

### 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, Peter Tomlinson, Suparna Sen,  
Paul Tuner

**Photographic Images** - Nejrion -  
[Dreamstime.com](http://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*

Is it just me that gets confused? What I can't understand is standards, well what I mean is why do I need so many? Just take charging up your mobile phone they all look so different. Don't worry I've been told there is a new standard based on micro USB or is it mini USB? I do pride myself on having reasonably modern phones and I can assure you the charging pods are all different. The reason for the annoyance,

you know there is going to be one and that being that I took the wrong charger for my phone on holiday. They all look the same and the difference between mini and micro USB is for the electronics buffs amongst you. Why can't I have colour coded plugs, blue for mini and red for micro, well that's what my mother used to say about dresses anyway? Something about red for danger apparently.

Now it doesn't stop there because the joy carries on with memory cards, just about every device I have seems to have a different format for the memory card. It's hard to believe there are so many, I really don't know what they all are but my card reader boasts of being a 19 in 1 card reader, I'm not going to bother you with the names because I don't think I could tell one from the other. All I know is that when I take the memory card out of the camera I go round each slot in the reader until I find one that it fits. It sounds horrendous but does anybody do anything different?

Closer to home I have been totally bemused by mini and micro SIM cards. The other half impatient to the end clutching an iPhone 4 in one hand and an iPad in the other has entered the world of micro SIMs. Now we could all get bored about how many people ever used a full sized credit card for a phone SIM, I thought I was old enough but I certainly don't remember them. In fact a SIM card was a SIM card, who ever called them a mini SIM? But anyway we now have the micro SIM. And of course you can't change it from phone to phone or iPad to phone and all the other combinations you can think of unless they are all the latest models from Apple.

This may not be a problem you might think? Well the holiday was a technological extravaganza because the back fell off his iPhone 4. It looks like it never had the two bottom case screws inserted but according to O2 it's now a write off as uneconomical to repair. Can you believe that, 2 miniature screws or micro screws or what have you and they're more expensive to put in than the £430 O2 have demanded for a replacement phone? Apparently we're off to Maplins this weekend to buy some of these screws for a DIY repair. I hope there aren't too many standards involved here. I'd hate to think that two screws that look the same are totally different.

Anyway the fun didn't stop there, the Channel Islands (Jersey in our case) are interesting and recommended to all for a few days at least (I never realised the average rainfall is 16 days per month, it makes the UK seem positively dry) but the Island is devoid of Wi-Fi (except in St Helier but that's a permanent traffic jam) you really are dependent on your mobile broadband. There was a good 3G signal all round the Island but that doesn't help you when you can't carry your phone





around and apparently it's difficult to stick it together with sticky tape when you've only got a touch screen. So here we are, buy a disposable phone and pop the SIM card in it. I can still remember the look on the guys face in the mobile phone shop (only in St Helier of course) when he looked at the micro SIM, you would have thought it could only have come from Dr Who's Tardis. So you can't easily buy mobile phones that use a micro SIM and surprise number 2 was that if you have a UK pay as you go SIM you can't have cellular data in the Channel Islands. Apparently the islands are foreign territory although Wikipedia thinks they are a Crown protectorate. Apparently the only way you can have cellular data in foreign lands and the Channel Islands is to have a contract SIM – just make sure it's not a micro SIM unless you have a spare phone with a micro SIM socket. Perhaps we could have adaptors, a 19 in 1 do everything – just joking.

Don't forget, Paris strikes permitting that Cartes 2010 is just around the corner for 7th to 9th of December.

Patsy.

## Contents

### Regular Features

Lead Story – Mumbai's Oyster Card, a dismal failure. . . . .	1
Events Diary . . . . .	3
World News In Brief . . . . .	.5,8,10,11,12,14,16

### Industry Articles

Google Android apps found 'sharing data' . . . . .	6
ICO release UK's first code of practice on data sharing. . . . .	7
Surf the wave. Don't try to change the mighty ocean. . . . .	9
Verifone launches bid for rival Hypercom . . . . .	11
The Reality of Mobile Payments for the Consumer.. . . .	13
FBI begin world-wide arrests of cyber criminals . . . . .	15
Private Key Management: Best Practice Tips from the Real World . . . .	17

## Events Diary

### November 2010

- 1-4 Sixth Symposium on ICAO MRTDs, Biometrics and Security Standards, Montreal, Canada  
<http://www.icao.int/MRTDsymposium/2010/>
- 16-19 2010 Smart Cards in Government Conference, Washington DC -  
<http://www.smartcardalliance.org/pages/activities-next-conference>
- 16-18 ID World International Congress, Milan, Italy - <http://www.idworldonline.com/>
- 17-19 InfoSecurity Russia, Sokolniki, Moscow, Russia - <http://www.infosecurityrussia.ru/>
- 23-25 Cards & Payments India 2010, New Delhi, India -  
<http://www.terrapinn.com/2010/cardsindia/>

### December 2010

- 7-9 Cartes 2010, Paris, France - <http://www.cartes.com/>

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





## Mumbai Oyster Card, a dismal failure.... Continued from page 1

In lieu of the Go-Mumbai card's poor performance, the Railway Board has issued a letter to both the CR and WR to stop the card's operations by December 28, 2010. BEST have also stopped issuing monthly and quarterly Go-Mumbai cards.

The Go-Mumbai scheme operated as follows: the card (a contactless smartcard) is initially purchased for 37 Indian rupees (53 pence GBP). Passengers flash their card against the station readers. The readers automatically deduct the maximum travel fare applicable from that station, and also records on the card the boarding station. When reaching the destination, you need to flash your card again to exit, and in case of any excess fare deducted at the boarding station, it will get refunded back to your card. (Pic? [http://www.kaizenengg.com/goc\\_auto.htm](http://www.kaizenengg.com/goc_auto.htm))

When you are low on credit you could top-up your Go-Mumbai card with further amounts (minimum Rs.50) as and when required.

However, in spite of having many similarities with the Oyster Card of London, the Go Mumbai Card failed to gain success.

One of the main causes behind the "Go Mumbai" smartcard's failure is that Kaizen Automation Limited, the company that provided Smartcard & equipment, failed to supply enough of the hand-held devices used by ticket inspectors to check the card's validity.

Another reason for the cards failure to live up to expectations was the high number of faulty gate readers. According to Manoj Nair's published complaint dated 26-April 2010 on "The Indian Express" portal, people need to move around the new Mumbai stations searching for the machines and in case they get hold of it, most of the times they tend to be not functioning and having a 'Out of Order' board.

