, banks in both South Africa and in the consumers' home countries will have to be even more vigilant than usual in order to effectively protect their customers from card fraud. There are, however, some simple steps that banks can take to protect their customers from fraud at this time of heightened risk.

### **Protecting consumers from card fraud**

Fighting fraud is a complex and ongoing challenge for banks and during the world cup they need to find the right balance between adequately preventing fraud and not blocking transactions incorrectly which can greatly inconvenience customers.

There are a number of different techniques that banks can use to ensure that they accurately identify fraud. The first is very straightforward – banks should encourage their customers to tell them if they are travelling overseas and make sure they have a way of incorporating this information into the fraud detection rules. This will help ensure that the bank is less likely to falsely stop a genuine transaction. In addition, banks should educate their customers about basic card security, including common pitfalls, so that they can endeavour to prevent fraud as soon as possible.

In the case of the world cup in South Africa, banks are likely to have a concentrated number of customers in one region who will be specifically targeted by 'professional' criminals. In this instance, banks must train their analysts on fraud trends in that country or location in advance, and make sure they can hit the ground running once the cards start being used.

It is particularly important that card transactions are monitored in real-time in order to identify fraudulent attempts at the earliest possible opportunity to prevent fraud losses from taking place. This real-time monitoring should use everything that the bank knows about the customer and their usual spending patterns, combined with a hot list of known fraud identifiers such as a risky terminal or a fraudulent sequence of events, to flag up suspicious transactions. Banks should also share this information with their peers, to identify fraud trends and enable them to respond as quickly as possible.

Finally, banks should implement bi-directional phone alerting, such as using SMS, to enable them to send alerts or calls to individuals' mobile phones whenever a transaction occurs that is flagged as suspicious, or is outside pre-defined parameters. Once the customer receives the message, the bank can respond to block the card immediately, if it is fraudulent.

While banks may already have some or all of these fraud preventative measures in place, they should also be taking more simple measures such as planning ahead by looking at the dates and venues where the football games are taking place. That way they can anticipate where and when transaction levels, and therefore the potential for fraud, are going to increase.

At large events such as the world cup, travellers will be naturally more susceptible to fraud but there are several ways banks can put their own minds and those of their customers at rest. A combination of customer education, communication and comprehensive real-time analysis techniques will help banks do their utmost to protect their customers and ensure card fraud doesn't ruin what should otherwise be a very memorable occasion for many people.

<sup>1</sup> <http://www.southafrica.info/news/business/464857.htm>





## World News In Brief

### One Card to open all doors of Ottawa

By the year 2012, Ottawa residents should be able to buy their morning coffee, hop on the bus, borrow library books, and go for a skate in a community arena, all using the same pre-paid smart card, says College Councillor Rick Chiarelli.

The idea for a debit card that covers all city services has been discussed in Ottawa for a decade, and finally the committee has wrested control of the issue by means of a motion at council that puts the smart card implementation into the hands of the IT committee. Now the committee is moving forward with a proposal that it plans to have ready in time for approval in next year's budget.

The O-cards will come with many features, for example, people will be able to load money onto their cards from their home computers. And the cards will be compatible with the city's new pay-and-display parking terminals.

### Lockheed Martin to work on FBI's Second Phase Next Generation Identification Program

The Lockheed Martin (LMT) -led Next Generation Identification (NGI) team is beginning to fully develop and deploy a new NGI system capability that transforms how law enforcement officials search an FBI wanted person's database. Development efforts began after a successful Critical Design Review (CDR) for the system's second phase, also known as Increment 2: Repository for Individuals of Special Concern (RISC).

The RISC fingerprint database, which is managed by the FBI's Criminal Justice Information Services (CJIS) Division, includes Wanted Persons, Known or Appropriately Suspected Terrorists, Sex Offenders Registry subjects, and other persons of special interest.

### Wal-Mart to Support Smartcard Payments in U.S. Stores

According to a new report, Wal-Mart is planning to make every last one of their payment terminals in the U.S. compliant with "a smartcard-based credit card technology that is widely used around the world but isn't common in the U.S".