As per the news published on 5 October, 2010, the BEST spokesperson NA Walawalkar said, "There was a problem of machines. A lot of them were plagued with technical problems". Hence, unless the technical glitches are addressed and the existing defected readers are repaired, the problem of using "Go Mumbai" smartcards will continue to grow.

Unlike in Oyster cards, where student concessions are given under various age groups with different savings options on Travelcards and bus and tram passes, in BEST buses, concession rate are available for senior citizens only, excluding students. In case of railways, no concessions are given (To note: majority of Mumbaikars travel in trains). Hence what happens is that a good number of students don't buy Go Mumbai card and instead use paper tickets instead.

The Oyster pay-as-you-go cards have reduced considerable travel costs for many Londoners. Whereas there are some serious doubts as to how far the Go Mumbai Smartcards have gained success in reducing travel costs for the Mumbai commuters!

Following BEST's Go-Mumbai card's unsatisfactory services, the top Central urban development officials are undeterred and are now planning for a more ambitious scheme of a new common mobility card in place of the Go-Mumbai card. The new card can be used in practically all modes of city transport such as buses, suburban trains, underground metro, monorail, fleet taxis, and also in autos and toll plazas.

Following The National Urban Transport Policy<sup>1</sup>, the common mobility card will act as a single ticketing card for boarding on a national, state or city transport, anywhere in India. For the card's flawless use across the country, there will be national standard specifications so that various systems can be integrated seamlessly, according to SK Lohia, officer on special duty (urban transport), in the central ministry of urban development.

Suparna Sen, Smartcard & Identity News

<sup>1</sup> *The National Urban Transport Policy (NUTP) was made in 2006 to integrate land use and transport planning in Indian cities, and to bring about all-inclusive improvements in urban infrastructure.*



## World News In Brief

### **Morpho Announced World's First Biometric-Based Signature Smart Card**

Morpho (Safran group) has announced the world's first EAL5+ Common Criteria certified biometric-based signature smart card at the 11th International Common Criteria Conference in Turkey.

With the help of Morpho's IDEal Citiz™ smart card, people will be able to use their fingers to sign electronic documents with the same legally binding status as with a handwritten signature. This makes it the first "Secure Signature Creation Device" as required by the 1999/93/EC Directive of the European Parliament and the Council, on fingerprint biometrics for strong user authentication in legal digital signatures. IDEal Citiz meets identification needs in both government and private markets.

### **Visa Launches First Canadian Debit SmartCard**

Visa Canada announced the launch of the company's first debit cards in the Canadian marketplace. CIBC is the first Canadian issuer to offer Visa Debit through its CIBC Advantage Card, which is currently available in all its branches. In Canada, the CIBC Advantage Card will provide Canadian consumers with the ability to shop widely online, by phone or mail and in more than 200 countries and territories around the world using funds directly from their bank accounts.

Debit cardholders will continue to be able to withdraw cash from automated banking machines (ABMs) and purchase goods and services at a Canadian merchant with funds directly from their bank account. At the register, the CIBC Advantage Card will be processed through Interac, Canada's existing debit network.

### **Gemalto and VeriFone Become Partners**

VeriFone Systems, Inc. and Gemalto, the world leader in digital security, announced a comprehensive strategic partnership to jointly pursue new chip card solutions based on the global EMV payment standard. The two companies are also in exclusive discussions for VeriFone to acquire Gemalto's point of sale (POS) solutions business.

Gemalto is also the preferred supplier of Machine-to-Machine (M2M) wireless modules and related solutions for VeriFone payment systems.

### **Ceelox Issued its First Patent**

Ceelox, Inc. announced that it was issued its first patent from the U.S. Patent Office. The patent, U.S. Patent Number 7,818,395 entitled "Method and Apparatus for Interfacing with a Restricted Access Computer System," provides the ability for a data storage component, such as an external flash drive, to interface with a computer without loading additional software or requiring administrative rights on the computer.

The issued patent is utilised within the Ceelox Vault product, which offers a File Manager-like interface with shortcut links to My Documents and Desktop and allows for the automated synchronisation of files located on the portable device. Vaults can be created by multiple users who may share a device, each with unique biometric access to the stored data. Encryption of the data insures that even if the drive is removed from the laptop or desktop, the data cannot be accessed except by the owner of the vault.

### **ViVOtech's NFC Technology to be used in the First NFC Add-On Mobile Payment Service in Middle East**

ViVOtech, the leader in Near Field Communication (NFC) and contactless payment systems, joined Teletech Middle East, a UAE based Services Provider Company, in providing end-to-end NFC Payment Infrastructure including Trusted Services Manager (TSM) and Over-The-Air (OTA) provisioning platform and NFC mobile payment wallet

Teletech Middle East will use the company's TSM and OTA provisioning platform and NFC mobile payment wallet software in its first NFC Add-On mobile payment service that is scheduled to commence before the end of 2010.



## *Google Android apps found 'sharing data'*

*By Tom Tainton, Smartcard & Identity News*



*Tom Tainton*

A team of American researchers have discovered that some of Google Android's apps are gathering and sharing data with third parties without telling users how the information is being used.

The group of computer scientists from Intel Labs, Penn State and Duke University studied 30 out of the 358 most popular Android apps that ask for permission to get location, camera and audio data.

The selected apps included The Weather Channel, Yellow Pages, BBC News Live Stream, Myspace, shopping app ixMAT and games such as Solitaire and Hearts.

The study used specially designed software called TaintDroid to log the information collected and how it was used. The technology found that half of the featured apps passed on location information, some sending updates every thirty seconds or even when the application wasn't being used. Seven of the apps shared specific data to the mobile phone device, including phone numbers, SIM card serial numbers and IMEI (International Mobile Equipment Identity) numbers.

The research concluded: "Two thirds of the applications in our study exhibit suspicious handling of sensitive data. Our findings demonstrate the effectiveness and value of enhancing smartphone platforms with monitoring tools such as TaintDroid."

How are Android app developers able to get away with these feats of data collection? Well, according to the study, it's because: "mobile-phone operating systems currently provide only coarse-grained controls for regulating whether an application can access private information. For example, if a user allows an application to access her location information, she has no way of knowing if the application will send her location to a location-based service, to advertisers, to the application developer, or to any other entity."

The findings suggest a considerable threat to users. The blanket permissions provided by the user when installing a new app presents malware and spyware criminals with a golden opportunity to collect private data under the legal protection of a simple warning.

An official statement from Google, however, says that there is sufficient warning to their customers and little evidence of underhand tactics. "When installing an application from Android Market, users see a screen that explains clearly what information the application has permission to access, such as a user's location or contacts. Users must explicitly approve this access in order to continue with the installation, and they may uninstall applications at any time."