The plans were unveiled at a smartcard conference held last week, with Storefront Backtalk quoting Jamie Henry, Wal-Mart's director of payment

services, as saying that the retailer was "working on making all payment terminals in its domestic stores chip-and-PIN-capable".

According to the US giant, signature-based credit card processing (which they use now) has become "a waste of time" and hence they want to shift to this new technology that is already in wide use in Europe and Japan.

### HCL Infosystems to deploy India's First Smart Card based PDS Solution

HCL Infosystems India's premier hardware services and ICT system integration company has announced that it bagged an order to implement India's first smart card based solutions for Public Distribution System (PDS) in the union territory of Chandigarh. As part of the project, smart card based ration cards will be distributed to the families living below poverty line in the region. These smart cards will capture all biometric, tax, demographic and personal information details, enabling authorities to ensure proper distribution of food rationing and other benefits.

### £30m Oyster Card Left Unused

Nearly £30million pre-pay Oyster cards are lying unused, transport chiefs have revealed. These cards are lost, broken, stolen or simply no longer needed by tourists who have left the country. Around 16.5million cards sat idle from April 2009 to last month. The average remaining on each was £1.80.

Last year alone, 31,000 Oyster cards were issued and topped up but were never used, even though they held £246,000 worth of travel. Around seven million are now in use and pay for 57million trips a week on Tubes, buses and trains.

Smartcard Group managing director David Everett said he was not surprised by the £29.85million left unspent on Oyster cards in the past year. According to him, people do not realise they are likely to have unspent funds. "People lose cards, don't spend them or put them away — and of course the person issuing them effectively benefits," he said.





## **RFI: The new Integrated Circuit Card Security Evaluation Laboratory for Chip Card Payment Products**

RFI Global Services Ltd announced the formal extension of its security evaluation capabilities, and is pleased to formalise EMVCo SEWG accreditation. This will enable RFI to formally become accredited for Visa Chip Security Program (VCSP) and MasterCard Compliance Assessment and Security Testing (CAST) security evaluation services for products supporting Visa and MasterCard applications.

## **Borer introduces Combined DESFire Smartcard and Fingerprint Reader**

Borer Data Systems (<http://www.borer.co.uk/>) is demonstrating a combined biometric and smartcard solution, which it says is "the latest in advanced access control". Biometric details are only held on the card, ensuring that cardholders retain possession of their personal data at all times. On enrollment, cardholder data together with PIN, biometric template(s) and a digital image are written directly to a DESFire smartcard.

Up to 16 separate encrypted files containing cardholder identity, PIN, biometric template(s), digital photograph, qualifications, and the like can be written to the card's memory. The cardholder's details, including biometric template, are protected using 3DES or AES encryption. The card reader supports three factor authentication using combinations of identification including card, card + PIN, card + biometric, card + PIN + biometric.

## **Briton Cut Down SIM to Micro Size!**

Got a shiny new 3G gadget with a microSIM slot, but no carriers is willing to give you a tiny SIM to put in it? Don't worry. Brit iPad owner John Benson took a local (and normal-sized) Vodafone SIM and cut it down to size using nothing but a pair of scissors to fit in his iPad.

It turns out that the standard SIM is internally no different than the new micro versions. The extra size is just plastic, and if you cut away the right parts you are left with a fully-functional, iPad-compatible card. John only used the knife to press scoring lines into the card to make his scissoring easier and more accurate. He used an existing microSIM as a template (that comes with an iPad). To make the iPad work with a non-AT&T account, John accessed the network settings, input the correct Vodafone APN (in the UK it is just "internet") and he was off.

## **Symantec rolls out Smartphone Security**

Symantec's Norton division is driving the Norton Everywhere initiative, aimed at bringing security protection and cloud-storage access to the Google Android and Apple iPhone smartphones, reports San Francisco Chronicle.

The free application, Norton Connect, enables users to access data stored in Symantec's cloud-based storage service. The Norton Connect applications are expected to be available in June this year from the iPhone and Android app stores.