The moral of the story is to download mobile-phone apps with discretion. This doesn't apply only to Android users. Lookout Mobile Security revealed at the BlackHat conference in August that third-party smartphone apps on the iPhone were stealing private information and transmitting it to China.





# *ICO release UK's first code of practice on data sharing*

*By Suparna Sen, Smartcard & Identity News*



*Suparna Sen*

In the wake of a leaked law firm's database of file-sharers' personal details, on 8 October, UK's Information Commissioner's Office (ICO) has launched a consultation on a new statutory code of practice in regard to personal data sharing. The consultation will run for 12 weeks, ending on Wednesday 5 January 2011.

In December last year, ACS:Law, a UK-based firm specialising in intellectual property law, announced that it has planned to target illegal file-sharers across the UK in order to generate revenue for the rights holders and themselves. The company operated by using a third party to obtain IP addresses of bit torrent users and then apply for a court orders for the relevant broadband provider to hand over

customer information including names and addresses. The Guardian Newspaper revealed that ISPs often charge around £65 for an individual customer's information. Using this information ACS:Law sends template letters requiring the accused copyright infringer to pay fixed fines of up to £1000 or face legal action.

However, on 21st September 2010, a security breach occurred on ACS website when users of 4Chan (an image sharing site and bulletin board) decided a Denial Of Service attack against ACS Law's website. When the web-server required a reboot the site displayed a 350MB backup file of the entire website available to download for a brief moment whilst the server started itself up. It contained emails, passwords and credit card details of people who were targeted by the firm for illegal file sharing.

Although the backup was removed quickly, the attackers managed to save a copy of the database and upload it to various public file-sharing networks, including torrents, which could be downloaded by anyone.

Since ACS:Law did not keep these details secret they themselves are in violation of the Data Protection Act. A spokesperson for the Information Commissioner's Office (ICO) said:

"The ICO takes all breaches of the Data Protection Act very seriously. Any organisation processing personal data must ensure that it is kept safe and secure. This is an important principle of the Act. The ICO will be contacting ACS:Law to establish further facts of the case and to identify what action, if any, needs to be taken."

Information Commissioner, Christopher Graham said, "Under the right circumstances and for the right reasons, data sharing across and between organisations can play a crucial role in providing a better, more efficient service to customers in a range of sectors - both public and private. But citizens' and consumers' rights under the Data Protection Act must be respected". He stressed that citizens and consumers should engage and benefit from responsible sharing of information, and should see that their personal data is handled carefully and safely.

The Information Commissioner's Office has released a draft code of practice which sets out a model of good practice for public, private and third sector organisations, and covers routine data sharing as well as one-off instances where a decision is made to release data to a third party.

The code covers a number of areas including:

- What factors an organisation must take into account when coming to a decision about whether to share personal data;
- The point at which individuals should be told about their data being shared;
- The security and staff training measures that must be put in place;
- The rights of the individual to access their personal data; and when it's not acceptable to share personal data.

The code of practice document for review can be found here:

[http://www.ico.gov.uk/about\\_us/consultations/our\\_consultations.aspx](http://www.ico.gov.uk/about_us/consultations/our_consultations.aspx)

The ICO has welcomed leading UK organisations to come up with various proposals and draft models on data-sharing. Information Commissioner, Christopher Graham continued: "I would encourage all organisations who handle personal data to engage with the issue and offer their comments and suggestions on the draft code we've issued today. Only then can we make sure we've got a robust and adaptable code of practice that can be applied across the board."





## World News In Brief

### Apple to Offer iPhone on Verizon

After more than 3 years of using only AT&T cellphone networks, CEO of Apple, Steve Jobs, has plans to make the iPhone available on Verizon Wireless, the largest wireless carrier in USA. Currently, Apple is making a version of the iPhone 4 for Verizon's network, said a person, who is in direct contact with Apple.

Apple and Verizon will begin selling the phone early 2011, said the person, who agreed to speak on condition of anonymity because the plans were supposed to be confidential and he did not want to alienate his contacts at Apple. Both Apple and Verizon Wireless declined to comment on the news.

### HID Global's First-Ever veriCLASS Embedded Reader Platform

HID Global, announced its 'veriCLASS' payment and ticketing embedded reader platform, the first comprehensive and scalable solution that gives developers everything they need to speed time to market for products that support both closed and open-loop payment schemes. The platform will also include major contactless technologies and protocols in one system.

veriCLASS payment and ticketing embedded reader platform is based on universally adaptable contactless reader technology, and includes a wide range of integration tools, support and global product approvals and technology certifications. The associated Developer Tool Kit, online Developer Centre and Embedded Device Manager enable integrators to take their own contactless solutions to market faster.

The open veriCLASS platform supports all popular card technologies, including MIFARE, DESFire and iCLASS, a range of protocols and payment schemes, including FeliCa, EMVCo, Calypso, MasterCard PayPass, Visa payWave and American Express expresspay, and all major operating systems like Windows and Windows CE.

### epay and Cubic Partners for \$1.2Bn Sydney's Smartcard System

epay, a division of Euronet Worldwide, Inc. has teamed up with Cubic for a US \$1.2 billion smartcard ticketing system for Sydney, Australia's largest city. The new electronic ticketing system will provide a smartcard solution comparable to London's Oyster system for travel on public transport in the greater Sydney region.

### Legic Partners with Bosch for Smart Card Solutions

Bosch Sicherheitssysteme, suppliers of security and access solutions, will use Legic's smart cards for its access control, time and attendance and biometric applications. Legic will also support NXP Semiconductors' Mifare technology in its reader platforms. By becoming a Mifare licensee, Legic should have its reader components and systems compatible with the portfolio of Mifare-based smart cards, including Mifare Classic, Mifare Plus and Mifare DESFire EV1.

### Barclaycard to Introduce NFC Stickers and Pre-Paid Wristbands

Barclaycard is set to increase its investment in contactless technology with the introduction of NFC stickers for mobile handsets and pre-paid wristbands. Colin Swain, head of research and development at Barclaycard, said that the bank is now developing wristband, mobile and sticker products for contactless payments, of which people can enjoy wristband contactless payments at events such as music festivals, etc to offer patrons pre-paid payments options for concessions.

### Mopay, First International Mobile Payment Provider to Connect to 80 Countries Worldwide

mopay, a global leader in mobile payment solutions, now connects its mobile payment platform to 80 countries worldwide. With almost 100% coverage in Europe, North and South America and Australia, mopay recently expanded its footprint to South Korea and India, further extending its reach in the Asian market.

Online merchants using mopay can now offer easy-to-use mobile payments to more than 3.3 billion consumers worldwide. The addition of India and South Korea adds another 600 million mobile phone users that mopay reaches.

### EMV Confirmed as Global Payment Standard

A EMVCo report (the EMV standards body collectively owned by American Express, JCB, MasterCard and Visa), has confirmed that over 1 billion EMV cards and over 15 million EMV terminals are globally active, leading to 36% of total cards and 65% of total terminals in circulation based on the EMV standard.





## *Surf the wave. Don't try to change the mighty ocean* *By Peter Tomlinson - Smartcard & Identity News*



**Peter Tomlinson**

Some 4 months ago, SCN reported that Ian Watmore is back in Cabinet Office, working on (amongst other things) eGov topics for the UK. That reminded me that it is nearly 6 years ago that Ian's team was running regular meetings of the Cabinet Office eGovernment Unit's cross departmental Smart Card Working Group, on whose list of volunteer invitees were Dr David Everett and other (alleged) experts such as myself. At the end (for the sessions ceased once Ian's planned regeneration of govt ICT was refused funding) it was clear that Home Office's ID card project could only produce a passport card. Other public sector bodies would not be able to validate that card without a huge network of bespoke terminals. We were not going to go the eID route of digital certificates usable on-line via any internet connected PC with an at least semi-secure smart card reader

(or in future via mobile phone). So we citizens were not going to have offered to us a vital component of a method to be, in today's terms, safe online. And the vision behind M Prodi's eEurope (and our ODPM National Smart Card Project) of many more public services being provided online, all across the EU, interoperable, in a secure manner, using eID with X25 digital certificates, was not going to happen soon.

What goes around comes around, so that by the end of last year the Treasury wanted us to have access to many more public services online, leading to Cabinet Office getting more than a little stirred up. M Prodi's vision coming true (but just for our island): routine public services available 24/7 and at much reduced cost to the state. Then came the election and the Coalition, after which Cabinet Office really got a move on. Not only has Ian Watmore been brought back (football having turned out to not be his forté), but also Martha Lane Fox was confirmed as continuing in her post. Control of Directgov (formerly Government Gateway) was moved back from DWP into Cabinet Office. The Information Assurance Advisory Council started a series of Workshops 'Helping people fend for themselves online', following on from its series on privacy of personal data in cyberspace – as this article is written, I'm preparing for another 'safe online' session.

With all this kicking off, we wondered what would happen next. In June it came, out of left field: the USA. On The White House Blog was announced a rapid fire consultation about, not just a method for public sector service providers to be sure who is using their services, but how everyone might have the means to have secure IDs for use online, whatever they are doing. While the USA Feds digested the responses, on this side of the pond we continued to wait. Nothing much appeared at the headline level, but a lot was happening in the background. So it came about that the programme now known as G-Digital emerged, morphed, re-emerged. Declared participants are Dept of Health, Directgov (Cabinet Office), Businesslink, and a support team known as the Club (a shared service team hosted by DoH).

By contrast with the Feds and their informal approach, in August G-Digital put out an EU rules procurement notice. Late in September they put out another one. They have a questionnaire for the supplier chain - it is on their web site<sup>1</sup>. They ask suppliers what they can offer and when, in support of the G-Digital concept of safe online methods for all public sector on-line services - which means potentially trickling down to local govt.

But isn't this Big Society time now? Should not this methodology be universal: potentially applicable to all service provision for all users? Should it not equally protect both users and service providers? Should it not be developed much more in public, as promises to be the case in the USA? Even developed in co-operation with the USA Feds, with the European Citizen Card project, and with the (very relevant) EU STORK public-private collaborative project?

A coda: eID can of course attest to your official identity: the one used for your passport, known by central and local government, known by bank and solicitor. But very often we only need continuity and an associated authentication process, using a pseudonym as a handle: I can identify myself as Xerxes as I contribute to one web site, as Aberfordman on another (after the village from which my father came), as (not telling)...

Important to citizens is that we can connect safely to a web site that is itself safe to use; important to the web site owner is that the user is a person at a system safe to have connected. As the computers handshake, the people responsible at both ends want to be safely involved in surfing the wave on the mighty and sometimes dangerous ocean.

<sup>1</sup> <http://gdigital.direct.gov.uk/>





## World News In Brief

### Elcomsoft Breaks BlackBerry Backup Encryption

Elcomsoft, the leading Russian company that makes a range of password-cracking utilities, claims that it has successfully broken the 256-bit AES encryption used by the BlackBerry Desktop Software. The 256-bit AES encryption is used to protect data backups of tethered BlackBerry smartphones. The latest claim by Elcomsoft will surely leave enough room for exploiting BlackBerry data.

Elcomsoft's Vladimir Katalov explained in a blog posting how RIM strangely used only an iteration of a standard key-derivation function compared to Apple who has used 10,000 iterations in iOS 4.x.

Launching a brute force attack against an archive protected by a 7-character password with moderate complexity could be completed in about half an hour with the top-of-the-line Intel Core i7 processor. The flaw is found in both the PC and Mac version of the program.

### Apple Launches MacBook Air Laptop

Apple released a revamped MacBook Air at an event dubbed "Back to the Mac" at its Cupertino headquarters. The computer is seen as an amalgamation of what Apple has learned from desktop computing and mobile devices. Like the iPad, the Air will have no hard drive and rely on flash memory. According to Apple CEO Steve Jobs, "It's like nothing we've ever created before". Analysts said the new product sends out a clear signal to the industry.

### Commercial Breakthrough for Precise Biometrics in Nigerian State ID Project

The Cross River State is the first Nigerian state to implement biometric technology and combine authentication and payment in a state-wide 'Smartcity' card. The state ID card program is the first of its kind in the world and a breakthrough for Precise Biometrics on the African continent. In the coming years, all citizens in Cross River State, close to 3 million people, will be issued a card. More Nigerian and African States are expected to follow the market development with biometric ID and payment cards.

The Smartcity card will be used by the citizens for personal identification in public services such as tax declaration, healthcare, social benefits and pension, as well as enabling commercial services such as e-payments.

### Cubic Delivers iPhone App to Transport Association of Karlsruhe

The transport association of Karlsruhe (KVV), Germany, has taken a step towards the mobile future: Passengers may now download a new iPhone application developed by Cubic Transportation Systems, a business unit of Cubic Corporation.

The App can be downloaded by iPhone users from the Appstore by searching under KVV. Users who are registered at the web portal of the KVV touch the app and the application opens ready to purchase a ticket. The ticket has two-dimensional (2-D) barcode when the screen is touched -- to enable the ticket to be inspected by a barcode reader.