## **All 10 Fingerprints Mandatory for UID**

The Cabinet Committee on Unique Identification Authority of India gave its in-principle clearance to guidelines for identifying individuals in the UID database by using all 10 fingerprints and a photo of the person as well as of the iris to prevent duplicate IDs being issued and establishing a person was just who he or she claimed to be.

In a billion-plus population, a mix of biometric and photographic record is considered necessary to ensure fidelity of information collected by the project. With the UID intended to help identify beneficiaries of welfare schemes, children aged between 5 and 15 will be included in view of the ambitious right to education.

## **Google adds SSL Encryption to its Search**

Internet search giant, Google has said that it has added Secure Sockets Layer (SSL) encryption to its popular search engine. As a result when the users search through the main URL, the SSL creates an encrypted connection between the browser and Google to protect users' search terms and search results from being seized by external users. It also protects the user data from Google's own Street View cars.

SSL is a security protocol used by banking and e-commerce sites for their users for protecting their transfer of information between the internet and their computer. It offers more security when compared to pages that encrypt only log-in pages and credit card data.





## China urges Tough Internet Laws targeting 'Overseas' Forces

Wang Chen, head of the Information Office of the State Council, urged the National People's Congress to adopt an "Internet Administration Law," to better define illegal activity on the internet, while also better defining rules on the administration of the mobile phone industry.

It is believed the measures would help enhance an ongoing crackdown on online pornography, gambling and fraud in China.

## Latest Version of Visa payWave Test Tool Released

Collis with Visa Europe announce the release of a new version of Visa payWave Test Tool (VpTT). The Visa payWave Test Tool (Version 2.0) is a portable and officially confirmed test tool that has been upgraded to enhance current functionality and includes the implementation of the most recent Visa Contactless Payment System functionality (VCPS 2.1). Included in the new functionality are sections on Reader Dynamic Limits, Consumer Device CVM Processing and VCPS Version Processing. In addition to this, two new card profiles have also been introduced to address the type of cryptogram that is returned during a refund transaction.

## Obopay rolls out Mobile Money for Banks Program

US mobile payments company Obopay have launched Mobile Money for banks, a program set to allow the country's banks to deploy their own branded mobile money service.

Obopay's Mobile Money is designed to enable bank customers to make payments for their purchases, send money from their own bank account using a debit card, send money to family members for emergencies or regularly scheduled payments as well as perform account-to-account transfers, all from a mobile phone.

## Protegrity and Thales to protect Customer Sensitive Data

Protegrity USA, Inc. a leader in providing Data Security Management Solutions, announced a partnership with Thales, leading provider of information systems and communications security, to strengthen sensitive data protection specific to the protection of cardholder data and personally identifiable information.

Through this partnership, Protegrity has integrated the Protegrity Data Security Platform, one of the

broadest protection platforms in the market and the first to offer flexibility in data protection supporting encryption, tokenisation, format controlled encryption, and masking, with the Thales nShield product family of hardware security modules (HSMs).

## ID Cards Must in All Emirates

Ministry of Interior's decision to make the ID card mandatory for processing driving and vehicle licensing transactions is not for Abu Dhabi alone but for all emirates. Emirates Identity Authority (EIDA) has said that the authority has decided to set up a large fully equipped and serviced tent at the headquarters of the Drivers and Vehicle Licensing Directorate in Abu Dhabi to process ID card applications of clients whose licensing formalities will not be completed without the card. The ID card became mandatory from Sunday, 2nd May.

## Sagem Orga do Brasil to deliver CardInk

Sagem Orga do Brasil, the leading Latin American smart card manufacturer, has appointed Cryptomathic to deliver its data preparation solution, CardInk. The system will be integral to Sagem Orga do Brasil's issuance of EMV debit and credit cards.

CardInk is Cryptomathic's second generation EMV data preparation system for single and multiple application cards.

## Bell ID wins Contract with Saudi Arabian Bank

Bell ID, a Dutch provider of smart card management solutions, has won a contract from a Saudi Arabian bank for the provision of both central and instant issuing solutions of EMV cards.

Bell ID has said that its ANDiS software suite will offer a set of features to meet the bank's requirements, namely EMV data preparation, smart card and application management, central issuance and instant issuance of chip cards at branch locations. The offered solution will enable the personalisation of MULTOS chip-based SPAN debit cards at more than 100 issuance locations in Saudi Arabia and various locations in Dubai and Pakistan.