Single tickets, day tickets and also group tickets for a day can be bought via mobile in this way, no matter which fare stage and where the person is located within the KVV area.

### Contactless Revolution Gains Momentum for Australia's Commonwealth Bank

Faster and more convenient payment options are becoming a reality for Commonwealth Bank customers, with the Bank announcing further momentum with contactless payments. Bunnings and Dymocks have signed on to offer customers a faster way to pay using their Commonwealth Bank debit or credit card when paying for items less than \$100.

With the Bank's new major contactless partners on board, the number of Commonwealth Bank contactless readers across Australia will grow to more than 20,000 by the end of the year, alongside nearly four million PayPass enabled debit and credit MasterCard's.



## ***Verifone launches bid for rival Hypercom***

***By Tom Tainton, Smartcard & Identity News***



***Tom Tainton***

Verifone Systems has launched a £337 million hostile bid for Hypercom, a global leader in secure electronic payment who holds 23% of Europe's market share. Verifone executives said the deal would expand its corporate footprint in Europe, where it does not have a strong presence. After seeing an initial approach rebuffed, Verifone's latest bid represents a 52% premium over Hypercom's closing share price. Shares in the company have rocketed in after-hours trading, rising 45% as investors speculated whether the Verifone bid might draw attention of other potential bidders.

The French-based company, Ingenico, could be considered a possible rival after showing previous interest – abandoning a \$332 million Hypercom takeover

attempt in 2008. But some experts have suggested the possibility is slim, pointing to the fact that Ingenico already holds the leading position in payment solutions in Europe.

Nevertheless, Hypercom have vigorously rejected Verifone's bid, claiming that it 'significantly underestimates the value of the company'. In an official statement, the company's President, Philippe Tartavull, said:

"We believe that VeriFone's proposal is opportunistic and intended to disrupt our business, which has successfully taken market share from VeriFone in several markets. Hypercom is currently experiencing the strongest growth in global order demand in recent years and we are focused on converting this demand into revenue in the second half of 2010".

Hypercom, who have reported strong sales in Asia and Europe, is preparing to mount a strong defence – announcing that it expects to exceed analyst's estimate of \$112 million in net revenues for the third quarter. The company is adopting stockholders rights plan to fight off Verifone, hiring UBS and DLA Piper as financial and legal advisors. In comparison, JPMorgan acts as Verifone's sole financial advisor and will provide new committed financing.

In a letter to Hypercom, Verifone Chief Executive Officer Douglas Bergeron wrote that his company would be prepared to take 'extraordinary steps' to win regulatory approval for the bid, including the sale of Hypercom's US terminal business, adding that: "consummation of the proposal would insulate your shareholders from the risk that Hypercom faces should it continue to experience disappointing financial and operating results in these challenging markets."

### **World News In Brief**

#### **TfL Plans International Contactless Transit Card by 2012**

Transport for London said it hopes to see a cross-border contactless transit and payment card rolled out by 2012 that would support access to transportation services domestically and overseas. The agency is working with several other transport operators in the U.S., Europe and Australia to "develop common standards for the technology", a Transport for London spokeswoman said. The department is also in talks with several card companies, including Visa Inc., MasterCard Inc and American Express Co to this effect.

#### **Identity Theft Costs UK £2.7Bn Every Year**

According to the findings of National Fraud Authority (NFA), on average, criminals earn GBP 1,000 in credit or benefits for each name they steal. The NFA said criminals steal more than GBP 1.9bn while around GBP 800m is spent every year attempting to detect and prevent the crimes.

A total of 1.8 million people are affected each year and in the most serious cases it can take more than 200 hours to resolve the problems caused by identity fraud.



## MasterCard to Launch Digital Display Credit Card in Taiwan

MasterCard Worldwide has entered a partnership with Taiwan-based financial services provider Bank SinoPac to launch the MasterCard-SinoPac Display credit card. With the new display card in hand, Taiwanese consumers will now be able to access a range of mobile financial services such as online transactions using 3D authentication security and non pre-designated account transfers.

The new digital display credit card features one-time password (OTP) security technology combined with two-factor authentication. To use the card, a cardholder needs to lightly tap a button on the credit card and a 6 digit screen in the top right corner will display the one-time dynamic password. The embedded technology eliminates the need to wait for a text message during the initiation of a non pre-designated account transfer.

## Accenture Introduces Large Scale Biometric ID Matching Solution for Public Service Agencies

Accenture has unveiled a new large scale biometric identity matching solution at the Biometrics 2010 conference designed to help public service agencies accurately verify the identity of individuals, whether for the purposes of detecting potential national security threats or for improving the delivery of government assistance programs and social services to citizens.

Accenture's Large Scale Matching Solution can de-duplicate all available identity data, including biographic and biometric data. It is said to be highly secure, flexible, built on proven, open standards, and scalable when deployed to a cloud platform.

In addition to supporting border management agencies, large scale matching can also help citizens access a variety of government services quickly and efficiently.

## HID Global and Sony to Create Contactless Smart Card Readers for Global PC Market

HID Global and Sony Corporation announce they have entered into a Memorandum of Intent for a strategic partnership to jointly develop an embedded contactless smart card reader platform for the global PC marketplace. The jointly developed platform will

be designed specifically for laptop manufacturers and will encompass Sony and HID Global contactless solutions and a broad range of other widely deployed technologies while supporting specific regional and application needs.

The new embedded reader platform will support Sony's FeliCa contactless card technology, HID Global's iCLASS credentials, as well as other broadly adopted technologies. Furthermore, the reader solution will support applications based on Near Field Communication (NFC).

## Monitise Unveils World's First Truly Global Mobile Money Technology Platform

Monitise unveiled its enhanced technology platform which incorporates a range of mobile banking and payment services to deliver fast and secure financial management by mobile phone across the world.

The platform enables financial institutions, mobile phone networks, service providers, payment companies and processors to offer a wide variety of Mobile Money services in both developed and emerging markets.

Monitise Globe enables clients and partners to offer services by text, mobile app, mobile browser and USSD, operating on over 2700 different types of handset. It is also already compatible with the next generation of 'wave and pay' payments from the handset.

## Visa Europe Released New 'Visa Device Profiling'

Visa Europe announces the launch of Visa Device Profiling, a new fraud management service which provides fast and accurate information on locations where suspicious cross-border ATM transactions are happening. The service provides banks with a cost-effective tool for combating all kinds of ATM fraud.

Visa Device Profiling draws upon Visa Europe's global transaction data to identify the locations worldwide where suspicious card usage activity and ATM fraud are most likely to occur. It can detect sudden shifts in ATM use, quickly and accurately identifying those ATMs that have potentially been targeted by criminals.

Visa Device Profiling is available to European banks through a simple subscription service.





## *The Reality of Mobile Payments for the Consumer* *By Tom Tainton, Smartcard & Identity News*



**Tom Tainton**

For years now, mobile conferences have been hearing about the revolutionary impact that NFC will have on mobile commerce. Retailers and consumers alike gazed ahead with teary-eyed wonderment, envisaging a future of quick and efficient contactless transactions. But it hasn't been smooth sailing. The mobile payments market finds itself in a state of transition, blighted by a history of mediocre trials and solutions, but looking ahead to a promising future of technology innovations and contactless possibilities. There's one key question on the industry's lips: Will mobile payments become a widespread reality anytime soon, and can NFC live up to its lofty reputation?

Today NFC is a relatively well-known concept. But, if you've been living in a cave for the last five years then here's a reminder: Near Field Communication (NFC) enables contactless transactions, letting consumers use their phone to pay for goods and services – for example buying tickets for concerts, sporting events and transit access to public transport and air travel. NFC was jointly developed by Sony and Philips Electronics in 2002, and two years later, the NFC Forum, a non-profit organisation dedicated to promoting the technology, was founded. To date, the group has 150 members.

It might seem that NFC has been around for a long time, but compared to mobile commerce it's still in its infancy. Mobile commerce was born in 1997 in Helsinki, no less. It was here that the first mobile phone-based banking services was launched using SMS. In 1999, two mobile phone enabled vending machines were installed in the Finnish capital, the machines accepting payment by SMS as well.

Suddenly, everybody wanted a piece of the action. By 2000, mobile-commerce services had spread rapidly, with Japan offering mobile purchases for airline tickets, Austria offering train ticketing via mobile devices and Norway launching mobile parking payments. Major Asian commercial platforms were also launched - Smart Money in the Philippines and NTT DoCoMo's i-Mode Internet service in Japan. A year later the first conference dedicated to mobile commerce was held in London. By 2008, University of Central Lancashire's Computer Science department ran dedicated courses in mobile commerce.

It's been quite a rise. And today, the barriers to a commercial roll-out seemed to be crumbling. For a start, many fast-food restaurants (such as Yo Sushi), convenience stores (7-11, for instance) and nationwide chains have installed NFC/RFID contactless readers at the point of sale. Europe's largest mobile-payments trial has recently begun in Spain, with 1,500 Spaniards getting the opportunity to pay for their products using NFC-enabled mobile devices. But while mobile payments have made significant progress, it's still hindered by a familiar problem: Getting everybody to agree.

The issue surrounds the various players in the ecosystem, from the banks and payment processors to the carriers and mobile vendors. How can these industries figure out a revenue-sharing model that everybody can agree on? For example, NFC payments require an NFC-enabled device – but not all mobile devices are being built with the relevant technology. And this might not happen on a seriously large scale until mid-2011.

In fact, NFC's endless possibilities also contribute to its downfall. There are NFC-based applications which have yet to be developed or even thought of. With that in mind, it's nigh on impossible to put in place an infrastructure under which banks, transit authorities and consumers can trust the security of NFC.

The future of mobile commerce is an exciting one, but it's also a daunting prospect. Mass acceptance will not be as quick and widespread as many currently believe. The true challenge is generating a healthy profit – and at this time NFC is not a lucrative business model. The benefits are proven. The demand is significant. But, as with everything, money talks loudest.





## World News In Brief

### More than 50 Million NFC Phones Expected in 2011

Major NFC chip makers - NXP Semiconductors and Inside Contactless, predict the launch of 40 to 50 million NFC phones or more by the end of 2011, along with a smaller number of NFC bridge devices.

In interviews carried out by NFC Times, representatives of both the companies stated that they have seen enough indications of future orders from phone makers to confidently forecast the end of the drought of NFC devices by 2011, especially during the second half of the year.

### GrIDsure and Modirum to Offer New Payment Authentication Solution to Customers Worldwide

GrIDsure, the innovative alternative to passwords and PINs, announced it has formed a strategic partnership with Modirum, the authentication software and consulting company. As part of the partnership, Modirum will be integrating GrIDsure's innovative solution into its authentication customer offering.

The new partnership means that GrIDsure's one-time pattern-based pass-code authentication system will be available as part of Modirum's '3-D Secure' offering for 'Verified by Visa' and 'MasterCard SecureCode' and internet banking authentication solutions. This will enable consumers to have a more secure alternative to traditional static passwords, when logging into web-based services.

### OmniPerception Showcases Next Generation Facial Surveillance Technology at Biometrics 2010

UK biometric company OmniPerception will be unveiling its innovative light immune real-time facial recognition technology for the first time at Biometrics 2010.

'CheckPoint.S' uses OmniPerception's tried and tested face identification technology in a unique way in that it can scan a face in seconds even when the subject is moving and not directly looking into the camera.

Developed by experts at the company's UK headquarters, the technology can be used in a variety

of applications, including as a covert surveillance solution that can automatically scan faces and check identity, providing an alert in real-time if a match is found.

### At Last - Simple UK Rail Ticketing!

In sharp contrast to the seven out of ten UK consumers that now book air travel online, two out of three UK rail passengers still queue up at the railway station to buy train tickets. Quno.com, a new rail search and booking service has finally made it quick and easy for travellers to search and book train travel online.

The Quno website features the internet's first visual rail timetable. This ingenious tool allows customers to compare every train service available for a particular journey at a glance and purchase their tickets quickly. Quno also makes the best tools from online travel sites available to UK rail passengers for the first time.

### HID Global to Acquire ActivIdentity

HID Global announces that parent company ASSA ABLOY has entered into a definitive agreement to acquire ActivIdentity. The acquisition will widen the scope of HID Global's security industry leadership with incremental capabilities focused on the convergence of physical and logical access control.

ActivIdentity provides identity assurance solutions, and helps commercial and government organisations to defend against security threats and meet compliance objectives, while eliminating duplicate infrastructure and simplifying the user experience.

According to Grant Evans Chairman and CEO of ActivIdentity, "The combination of ActivIdentity with HID Global represents an important industry inflection point of logical access and physical access delivery capabilities".

The transaction is expected to close in December 2010 subject to regulatory clearances and approval by owners of a majority of the outstanding shares of ActivIdentity.





# FBI begin world-wide arrests of cyber criminals

By Suparna Sen, Smartcard & Identity News



Suparna Sen

October 1st brought us the news of the FBI busting one of the world’s “largest cyber criminal cases” that involved \$70 million (£44.4 million) of “bank fraud and money laundering” by a large group of hackers settled in East European countries such as Ukraine, Russia, Belarus and Kazakhstan.