# *MasterCard Continues to Displace Cash*

## *By Suparna Sen, Smartcard & Identity News*



*Suparna Sen*

On 10th May MasterCard appointed Andrew Ong of Western Union to the position of 'Global Head of Global Person-to-Person (P2P) Payments. Andrew Ong's new role will be 'to be responsible for identifying and evaluating new P2P payment solutions that will continue to displace cash and cheque payments.'

It was in 2007 that MasterCard Worldwide along with State Bank of India (SBI) announced the launch of MasterCard MoneySend that allows consumers to send intra-country person-to-person money transfers using the ATMs. This month the MasterCard MoneySend programme has started in the United States.

MasterCard announced that with this new platform, MasterCard customers can now transfer money easily to their friends or colleagues in about one to two banking days. The receiver will get an instant online notification once the money is successfully sent.

To join the MasterCard's MoneySend service, you will need to have:

- A MasterCard or Maestro card
- Both the sender and receiver must have account in the bank that offers MoneySend facility
- You need to visit the banks nearest ATM to withdraw the money
- You will need to register for a MoneySend ID and PIN (For online usage)

To transfer money the sender will need to know the recipients bank account details and input them into a public ATM. Presumably one without a good memory would have to write this information down on paper for the initial or one-off payment to a recipient.

Another very vital point – in case you end up providing wrong information regarding your personal details, it is you who will be totally held responsible. I have yet to come across a single bank that verifies the information in real-time and assure the sender that the entered combination of account name and sort code indeed belongs to the concerned receiver.

Some participating banks may offer email notification and you must contact the participating banks to find out if this feature is implemented.

Using MasterCard MoneySend inevitably incurs fees, and MasterCard again asks you to contact your participating bank for information about costs.

However in spite of its limited features, for many people, MasterCard MoneySend happens to be a cheap and easy way to send money internationally. If you are looking for a bank account replacement card, don't go for MasterCard MoneySend Prepaid Card, but if you already have a bank account and simply want to send and receive money to friends and colleagues, this may be the system for you. The fees charged on Prepaid Card are also relatively low, including the fees for transferring money.

To conclude, whether you choose MasterCard's MoneySend or not, one thing is clear – the very person-to-person payment transfer is far from the simplicity of cash. You have to open account; have to have a debit/credit card, etc to enjoy transactions. Thus, the MoneySend programme is a tiny step towards displacing cash, and really only targeted towards foreign workers sending money back home on a regular basis.





# PREPAID2010

CONFERENCE & EXPO  
LONDON  
14-16 JUNE 2010

# Prepaid is in your hands

TRANSPORT

MOBILE

CONTACTLESS

DISTRIBUTION & LOAD

CORPORATE

PUBLIC SERVICES

VIRTUAL

GIFT CARDS

## Speakers at Prepaid 2010 include:

Peter Lewis, Head of Oyster, **TFL**

Nicola Kaye, SmartCard Programme Support Officer,  
**Bracknell Forest Council**

Allyson Lloyd, Corporate Catering Manager, **Croydon Council**

Marianne Lewis, Programme Manager, **Croydon Council**

Kieran Fitsall, Supplier Relationship Manager, **Westminster Council**

Daryl Wallace, Project Manager **Hillingdon Council**

Steve Pennant, Programme Lead, Connected London, **London Councils**

Kevin Farquharson, Director, **Smartran**

Richard, Poynder, Chairman, **Smartex**

A growing number of authorities are using smartcards to provide social benefits, healthcare, concessionary transport and cashless catering services. Prepaid 2010 brings together the operators, councils, banks, card associations and system integrators behind the latest innovations in multi application cards in the UK. This is your chance to find out how to reduce costs, increase revenues and improve standards of public services for your organisation.

Please quote PPAC when registering

Prepaid 2010 is free to all local authority members

w. [www.prepaid-conference.com](http://www.prepaid-conference.com)

t. +44 (0)20 7067 1831

Organised by

**CLARION**  
EVENTS