The cyber criminals managed to steal 70 million dollars from American bank accounts by infusing “Zeus” Trojan computer virus into the concerned bank account holders’ PCs. Following the investigation, the FBI charged and arrested over 100 suspects from the US, with more worldwide arrests taking place in countries including Ukraine, The Netherlands and the UK.

## “Operation Trident Breach”

In May, last year, “Operation Trident Breach” was launched after FBI agents in Omaha, the largest city in the state of Nebraska, USA, got the news of suspicious banking transactions in the form of automated clearing house (ACH) batch payments to 46 separate bank accounts throughout the United States.

Working quickly with the local, state, and federal cybercrime task forces and foreign police agencies in the Netherlands, Ukraine, and the United Kingdom, the FBI arrested more than 150 suspected members of the hacking ring that was spread across the US, UK and East Europe.

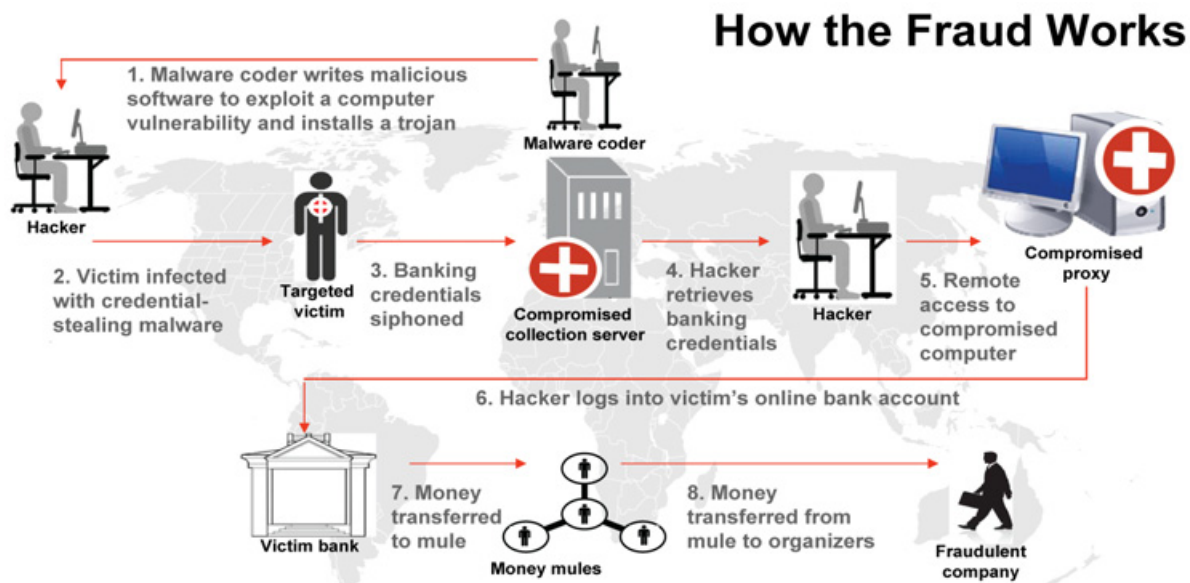
According to the FBI, the hackers used to target bank accounts of small companies, municipalities, churches, and U.S citizens who usually added less importance to network security and taking necessary steps to curb online frauds.

## How did the cyber criminals operate?

The FBI said that the suspects worked as “mules” or couriers (who transfer money to the criminals after keeping a certain percentage for themselves) for the hackers residing in Eastern Europe. The hackers used to infect the victims’ PCs with the Trojan horse virus – “Zeus”. The virus is carried in an e-mail. The Zeus virus captured passwords, account numbers and other banking details of persons, and send the details to a remote server in real time for the hackers to get free access of the victim’s personal online bank account data.

After getting hold of an individual’s personal bank details using the virus, and seizing victim’s money, mules transfer the money. “The mules could either wire it back to their bosses in Eastern Europe, or turn it into cash and smuggle it out of the country”.

To note: Zeus can be bought for a few thousand dollars per copy in underground online forums or black market.



Law enforcement agencies across the globe combined their efforts, and on September 30th security services of the Ukraine (SBU) detained 5 suspects and issued 8 search warrants. On the same day, UK law enforcers arrested 20 members of the gang, believed to be responsible for stealing over \$30 million from banks worldwide between October 2009 and September 28, 2010. On the 8th October 2010, U.S. police accused 37 foreigners involved in seizing \$3million from US banks of which 21 are Russians.





Interpol, the world's police and crime-fighting bodies have demonstrated their agreement on the need for a safer and more secure internet framework by its long-term engagement with ICANN, the organisation which develops and agrees policies for the future of the web.

SOCA (The UK's Serious Organised Crime Agency) e-Crime Senior Manager, Paul Hoare emphasised the value of collaboration in the fight against cyber crime added: "Working jointly with the FBI and other global partners, we have produced a recommendation for changes to the domain registration process. This would see minimum standards made a condition of accreditation by ICANN, making the internet a much more hostile environment for criminals".

## World News In Brief

### **AT&T Debuts Encrypted Mobile Voice**

AT&T Co. has launched a new two-factor encryption service for sensitive-but-unclassified mobile voice communications - AT&T Encrypted Mobile Voice. The solution comes out of the AT&T lab, said Stacey Black, vice president of strategic products for AT&T Business Solutions.

The on-demand service is built on an encryption engine on a chip, TrustChip from KoolSpan Inc., and encryption management software, One Vault Voice from SRA International Inc. It works on BlackBerry and Windows-based smart phones.

### **Denver Transit Service to Use New Smart Card Ticketing System**

Transit riders in the Regional Transportation District (RTD) of Denver, USA are to get a faster, more efficient advanced fare collection system. The Denver transport authority has signed a four-year, \$15 million contract with ACS, to let the public transportation users receive smart cards free of cost from the city, load them with a pre-paid amount, and simply wave the smart card in front of a scanner when boarding for a contactless ticket entry.

### **Oberthur wins Best Prepaid Manufacturer Award at Prepaid Awards 2010**

Oberthur Technologies, a global provider of security solutions, is the winner in the Best Prepaid Manufacturer category at the 3rd Prepaid Awards 2010. The award recognises Oberthur Technologies' leadership, delivering millions of prepaid cards globally each year for both the financial and telecoms sectors through its Card Systems Division.

### **Automation of Password Resets to Cut Cost and Complexity**

HTK's new IVR-based Horizon Password Reset will henceforth allow IT departments to significantly cut their costs by automating the password reset process. By using the new Interactive Voice Response (IVR) developed by HTK, a company can considerably cut down the cost and time wasted resetting forgotten, expired or compromised passwords.

The IVR-based Horizon Password Reset service comes at a cheaper rate and enables automation of the password reset process. Users just need to call the IVR service and are taken through a set of pre-defined steps for identification and verification.

### **Visa Confirms Collis Brand Test Tool for payWave Contactless**

Collis has announced that its Brand Test Tool (Collis BTT) has recently been approved by Visa Inc, which will be used by acquirers to meet the testing requirements for Visa payWave contactless (ADVT-qVSDC) terminals. The Collis Brand Test Tool (Collis BTT) will enable terminal acquirers and vendors to validate the payment brand testing of their EMV terminals (POS and ATM).

The Collis BTT is used to test the behaviour of a terminal for both contact and contactless payments, without the need of physical test cards. The ultimate goal of tests performed by the Collis BTT is to have an EMV-compliant and payment association-certified terminal that can perform trouble-free transactions within the entire payment infrastructure.





## *Private Key Management: Best Practice Tips from the Real World*

*By Paul Tuner, Vice President of Product and Customer Solutions, Venafi Inc.*



**Paul Tuner**

It has always been taken for granted that the entire IT security industry understands that, as part of digital certificate management, it is necessary to manage the private keys associated with those certificates. A recent conversation with an analyst made it clear that this assumption was just that – an assumption. There were two reasons, he said: 1) very few people realise that managing certificates also requires the management of private keys, and 2) not many people understand how critical the security of private keys is in protecting sensitive data.

It has always been believed that, “the key is the data.” The point is that if you protect data by encrypting it with a certificate, the private key becomes the data or asset that has to be protected (i.e. that encrypted data is effectively useless without the key but if the wrong person gets that key, the data is at risk).

This can be related to a topic which many of us have already spent considerable time thinking about - symmetric keys. Let’s say, based on PCI or some other regulation that an organisation decides to encrypt the columns that contain personally identifiable information (PII) on its database using symmetric keys. What happens when you retrieve that data from the database? The database is going to decrypt the data using the symmetric key(s) and pass it across the network. So, assuming there is still a concern about the security of that data, how can that organisation ensure that the data is secure as it travels across the network? The answer is that it is encrypted using a certificate and private key. It is just common sense that any organisation would want to implement the same security procedures for its private keys as it does for its symmetric keys.

There are, of course, objections that can be made to this approach: “We’re not subject to PCI because we don’t process credit cards.” That may well be the case but, what other types of data can be passed across a network and the Internet that you might want to assure is properly protected - based on the industry you are in? They would include:

- Bank account information
- Insurance information
- Patient healthcare records
- Employee salary and benefits information
- Corporate financial information
- Stock account information
- Corporate trade secrets, etc

How private keys are generally managed today? Most organisations are doing it manually (with a spreadsheet and reminder notes) with no dual control. Here are the typical steps an administrator goes through to generate a key pair (which includes a private and public key) and get a certificate.

- Create a keystore, if one doesn’t already exist
- Assign that keystore a password to protect its contents, including the private key(s)
- Generate a key pair (public and private key)
- Generate a certificate signing request (CSR)
- Submit the CSR to the CA
- Retrieve the certificate from the CA
- Install needed CA certificate(s) in the keystore
- Install the certificate in the keystore
- Backup the private key (if deemed necessary)
- Extract the private key and certificate so they can be placed on other systems (e.g. for load balanced configurations)





How do typical organisations secure and manage their growing private key inventory—the keys required to encrypt data in transit? How are the keys protected against loss, misuse or theft? These become especially important questions given that, according to Gartner, the majority of data breaches are executed from inside organisations. In most cases, the private keys are not being protected.

The PCI DSS requirements for private key management cannot be accomplished in an IT environment that relies on manual processes. There are both security risks and operational challenges when administrators attempt to perform these steps manually.

The problem with administrators performing these steps manually is that it opens them up to a host of potential security problems, either because they are not following best practice or because they are malicious. Here are some security challenges that present themselves:

1. Administrators normally use the same keystore password on multiple systems (sometimes hundreds) so it is easy to remember them.
2. Administrators usually have to share keystore passwords with other administrators because they're all sharing in the work managing a group of systems.
3. Administrators rarely comply with corporate password rotation policies (e.g. change every 90 days) for keystore passwords and will often use the same password for years. (One administrator at a very large bank told Venafi that they call keystore passwords “passphrases” so that they don't have to comply with the corporate “password” rotation policy. If you can believe it, this practice actually got them in compliance with their auditors.)
4. Administrators who have direct access to keystores and the passwords that protect them **can make copies of private keys** which can be used to decrypt the data you're trying to protect. This is a big problem if those administrators leave the organisation.
5. Most organisations don't make it a practice of replacing private keys when the administrators who have had access to them are reassigned to a different department or leave the organisation.

Given the typical re-use of the same password across multiple systems, the fact that passwords aren't changed for years and the sharing of passwords amongst multiple administrators, organisations are exposing themselves to massive risk.

If these challenges exist within your organisation or department, here are some recommended best practices to better protect the private keys that safeguard critical corporate data:

- **Automate:** Use an automated key and certificate management system that removes the need for administrators to access keystores directly and the passwords that protect them
- **Rotate Passwords:** Change keystore passwords regularly
- **Separate Duties and Roles:** Have a different set of administrators manage keystore passwords than the administrators who manage the systems where the keystores reside
- **Proactively Change Keys:** Change private keys (and the corresponding certificates) each time an administrator who has had access is reassigned or leaves the organisation

The management of private keys and certificates is central to the security of all data. It is only by following best practice, and not making assumptions, that system administrators can be assured that all data is safe. Without policy-based management capabilities in place, there will continue to be high-profile data breaches and system outages on mission-critical applications with increasing frequency and cost.





# NEXT GENERATION CARDS & PAYMENTS

CONFERENCE AND EXPO  
BRUSSELS, BELGIUM  
25-26 NOVEMBER, 2010

**FREE**  
to attend for  
all banks

## Profitable payments business models for the post-SEPA competitive market

The competitive landscape for payments in Europe is changing. Banks are being forced to reinvent the business models for traditional banking services as emerging non bank players and other financial institutions offer innovative payment solutions through alternative banking channels. Next Generation Cards & Payments is Europe's only **FREE** event for banks, bringing together senior cards and payments professionals from leading banks, mobile network operators, regulators, new card schemes and non-bank financial institutions to define the future for their businesses.

**w. [www.nextgencards-payments.com](http://www.nextgencards-payments.com)**

**t. +44 (0)20 7067 1831**

Lead Sponsor:



Co-Sponsors:



Media Partners:



