

### 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** –  
DreamingSpire , Suparna Sen,  
Matthew Berzinski, Tom Tainton,  
Peter Tomlinson,

**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.

## Our Comments

Dear Subscribers



*Patsy Everett*

Do you ever have one of those weeks when everything just seems twice as hard as it should be? I don't know about you but I dread having to call my bank for whatever reason, having gone through all the automated, please enter your account number rig morale, we eventually get to a human being and then it gets worse.

Please can you tell me what transaction you did on the 16th day of last month? It goes on and eventually you get so confused and flustered you begin to wonder if it's actually your account let alone bank and who exactly is the customer here. I don't know if this has ever happened to you but then sometimes you are told, not always politely, that you have failed security and they are unable to help you, good bye!

There has to be a better way, authenticating people has just become too difficult. The first problem is that each organisation has a slightly different approach to how they authenticate you, there may be passwords or PINs involved a check on recent transactions or perhaps a check on previously shared personal information. Don't we need a standard way of authenticating people?

Then there are those PINs and passwords, sometimes they are numeric, sometimes they are alpha based, sometimes there must be a number, sometimes at least 9 digits, oh and successive digits in a sequence are not allowed. I could go on and on but what a ridiculous state to be in. We can debate whether it is advisable to have a common password but dear friends tell me who can remember 10 different passwords unless they are used everyday, so then we have to write them down, is that safe? Any way all these different systems prohibit a common password by their weird and wonderful rules of acceptability. Has anybody ever examined the reaction of users to all these different systems?

Well I can hear you thinking what is the solution then? So let's gently wander through the garden to see what might be acceptable to both the prover and the verifier (don't worry this is just about the extent of my technical knowledge). In everyday use we need to prove our identity in both the physical and virtual worlds. In the former case a photo identity card like a driving license is widely accepted, now I have no problem with this but how about those people who don't have a driving license? Well why don't they just go and get one! So I guess the thing here is that we have a common document that does involve a registration process. Now here is the test, if I went to the bank and on presentation of the photo ID I (previously registered with the bank) was allowed to empty my bank account would that be OK? Well who would be on risk here in the event of fraud? What is the probability that someone could counterfeit my photo ID and look sufficiently like me to be accepted by the bank teller? Doesn't this just make you feel a little nervous?

It all sounds a bit like single factor authentication so we just need





something else. Now I can speak with authority here, the other part of the family has spent at least 30 years trying to persuade people to carry widgets not too different to the gizmos the banks are currently providing to be used in conjunction with your debit or credit card for on-line banking. However in this case, you don't need to carry them around at all because normally you would be doing the banking at home in the evening.

There is light at the end of the tunnel, everybody these days does carry a widget around with them, usually in the disguise of a mobile phone. So what I need the teller to do is to authenticate the phone in my purse as the one belonging to me and previously registered with the bank. They could send some code by SMS which I just replay to them, probably wouldn't take more than 10 seconds. Still remembering minutes or what seemed like hours of previous exasperation it would be pretty good for me and would also do the business in the on-line world although we would also need a virtual driving license or something to get back the two factor authentication!

This may seem like a rant but is it really that difficult to authenticate people?

Patsy.

## Contents

### Regular Features

Lead Story - Good Government does it Online .....	1
Events Diary .....	3
World News In Brief .....	5,10,16,19

### Industry Articles

Overcoming Barriers to Strong Network Authentication .....	6
Myki Ticketing Fails To Win Over Public .....	8
Interview with Sebastian Hans - Chair of the GlobalPlatform IP Connectivity Task Force .....	9
Miracle Payments begin in India .....	12
TwinSet, a contactless HF/UHF smart card .....	15
The Future for Transport Smartcards .....	17

## Events Diary

### July 2010

- 7-8 The Future of Cards and Payments, Le Méridien Piccadilly, London, UK - <http://www.marketforce.eu.com/Conferences/cards10/>
- 20-22 Mobile Money Services Africa, Johannesburg, South Africa – <http://www.iir-telecoms.com/event/mmsa>

### August 2010

- 25-26 5th ID, Smart Card & Ticket Security & Anti-Counterfeiting Technology Summit, China – <http://www.cids.com.cn/En/>

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





## .... Continued from page 1

During the early part of this year, there was background activity. Even during the pre-election purdah period we heard about it. Indications that cyber security concerns would bring pressure on Whitehall Departments to be safe online – safe for us to use, safe against attacks. The Office of Cyber Security had been created for that purpose, as promised last year.

From mid April until mid June: silence. Then announcements began to appear, along with some informal messages.

**15th June from Cabinet Office:** Whitehall shake-up in drive for efficiency. An Efficiency Board full of talent. A Cabinet Office Structural Reform plan. A whole list of tasks (although not always clearly titled). Those tasks nearly all started in June. A few start later. One of them (Establish and have in place a robust implementation plan for each central govt dept) runs May to Sept this year.

**18th June from Cabinet Office:** Martha Lane Fox reinstated as UK Digital Champion, to be a member of the Efficiency Board. DirectGov enhancement to resume.

**25th June:** the second stage of the public transport smart and integrated ticketing project is definitely approved for the 9 largest metropolitan areas outside London – the informal news is that the funding is only to the end of this current financial year. ITSO Ltd's funding also appears to be OK for a while, but not yet confirmed to the Members.



*(left) Martha Lane Fox, who became the face of dotcom Britain in the 90s when she co-founded lastminute.com.*



*Ian Watmore, a former permanent secretary and former chief executive of the Football Association.*

**End June:** Ian Watmore is back in Cabinet Office. Chief Operating Officer of the Efficiency and Reform Group. But not visible until September – behind the scenes until then, getting himself up to speed part time, then he will be working on the current year savings (the £6.2bn). In 2004 he had a plan for regenerating govt ICT, so he knows what's what. That plan included taking some smart token concepts through into service delivery. Other countries are doing it: Germany is now following the Baltic States in introducing a citizen token for use online, complete with digital certificate for strong authentication (its also an ID card, but we don't talk about that here).

So we cannot yet really be sure what will happen to keep us and the public sector safe and conveniently online, or when. But recent experience indicates one word about the engaged people in the public sector: training.

By DreamingSpire.





## World News In Brief

### **Stagecoach to expand Smartcard Options for Bus and Rail Passengers**

Stagecoach Group is set for a major expansion in the use of smartcard technology on its bus and rail services in the UK, the company announced. The expansion will build on its sector-leading position as the country's first transport group to pioneer the Government's preferred technology across both modes.

More than 53 million smartcard transactions are already made on Stagecoach buses and trains each year, including the UK's first use of the Government's ITSO technology on the national UK rail network and the country's first contactless bankcard payment scheme in Merseyside.

Stagecoach Group has also developed its own StagecoachSmart travel card, using a system provided by Vix ERG, to offer multi-modal ticketing on its bus and rail services using the ITSO technology. The company recently became the first UK bus operator to roll out a smartcard system across an entire operating area with the launch of StagecoachSmart throughout its Cambridgeshire bus operation.

### **FBI Fails to Crack Brazilian Banker's Hard Drive Codes**

After a year of failed attempts, the FBI has admitted defeat in its attempts to crack the encryption codes protecting hard drives belonging to a prominent Brazilian banker arrested in connection with a money laundering investigation.

According to local press reports, Brazilian police seized 5 hard drives from Daniel Dantas in July 2008, but after 5 months of failed attempts to decode them, the FBI was called in. However, the Americans had no more luck accessing the files, which were encrypted using TrueCrypt, the free, open-source software and another program. The drives were handed back to Brazilian authorities, which have no powers to force either TrueCrypt or Dantas to hand over the pass-codes, in April.

### **Fiver-only ATM Network Launched**

A network of free-to-use ATMs that only dispense £5 notes has been launched in the UK by operator Bank Machine. Bank Machine has introduced the 21 ATMs as part of a 'fight for fivers' campaign designed to increase the number

of notes in circulation. After trialling 2 fiver-only machines in London, increasing circulation by 100,000 a month - the firm is now installing several more in Martin McColl's shops. In a bid to increase the number of fivers in circulation, last year the Bank asked HSBC to stock 100 UK cash machines with them for a trial period.

### **Romanian Police bust ATM Skimming Factory**

According to local press reports, police raided 38 locations in Craiova, 6 in Bucharest and 3 in a neighbouring county. Those detained face accusations of being members of an organised crime group, unauthorised access to a computer system, possessing card-cloning equipment, access device fraud and distributing fake electronic-payment devices.

The skimmers were either sold to other criminal gangs or used by ring members in Italy, Germany, Sweden and Romania, say authorities. Meanwhile, reports also claim that the Romanian Directorate for Investigating Organized Crime and Terrorism has arrested 5 fraudsters allegedly part of a card cloning gang.

### **Atmel Approach INSIDE Contactless for Sale of its SMS Business**

Atmel Corporation, a leader in microcontroller and touch solutions, announced that it has entered into a definitive agreement to sell its Smart Card (SMS) business based in Rousset, France and East Kilbride, UK to INSIDE Contactless S.A. ("INSIDE") following the completion of the information and consultation process with the works council of Atmel Rousset in France (the "Works Council"). As previously announced, INSIDE signed the agreement on May 2, 2010 subject to acceptance by Atmel following completion of the information and consultation process with the Works Council.

Pursuant to the definitive agreement, INSIDE will pay \$37 million in cash at the closing, subject to a post-closing working capital adjustment and an additional cash consideration of up to \$21 million if certain earn-out targets are met in 2010 and 2011. As part of the transaction, Atmel has agreed to make a minority investment in INSIDE of approximately \$4 million. The transaction is expected to close by the end of the third quarter of 2010, subject to certain closing conditions.



# *Overcoming Barriers to Strong Network Authentication*

*By Matthew Berzinski, Product Manager, Passlogix Inc*



*Matthew Berzinski*

Strong authentication is slowly gaining acceptance for protecting access to sensitive enterprise applications, but adoption for network logon is close to zero. Despite the security benefits of requiring authenticators such as smart cards, tokens and biometrics to open the network 'door,' technical and financial stumbling blocks have barred the way.

Today those barricades are falling. New technology is enabling two-factor network authentication without a lengthy logon process, burdensome back-end administration, or lock-in to a single proprietary method of authentication. The new methods are also slashing back-end infrastructure costs from more than \$100 per end user to as little as \$15.

In environments where users already carry government-issued citizen identity cards or RFID-based door access badges, even front-end costs are dropping because those devices can now do double duty for Windows logon. This eliminates the expense of buying, issuing and managing new devices dedicated to network authentication.

All of these new capabilities are making it far easier for IT managers to justify the investment in strong network authentication. Once the infrastructure is in place, applications can be more easily strong authentication-enabled as well. The upshot will be better security for both network and application access.

## **Beyond Passwords**

The growing interest in two-factor authentication is being spurred by rising recognition that passwords are an imperfect solution for protecting an enterprise's information assets.

Simple passwords can be easily hacked and shared. Complex passwords increase help desk calls and associated costs. Both can be physically pilfered from written password lists that users are forced to maintain as memory aids because of the number of passwords required to sign on to different applications, databases and Web accounts.

Organisations are also becoming increasingly interested in two-factor authentication as a means of facilitating compliance with a variety of government and quasi-government data protection regulations.

From global requirements like the Payment Card Industry Data Security Standard (PCI DSS) to the EU's Basel II banking regulations and U.S. mandates such as HIPAA for healthcare information and Sarbanes-Oxley for corporate governance, the use of strong authentication can help validate data protection intent. It can also provide an audit trail linking individual users to each point of data access, ensuring that the culprit can be identified in the event of a breach.

## **Sticking Points**

Despite these incentives to adopt strong authentication, however, initiatives for network protection have traditionally been stymied first and foremost by cost and related return-on-investment concerns.

Using a smart card or other two-factor authentication device for Windows logon eliminates one password, but it typically leaves six or more application passwords to deal with. That makes it difficult for IT managers to make a business case for paying \$100 per user to get rid of a single password, particularly given the \$50-per-user cost of abolishing all application passwords and simultaneously implementing two-factor application authentication via enterprise single sign-on (ESSO) technology.

Strong authentication at the network level has also faced the same hurdles that have slowed adoption at the application level: user resistance, administrative complexity and authentication 'method wars.'

Certificate-based smart card authentication, for example, can take as long as 15 seconds and unleash user wrath leading to failed deployments. The need to install, manage, mirror and back up a separate proprietary infrastructure for any kind of authenticator has been an additional deterrent. So has the need to choose one type of authentication device from one vendor, even though a single method rarely meets an organisation's needs.





## **Paving the Way**

What has changed in the past year is the development of universal authentication management technology that removes all of these impediments – including cost.

For the first time, any mix of identification devices from any vendor can now be used for Windows logon. That includes authenticators already deployed for other purposes – such as proximity card/building ID badges and national identity cards – as well as ‘simple’ smart cards requiring only a card ID number without an elaborate PKI certificate back-end, standalone or built-in laptop biometrics, one-time passwords via mobile phones, and question and answer sequences.

The use of Microsoft Active Directory for data storage and administrative policies eliminates the need for proprietary authentication servers or other back-end infrastructure, lowering back-end costs to \$15 per user as well as relieving the burden on IT staff.

Users simply present their authentication device to the workstation at network logon, and the system does the rest.

A user with a door access badge, for example, simply taps the badge on a badge reader attached to their computer and enters a PIN code. The system retrieves the user’s logon credentials from Microsoft Active Directory and compares them on the client. If they match, the system provides Windows with the information needed to log that user on. Another tap of the badge locks the workstation or logs the user off.

This fast, simple logon process eliminates barriers to user acceptance. Device types can be mixed and matched, making it possible for organisations to support multiple authentication methods that may be required by different end users from a single administrative interface.

In addition, the ability to support any authentication device gives organisations the flexibility to change device vendors or types without making costly changes to the back-end authentication infrastructure.

## **Security Plus**

With this new technology at their disposal, chief security officers and IT managers have the tools they need to add a second ‘lock’ on the network door in a flexible manner and at an affordable price – whether using a building ID badge, certificate-less smart card, simple swipe of a finger, or any other authentication strategy or device mix.

Implementing this extra identity check will make it possible for organisations to improve security over password logon as well as support regulatory compliance efforts related to data protection without the technical and economic obstacles of the past.

At the same time, by supplying core infrastructure, it can serve as a sparkplug for accelerating the adoption of strong authentication for applications and other enterprise information assets as well.

After years of languishing on organisation wish lists as a security project that could not even be considered because of the numerous problems involved, two-factor authentication is now – finally - ready for prime time.





## *Myki Ticketing Fails To Win Over Public*

*By Suparna Sen, Smartcard & Identity News*



*Suparna Sen*

The Australian public has judged the new contactless ticketing scheme a failure. The Myki card scheme has so far cost a whopping \$1.35 billion, and a recent survey (taken from January to March 2010) revealed only one in every 20 train travellers use Myki.

Myki is a new plastic RFID-based smartcard to be introduced in all trams, buses and trains in the Victoria's cities by the end of this year. Myki will replace the existing Metcard transport ticketing system.

Last month, the Myki smartcard system failed one of the many tests organised by the Transport Ticketing Authority (TTA) for its successful implementation in trams and buses in Melbourne (the capital city of the Australian state of Victoria). Due to technical problems, Myki operators 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. Now, the Victoria state government has taken up \$120,000 publicity campaign to promote the troubled Myki smart cards.

Currently, Metcard is used across all public transports in Melbourne city. The prototype testing of Metcard got started in December 1993, with the system commencing full revenue service from May 1998 at a cost of \$330 million.

Myki based on contactless smartcard technology is designed to replace the magnetic stripe Metcard and also V/Line regional ticketing systems. John Brumby, Premier of the state of Victoria gave his reasons for the introduction of the Myki ticketing system. "Well, myki will offer a number of benefits to public transport users in terms of convenience, lower fares and durability."

You can use the Myki smartcard to travel conveniently without buying the tickets every day. The Myki card will operate by simply touching the card on a myki reader when you board a train, tram or bus, and then you touch off against the reader at the end of each leg of your journey. Once you press the card against the reader, it will read the card and show you green light if touching is successful and red if it's unsuccessful or if the card is having some problem. The reader shows orange when your Myki card balance is low.

Myki offers its users lower fares than the current 2-hour and Daily Metcards. For example, a 2-hour Zone 1 full fare using myki smartcard is \$2.94; while a 2-hour Zone 1 full fare metcard costs \$3.70. That is a saving of 76 cents by travelling with a myki card!

Myki card is durable, made of plastic compared to Metcard which is made of cardboard.

The Myki smartcard ticketing project began as early as in May 2005 with a scheduled delivery date of March 2007. However, the scheme failed due to contractors' continuous experience of "less than optimum performance" during myki's trials on trams where electrical currents and interference were creating problems. Also, software problems were causing issues with Myki's touching on and off.

TTA, responsible for the management of the new public transport ticketing system, has paid a lump sum \$721,000 to Chadstone and Highpoint Shopping Centres to allow parking its Myki promotional truck in front of the shopping centres. TTA has also spent \$14,412 on smaller displays inside these two shopping centres and at festivals, besides paying \$6000 bill to the security (over six months) for guarding the truck from damage.

Complaints have already started pouring in as to the overpriced Myki system still not working on trams. Research obtained by the Herald Sun under Freedom of Information laws shows that the TTA's own research ranked Myki as 62 out of 100, while Metcard got an overwhelming 78. The Transport Department research also found out just 5% of train travellers use Myki, or about 20,000 a day out of the 100,000 plus Myki cards issued.

Balance has to be kept in the Myki smartcard account to use its services when you wish to, even though there's no guarantee of any service being delivered. Besides, the Myki officials keep on telling you to carry a Metcard whenever you go out in case you need it anytime Myki stops working.

The government is continuing to pay for the existing Metcard system alongside Myki to ensure commuters have a chance to switch over to Myki, before Metcard is completely removed from the transport network. A total cost of around \$1.35 billion, with \$494 million for start up and \$50-55 million per year to run the system is only adding more confusion and distress on the part of Melbournians.

People are just frustrated by the government's plan to dump the popular city saver fare system – Metcard when it is working just fine. Melbournians are reluctant to pay \$10 for a plastic Myki and all the more reluctant to pay more in order to put value on it. Further, you and I have to shell out another \$10 to replace the existing card every 2 to 3 years. (According to Melbournians, Metcards work just fine as long as you don't bend them)



## *Interview with Sebastian Hans, Chair of the GlobalPlatform IP Connectivity Task Force*

*By Tom Tainton, Smartcard & Identity News*



*Tom Tainton*

GlobalPlatform, the international specification body for smart card infrastructure, has launched an Internet Protocol (IP) Connectivity Task Force to ensure that GlobalPlatform Specifications and Configurations support and drive the future integration of smart card technology with the IP landscape.

Sebastian Hans, Chair of the Task Force, shares the reasons behind the launch of the group, its aims and objectives, and the future impact of the internet on the smart card industry.

### **What is the IP Connectivity Task Force and how did the idea come about?**

GlobalPlatform has the ability to create task force groups when members, through their engagement in the Advisory Council (a forum open to all members), identify the need to dedicate resources to defining GlobalPlatform's role within a particular market sector or relevant to a specific application. Task forces provide a platform for strategic discussion and collaboration between all members of GlobalPlatform on a targeted area of interest.

Created in response to the increasing demand for personal and consumer IP technology, GlobalPlatform launched an IP connectivity task force in April 2010. The group brings members together to discuss new business requirements for network-capable objects, and to identify how GlobalPlatform technology can progress to meet these advancements.

GlobalPlatform has launched two other task forces since its inception in 1999 – the mobile task force and the government task force. Established in 2006, the government task force determines GlobalPlatform's role in addressing the long-term needs of governments engaged in large-scale smart card deployments for e-ID. A year later, the mobile task force was created to actively contribute to the development of mobile telecommunications standards and address key issues associated with the migration of payment applications onto mobile devices.

### **Why is there increasing demand for consumer IP technology?**

Since the mass adoption of the World Wide Web over a decade ago, customers no longer view the internet and their handset as a tool but an indispensable part of their lives. Simplifying the digital life of customers is key to staying ahead of the competition by providing value beyond today's services.

There is a trend for all devices to be integrated with IP technology, so that the end user can connect with the IP network. In today's marketplace, a device without this level of connectivity can become obsolete.

### **How will the approach help GlobalPlatform and smartcards advance in the online marketplace?**

The IP connectivity task force's vision will be shared with GlobalPlatform's Technical Committees so that they can look at how GlobalPlatform Specifications can be advanced to create an environment that will encourage technology developers to capitalize on the smart card's ability to connect with IP-based infrastructures.

Last year, the GlobalPlatform Card Networked Framework v1.0 was released – a technical document which enables a smart card to securely and effectively manage the card, based on web technology, and in 2008 GlobalPlatform also documented a variety of ways to upgrade a smart card program to facilitate IP network connectivity to ensure it accommodates a range of implementer requirements in Amendment B to Card Specification v2.2.

The launch of the task force will ensure GlobalPlatform can build on this contribution to the marketplace and support a rapid migration of smart cards to IP connected environments.

### **How will the task force benefit GlobalPlatform members and customers?**

The internet is a vital tool in delivering exciting and interactive services to end-users, and it is critical that GlobalPlatform's Specifications can interact and support its evolution. By setting up the task force,





GlobalPlatform will be able to build on its significant contribution to this marketplace and by sharing its wealth of expertise, will support a rapid migration of smart cards to IP connected environments.

In turn, this will provide GlobalPlatform technology users with the ideal platform to develop new services and sustainable commercial partnerships.

### **Does the task force indicate the future of the smartcard industry and its transition to the online marketplace?**

In response to the momentum behind IP connectivity, the task force will bring members together to discuss what more the organization can do to drive the market. GlobalPlatform should help the application provider to support new use cases related to offering secure services to the end user via an IP network.

Different industry bodies such as the European Telecommunications Standards Institute (ETSI), Open Mobile Alliance (OMA) and International Organization for Standardization (ISO) have already started to address the issue of IP connectivity. The intention of the task force, however, is to ensure that whatever the environment (home computer, mobile phone, consumer product) or usage (application to application, or token to token) there is a standard solution that allows a service provider to deploy the solution.

### **What are the challenges facing the task force?**

GlobalPlatform will be challenged to integrate the smart card into the general purpose IP network to solve matters such as how to obtain an IP address within a home network or how to enable the integration of IP-based services. We will also be examining means of protecting the card and its services and new ways to communicate over IP networks.

### **What are the long-term objectives of the IP Connectivity Task Force?**

GlobalPlatform's objective is to identify and document use cases for smart card and IP networks and to define requirements, both business and technical, within these use cases. We will identify how GlobalPlatform technology (existing and future) can be leveraged and, in doing so, contribute to the growth of this technology in a standardized and highly specified manner.

Additionally, the task force intends to analyze the business benefits of IP connectivity solutions, identify gaps in GlobalPlatform's own set of specifications and to contribute, if needed, to specifications and standards of other groups to facilitate the integration of smart cards within the IP connectivity landscape.

## World News In Brief

### **OFT Considers Action over Visa's Exclusive 2012 Olympics Deal**

The UK's Office of Fair Trading (OFT) is considering whether to take action over an exclusive deal between the London 2012 Olympics and Paralympic organisers and Visa, which will prevent fans using other cards to buy tickets. The deal means that UK cardholders will not be able to pay by card for tickets for the London 2012 Olympic and Paralympic Games, or withdraw cash at any Games sites, unless they have a card which runs on the Visa payment system.

### **Bell ID Launches PIN Host System for EMV**

Bell ID announces the release of a software solution to address easy and secure PIN management of EMV cards and applications within complex IT networks: ANDiS PIN Host System (PHS). ANDiS PHS offers centralised generation, enrolment,

change, (un)blocking and verification of the PIN. Furthermore, it enables multi-channel distribution via post, internet, SMS, ATM, branch and telephone (IVR), and enables banks to implement a more considered and coherent PIN management strategy. This is particularly critical when "offline PINs" on the chip and "online PINs" on central systems need to remain synchronised, where multiple applications are loaded onto the chip and where multiple channels can be used to block, unblock or change the PINs.

The solution follows the VISA and MasterCard guidelines for PIN management and can be used with a variety of HSMs from different manufacturers.

### **Visa Likely to Endorse Second iPhone Attachment**

Visa Inc. is likely to endorse another accessory that could turn Apple's iPhone into a contactless-payment device and may be planning to have an



exclusive agreement with the technology vendor, Wireless Dynamics Inc., NFC Times has learned.

The device, iCarte, announced last fall by the Canada-based technology company, offers full Near Field Communication functionality and embeds a secure chip that could store credit, debit or prepaid payment applications. NFC Times saw a brief preliminary plan from Visa calling for trials of the iCarte with the card network's payWave application starting in the late third quarter. It also mentioned "exclusivity" with iCarte. However, Visa declined to confirm the plan.

### **ABN AMRO's First Step towards New Payment Method**

The future ABN AMRO debit cards may have the innovative Maestro PayPass technology developed by MasterCard. These contactless payments are made without having to enter a PIN or swipe a card through a terminal.

### **GyD Ibérica produces Ferrari Card for Banco Santander**

GyD Ibérica, the Spanish subsidiary of security technology specialists Giesecke & Devrient (G&D) has produced the Ferrari credit card for Banco Santander in connection with the bank's sponsorship of the Ferrari racing team for the next five years. The card unites the images of Banco Santander and Ferrari, with red being the dominant colour. Santander's Ferrari card incorporates cryptographic technology and operates through an EMV compliant microprocessor chip placed on the card to protect users from fraud.

### **UK Police Arrest Teenagers Linked to £7.9 Million Cybercrook Forum**

UK police have arrested two teenagers as part of an investigation into what is believed to be the biggest English language cybercrime forum in the world. The two males, aged 17 and 18, were arrested by the Met's Police Central e-Crime Unit (PCeU) and remain in custody on suspicion of encouraging or assisting crime, unauthorised access under the Misuse of Computer Act and conspiracy to commit fraud.

The arrests are part of an eight-month investigation into a global Web forum with almost 8000 members that has seen officers so far recover more than 65,000 compromised card numbers, which at an estimated industry loss of £120 per card, could have cost up to £7.9 million, claims the PCeU.

### **Nokia Announces NFC-based Symbian Smartphones in 2011**

Nokia has been called upon to revamp its troubled smartphone division and announced that all Nokia Symbian smartphones will support NFC starting in 2011. Nokia veteran Anssi Vanjoki, who will head Nokia's new Mobile Solutions division starting in July, told an audience at the 10th anniversary meeting of the mobile-banking group Mobey Forum in Finland that Nokia remains committed to NFC. However, he declined to say which quarter the first NFC-enabled Symbian phones would arrive and was also not clear about the type of chips the phones would support to store payment and other secure applications.

### **Fraudsters Pocket \$10 Million in Four Year Micro-Payment Scam**

The Federal Trade Commission (FTC) has called time on an elaborate four-year old micro-payment scam that saw more than \$10 million in bogus charges placed on consumers' credit and debit cards. More than a million consumers were hit with one-time charges of \$10 or less, and their payments were routed through 16 dummy corporations in the US to bank accounts in Eastern Europe and Central Asia.

Most consumers either didn't notice the charges on their bills or didn't seek chargebacks because of the small amounts, which ranged from 20 cents to \$10. Consumers who called the toll-free numbers that appeared on their bills either found them disconnected or heard recorded messages instructing them to leave a message, but no calls were returned.

Find more information on <http://www.ftc.gov/>

### **MasterCard PayPass Records Double-Digit Growth in First Quarter**

MasterCard PayPass, a contactless payment service introduced by MasterCard Worldwide in 2004, recorded a double-digit growth of 49% in the first quarter ended March 31, 2010, compared to the same period last year.

Its group head, product and solutions, Asia Pacific, Middle East and Africa, Shuan Gaidan, said that 94% of PayPass users reported "very satisfied" or "satisfied" with the service in a study.

The MasterCard PayPass contactless payment feature allows cardholders to make simple transactions with just a tap of the card on a special terminal or reader. As of first quarter 2010, there are nearly 75 million PayPass cards and devices issued for use at around 230,000 merchant locations worldwide.





# Miracle Payments begin in India

By Suparna Sen, Smartcard & Identity News



Suparna Sen

Miracle Software Solutions, a growing IT software development company based in India has launched a unique payment card entitled 'Miracle Card' in the city of Pune, starting with the Aundh suburb. Miracle Card's are intended to be used by consumers as an alternative to cash to purchase small value items such as groceries, medicines and news papers from local shops.

Miracle Card cardholders are initially required to Top-up their card, which can be done either by visiting a registered seller or done online from another Miracle Card holder or by visiting the Miracle Software Solutions Office. You can top-up your card with the amount you desire but with a minimum top-up rate of 50 Indian rupees (70 sterling pence). Registered merchants must have an internet connection and a smartcard reader to facilitate transactions.

At a shop, payment works by a 'flash' of the Miracle card above the shopkeepers contactless smartcard reader. An image is then displayed on the shopkeeper's terminal, and the shopkeeper is responsible to authorise the transaction.

In addition, Miracle cards can be used to make internet purchases. When making an online purchase you verify your miracle card as genuine by providing numbers from a grid that you will find on the back of each card. Grid references are randomly generated by Miracle Software's back-end servers. The cardholder is verified by providing a personal transaction password.

Rakesh S. Jadhav, Head Business Development of Miracle Software Solutions, Pune, shares the reasons behind the launch of 'Miracle Card', its features and the future impact of the smartcard on the smart card industry.

## Why the name 'Miracle'?

Miracle as the name suggest is something that is transformational and this is what we would like to do. With our focus on innovation we work on newer technologies and have features that add value to the users and society. With the above idea, we believe we can definitely bring in the transformation /change in the way the purchasing is done.



## Miracle Card Front & Back

(The social/environmental message "Go Green, Save Trees" and "Save Tigers" is printed at the back of each card. Aircel, a leading mobile operator in India has partnered with WWF-India to help "Save Our Tigers" whose number is on the decline)





### **How many sellers or stores are currently offering this smartcard system so far?**

We have recently done a soft launch in Aundh in Pune. Currently we have 5 Sellers registered with us. This includes a Milk and Paper vendor too (Now, he will not have to go in person, to every house, to collect money for the monthly bills). There are few prominent malls who have shown interest too. The list will keep increasing.

We plan to cover Aundh and Baner in the next 3-5 months and increase the Seller network to 60+

### **What are the defining features of the Miracle Card scheme compared with other e-purse/ prepaid solutions?**

The below are the key features of Miracle Card vis-à-vis other cards.

- One Card for a Family. The Primary Card holder can share the card with his dear ones anytime. (The Primary Card Holder when gets his online account can upload the photographs of the persons whom he would like to use the card.)
- No Money Lost if Card is Lost! (Suppose a TOPPED UP card gets lost and worst case it gets into the hands of a miscreant who wants to purchase some items using that card. As soon as the card is flashed on the reader of the Registered Seller all the photographs linked to the card will be flashed on the screen of the Seller. The Seller can immediately stop the purchase.
- Very low TCO for Sellers (Just an Internet Connection and Reader!)
- A Powerful instrument for Branding and Advertising (Seller can have their Logo on the Card)

### **Few Prominent Security measures**

1. Photo ID validation
2. Hack proof card (Latest Contactless technology used)
3. Security Grid and Transaction password validation for Online Purchase/payments
4. No Credits involved in any part of cycle

### **What was the justification in having a high minimum top-up rate of Rs. 50? (Indians usually top-up phones by Rs. 10 and 20 and that Rs. 50 is a lot for many Indian people)**

There is no specific justification for having a minimum. Topup of Rs. 50. It will help the Seller to TOPUP rather than doing a TOPUP of Rs. 10/Rs. 20. Also, for the Buyer, it will help them to purchase 2-3 items where the amount may total to more than Rs. 20-30 most of the times.

### **Is the scheme aimed at a particular social class?**

No this scheme is not aimed at any particular social class per se. It is open across all the classes. It is the concept that drives in – A Family or an individual always does budgeting at the start of the month for his regular expenses and also keeps aside cash for the same. Hence, to facilitate cashless for these regular expenses we have introduced this card, so that it can help people across all classes.

To give you a specific example how it is being thought of to be used in higher classes in India– There is an up-market area in Aundh wherein there are typical business families living in independent bungalow/houses. They send their servants for general /regular purchasing to the stores. Here, we have proposed that every family can have one card and they can also upload the photograph of their servant. Once the Card is TOPPED at the start of the month, they do not have to give cash to their servants to get their regular items. It's safe and secure and the store can also be sure of the purchasing!

### **Miracle Software Solutions states in case a smartcard is lost or stolen, it can be blocked 'immediately'. But what about the balance that is on the card. Will it be refunded back to the card holder?**

A person may not necessarily hurry to block his card. Though his card is blocked his online account is still active. He can either opt for a new card by contacting the company where in the card will be TOPPED with the earlier balance. or irrespective of card lost, he can redeem his amount from the online account itself and ask to redeem. Company will pay back to the card holder





*The company's website: <http://flashtopay.com/>, under terms and conditions, it is stated that in case of loss, theft or damage of the Miracle Card, "you may lose any value which is stored on it in unless you have uploaded your photograph. A vigilant Seller can easily stop any misuse of card by verifying the photograph in the application against the person (miscreant) who is trying to misuse the card.*

**- Does it mean that uploading photographs of all those who use the card is optional and not mandatory?**

Yes, we encourage the Card holder to upload his/her photograph. There are cases where some buyers do not use internet connection but would like to use the card. In such cases we request for their photograph, we scan it and upload them against their card and registration in the system.

During our soft launch in Aundh in a prestigious society, there were some 8-9 people viz. from house keeping, electricity and plumbing dept who work in that society but used to do regular purchasing from the stores in that society. They do not have internet connection at home but we asked for their photograph and uploaded in the system.

**For sending gifts online, customers have to select the other Miracle Card holder's number, which means the receiver has to register with Miracle to get the gifts. Can't the process be simplified?**

Every Buyer (Customer) after enrolment is a registered Miracle Card user. The Miracle Cards can gift value points online only to a registered Miracle Buyer (Customer). The operation is similar to that when one is doing online payment to a registered Seller but here the Customer has to select the other Customer ( also registered with Miracle) for gifting value points.

**What about the change of address issue? If someone shifts to a new locality, how will he/she inform the company about the change of address? And, what's the procedure of doing it?**

Since every Card holder gets an online account, they can change details like address, etc in profile section itself of their account. But for people who don't use internet they will have to write to us.

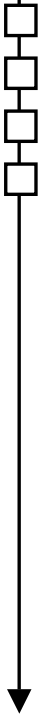
**The Miracle Card does not carry an expiry date. Why doesn't it have an expiry date?**

Typical life of a Smart card is 10 years (the life of chip in smart card). And hence by default the expiry date is 10 years from the date of enrolment (The card will also get deactivated when not in use for one year or more).

**What measures have Miracle Software taken to ensure successful promotion and take-up of the miracle card?**

We have clearly drafted our marketing strategy for Miracle Cards. As per our plan,

- For developing Seller Network own organisation's Marketing resources who would be involved in directly (explaining about the value proposition that Miracle Cards bring in to them, etc).
- For developing the Buyers network we would be conducting promotions and for which we have tied up with Local Advertising agency for promotion material and resource support. We are also in advanced stage with tie-up with Management institute in Pune wherein their management students can participate in promotion as part of their Marketing Project.





## ***TwinSet, a contactless HF/UHF smart card: Interview with Patrick Sure, ASK Transport and banking business line manager***

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



***Tom Tainton***

### **What is TwinSet?**

TwinSet is a contactless smart card that combines high frequency (HF) and ultra-high frequency (UHF) chips on the same card. Whereas before applications required two different cards to address identification issues, TwinSet allows three different chips to be embedded on the same inlay: A UHF chip for fast track access such as parking control, a HF chip for compliance with existing equipment for building access control, and a contact chip for logical access control. Contactless smart card holders have always been offered several cards to combine access control and identification services. TwinSet now combines features and applications that have previously been separated on several media and creates a new marketing tool for added value services.

### **What sort of markets will the card be penetrating?**

The electronic citizen identity sector, as well as eGovernment secure identity markets, is the perfect target for this contactless medium. ID cards, driving licenses and electronic passports comply with HF standards with a short reading communication distance while border crossing programs and outdoor access control systems have UHF frequency with a long range communication distance.

### **What are some of the key features of TwinSet?**

Well, TwinSet has a very long reading range of up to 5 metres as well as a low activation level. The unique radiation pattern allows the card to be read from all possible orientations and it's highly durable which reduces the risks of the card failing. TwinSet is a standard contactless card, ticket or inlay which can be easily implemented on existing contactless infrastructures.

### **How will TwinSet benefit the end user?**

TwinSet is all about innovation, and benefits users in a number of ways whether it be eIdentity or access control. For example, the dual technology product has been requested for applications where the holders of contactless banking cards with HF chips can be identified with their UHF chip and thus benefit for customized services when they access their bank. Of course, HF and UHF credentials must address performance, durability, privacy protection and security issues.

In another instance, TwinSet gives an employee or government agent the ability to access a parking area in UHF while driving through a large gate – without having to touch the card to a short range reader. He can then enter the secured access building using the very same card by placing it onto a short range reader, activating the appropriate advanced security mechanisms. Such a component can also be used as a car registration license and a driving license at the same time.

### **How does TwinSet keep sensitive information secure?**

TwinSet meets two requirements: securing documents while offering more services for the citizen. The security of documents is ensured through a chip and biometric feature. E-services for the citizen include strong authentication and e-government procedures. These applications require a short reading distance of up to 10cm. The contactless medium facilitates citizen mobility but at the same time places an impetus on secure identification.





## World News In Brief

### **Medical Insurer Warns 70,000 Georgians of Security Breach**

USA's largest health insurance company has warned 70,000 Georgians that their personal medical information, social security numbers and credit card data may have been wrongly accessed because of a website security breach.

Information was exposed for 5 months, said company spokeswoman Cindy Sanders. It affected applicants under the age of 65 who were applying for individual policies. She said the problem occurred following a faulty website upgrade in October last year.

Company officials believe most of the unauthorised access was accomplished by the attorneys for the user. But the company's investigation has yet to identify 10 computer addresses that accessed information. Sanders said some of that access could have been done by those with authorisation, such as insurance brokers seeking client information.

### **Wells Fargo deploys New Mobile Banking Applications**

US financial services provider Wells Fargo has launched new mobile banking applications for Android, BlackBerry and Palm handsets. In addition to Wells Fargo's existing mobile banking app, the three new Wells Fargo Mobile Banking apps are available via the Android Market on Android-powered devices, via the Palm App Catalog for Palm devices, and via a wf.com for BlackBerry smartphones.

Through Wells Fargo's Mobile Banking applications, customers can access their current available account balances, transaction history and credit card payment information. Customers can also transfer funds to their other accounts or to other Wells Fargo customers and pay bills. Wells Fargo Mobile Banking is integrated with each smartphone's built in GPS (Global Positioning System) feature so customers can search for the nearest ATM or Wells Fargo banking store. In addition, customers can receive alerts on their mobile devices.

The bank has also expanded enrolment options for its text banking service, which enables customers to view account activity, view credit card payment information and find nearby ATM locations.

### **Dutch Banks and Telcos Consider NFC Mobile Payment Launch**

Three major Dutch banks and three mobile

operators are considering a coordinated roll out of NFC-based mobile payment in the Netherlands. The banks - Rabobank, ING and ABN Amro and telephone companies - KPN, Vodafone Netherlands and Rabo Mobiel, are considering offering customers contactless payment, loaded onto SIM cards in NFC phones. The payment applications would support either MasterCard PayPass or Visa payWave.

### **Internet Authorities Adopt New dot org Security**

The company that oversees Web addresses ending in .org said that it was introducing extra security measures to guard against identity theft. .Org, which is monitored by the Washington-based Public Interest Registry, is the first generic domain name system (DNS) to adopt the extra measures, but others, such as .com and .net, are expected to follow.

The new DNS security measures will authenticate the origin of data on .org websites, ensuring its integrity, the Internet Corporation for Assigned Names and Numbers said during a week-long meeting in Brussels.

### **First Data and INSIDE Contactless Upgraded MasterCard NFC Stickers**

First Data Corporation in association with INSIDE Contactless has introduced the new MasterCard PayPass contactless payment tag for mobile phones. The new product is based on INSIDE's MicroPass payment platform and enables mobile phones with contactless payment capabilities. MasterCard PayPass mobile payment tag will be marketed and sold to MasterCard licenced financial institutions and card issuers.

### **IBM to produce ICs and PIV Cards for Infineon**

Infineon Technologies AG announced that IBM will manufacture Infineon-designed highly-secure integrated circuits (ICs) used for secure identification applications, including electronic passports compliant with international travel regulations and the U.S. Personal Identity Verification (PIV) cards. The planned production at IBM's chip fabrication plant in Burlington, Vermont, provides U.S. manufactured components for suppliers to U.S. government electronic identification programs.





# *The Future for Transport Smartcards - at The Waterfront, 27th May 2010*

*By Peter Tomlinson - Smartcard & Identity News*



**Peter Tomlinson**

This year's Waterfront conference on the subject of smart cards used in public transport within the UK (now with a nod to mobile phones as alternative carriers of the smart token) was held at the London premises of lawyers Bircham Dyson Bell. An appropriate venue: the new government is in place, relevant parts of competition law are both about to be reviewed and also currently being used in the study into the operation of bus services. There was an excellent team of speakers.

The keynote address was given by the recently appointed CEO of ITSO Ltd, Michael Leach. He introduced the company's developing strategy under the heading Developing a Roadmap for the Future of ITSO. Having now heard

Michael 4 times, in front of groups of people with differing affiliations, he is like an artist painting a complex picture that he revisits day by day altering it every time and steadily sharpening up the components. Featuring strongly is the evolution of ITSO: "into a customer-centric, service oriented organisation with the capacity and capability to work in partnership with our members". For the supplier community: "We must move all ITSO products onto the latest version of the specification quickly and cost effectively. This will require the development of new ways of working between ITSO and the supplier community and a move away from ITSO only providing a 'technical toolkit'." we heard, will be provision of training courses. Those are fine words, but they need anchoring in solid ground, both technically and given the new government's inheritance of an investment led Dept for Transport strategy, financially.

ITSO did not develop a comprehensive system-wide strategy for both user-facing functions and information security has been well known for 8 years. The owners and operators of the promised set of interconnected schemes were expected to get together and supplement the ITSO toolkit with common methods for ticket handling, journey management, service quality and information security. The Martini principle of an ITSO card being useable 'anytime, anywhere' stretched only to being able to load and use local ticket products wherever you are: no provision, either in card or terminal, for common methods for through ticketing or even for helping you to cope with local ticketing in the places that you visit. But make no mistake: the ITSO Environment's distributed architecture is a major achievement - multiple interconnected schemes and many product-led organisations (private or public sector), all being able to connect to any back office node and receive data from any other node, with over 20 back office systems now on the network or about to join. And the resulting schemes operate well when handling wrinkly passes (English National Concessionary Travel Scheme, ENCTS) or basic single operator or PTE period passes. Now we need to go beyond bus passes and rail season tickets - we have to transform historic ticket product environments into common electronic products rather than simply code them up as 2D barcodes. Now we, politicians and practitioners alike, need to understand that we are building a national asset, able to support a far wider set of individual citizen eServices than just electronic bus ticketing.

ITSO Ltd is in effect presiding over a co-operative, with public sector service operators, private sector bus/train companies and suppliers, all bound together. But it is also a company limited by guarantee, so in effect the company's Board rules. And, from the middle of 2009, the Board has been controlled by the votes of the Dept for Transport.

But ITSO Ltd is also the government's Regulator of smart media ticketing where that method uses the ITSO Environment of smart media, compliant equipment, the Virtual Private Network (VPN) that interconnects the schemes and the security key and permissions service. Regulation is by way of the ITSO Licence from DfT and the growing number of subordinate Licences granted by ITSO Ltd to the schemes - no statute law about this regulation beyond the competition provisions are going 'we heard' to be reviewed. In practice the Licensees are a self-regulating co-operative until ITSO Ltd intervenes. In this regulatory regime the supplier chain sticks out like a slightly sore thumb, because on the one hand supplier members of ITSO are not a party to operating via the Licences, while on the other hand they are suppliers to the Licensees - the ITSO community has to resolve that.





Another key presentation was about the Scottish Entitlement Card scheme, contrasting it with the failure of the English Local Authorities to develop either an equivalent national scheme or anywhere near a full set of local schemes using common methods. Sid Bulloch gave his view that effective use of smart technology for non-transport citizen services needs central co-ordination and core development finance. The lesson learned in that environment may well have a wider application to ITSO ticketing schemes, and so last year a very progressive Minister, Lord Adonis, committed DfT to taking the lead. Very importantly, we also heard from Scotland that those operating a scheme must have specific training: north of the Border over 70 people have gone through that training (would need 650 people in England for the same ratio of trained staff to population). Also repeated for us (by Mick Davies during his session) was Janice Morphet's reported comment on the aftermath of the English National Smart Card Project (NSCP, which some 7 years ago was promoted by the Office of a previous Deputy Prime Minister): "we let 1,000 flowers bloom". Mick observed: "but they died at the end of the year". Then, in his LASSeO role, he very quickly encouraged us to not despair in the task of improving service delivery by being smart.

Although not described on the day, the Dept for Work and Pensions with its 'Building a society for all ages' has been dipping its corporate toe into the citizen service smart card waters (see <http://www.hmg.gov.uk/media/33830/fullreport.pdf> - its intro page and <http://www.hmg.gov.uk/buildingasocietyforallages.aspx> which has been copied away to the National Archives for the time being). Although they were thinking of starting with further uses for the ENCTS bus passes, unfortunately DWP's effort turns out to be a 'learning on the job' exercise – it ought to be a training opportunity for businesses in the supply chain to thrive on.

Providing that this government does endorse the inherited smart media ticketing strategy, every local authority in England will within two years have access to a local or regional, public sector controlled, ITSO-compliant back office and smart media issuing facility. There should, by then also be a national agreement between ITSO licensed scheme operators on governance, including cooperative methods for managing information security and service quality. Michael Leach has several times reminded us that included in the ITSO Method is provision for third parties to make use of private data areas within the ITSO application area, and, if they wish, to provide their own local security environment within the national network – LASSeO is expected to coordinate development of common methods, but needs funding in cash and in kind. Thus, for the first time, discussions are now starting about a cost effective way for local citizen service schemes to piggyback on a national network. For local citizen services in environments such as libraries and third sector organisations, it should be possible to deploy low cost terminals at the point of service. On the few occasions that require the full panoply of the ITSO method, there should by then be an online service (a remote server based ITSO certified host) as part of the public sector ITSO-compliant facility to which the citizen service scheme is affiliated.

A footnote: struggling to be formed for the supply chain across the piece is a trade association, the Smartcard and Secure eServices Association (SSeSA). Currently squatting on AIDC's web site ([www.aidc.org](http://www.aidc.org)), it will soon have its own site at [www.ssesa.org](http://www.ssesa.org). For more information, contact [ssesa@aidc.org](mailto:ssesa@aidc.org).



## World News In Brief

### Visa CodeSure gets the Green Light

Visa Europe has announced a major step forward for online security. Following on from a number of consumer pilots and rigorous testing with European banks, Visa CodeSure is now fully available for commercial launch. By providing a Visa card with an alpha-numeric display, a 12-button keypad and battery embedded in the card, fraud online will be significantly further reduced. As the cardholder is required to enter their PIN for each online transaction, the Visa CodeSure card will prevent any unauthorised use. Visa CodeSure works on any Visa debit, credit, prepaid or commercial card.

Since its development in 2009, Visa and its partner, Emue Technologies Pty Ltd., have undertaken extensive pilot trials with eight European banks and their cardholders in a number of countries including the UK, Italy, Israel, Turkey, Switzerland and Germany.

Sandra Alzetta, Head of Innovation at Visa Europe commented: "The banks and their cardholder trials have shown an appetite for innovation and the broadening of a payment card's use. This exclusive Visa solution is an extremely convenient way to bring a similar level of security to payments online as we now enjoy on the high street with chip and PIN. The solution goes beyond just online and remote shopping but also allows organisations to use the card in place of other online log-in systems to access, for example, corporate virtual private networks (VPN)."

Visa has extensively tested the product's durability, safety, reliability and security before enabling it for commercial launch. The Visa CodeSure card offers banks a solution to fulfil all of their multi-channel

banking requirements. The use of PIN-generated one-time passcodes and using mutual authentication technology, will provide banks with an attractive solution that enables security and convenience in the same device - a Visa payment card.

### HID Global's OMNIKEY 6221 USB Reader combines Flash Memory with Contact Smart Card Technology

HID Global has announced a portable, dongle-sized USB smart card reader that includes a removable MicroSD flash memory slot and reader for subscriber identity module (SIM)-sized contact smart cards. By supporting flexible memory up to 32GB, the OMNIKEY 6221 USB reader is both cost effective and a future-proof investment for organisations looking to improve mobile document security.

"Data transported via traditional USB sticks or media such as CDs is vulnerable to unauthorised use through loss or theft, and electronic content distributed in this way can easily be pirated by simple copy and redistribution," said Alan Fontanella, Senior Director of Product Marketing for HID Global's Identity and Access Management business. "We've solved this problem by packaging flexible memory and contact smart card technology into a convenient and robust USB-based mobile-data security design that's easy for users to attach to a key ring and carry with them. The smart design also protects both the memory and SIM-sized smart cards under a removable cover to prevent their accidental loss."

## *Smart Event – The Innovation Forum for Mobility and Trusted Technologies & Services Sept. 21-24, 2010 -Sophia-Antipolis, French Riviera*

Smart Event is renowned as a major Industry & Research Forum in e-ID, e-mobility and Smart Security.

Thanks to its 3 international conferences – eSmart, the future of smart security technologies; Smart Mobility, building trusted mobile applications; World e-ID, the next e-ID management technologies & services - exhibition, live demos and other SIG meetings, Smart Event has become a key meeting place for world-class researchers, innovators, developers and business decision-makers. Joining Smart Event offers unique opportunities of knowledge-sharing, learning, and networking: 150 speakers, 700+ participants, 40+ countries represented...

More at [www.smart-event.eu](http://www.smart-event.eu) – Contact [Lperron@strategiestm.com](mailto:Lperron@strategiestm.com)



# SMART EVENT '10

The Innovation Forum for Mobility  
and Trusted Technologies & Services

September 21-24, 2010 - Sophia-Antipolis, French Riviera



<b>e-Smart</b> The future of Digital Security Technologies	<b>Smart mobility</b> Building Trusted Mobile Applications	<b>World e-ID</b> The next e-ID Management Technologies & Services	<b>Smart University</b> State-of-the-Art ICT Knowledge & Training	<b>WORKSHOPS &amp; SIG MEETINGS</b>
---	---	---	--	-------------------------------------



## Join IT mobility and security key event!



Smart Event gives the industry and research the opportunity to explore and discuss the dynamics of innovation in three interconnected areas: digital security, e-mobility and e-ID.



Taking place annually in September in the French Riviera, on the Sophia Antipolis technology park, Smart Event offers:

- 3 international tech conferences: **e-Smart**, **Smart Mobility**, **World e-ID**
- 18 high level trainings: **Smart University**
- exhibition, live demos and other SIG meetings



The growing participation of world-class researchers, innovators, developers and business decision-makers shows a clear recognition: attendance figure has nearly doubled over the five past years to now reach 700, coming from over 40 countries.

This success relies on a combination of four features that make this event unique:

- live exchanges across the full value chain
- balanced mix of technology between R&D and strategy
- large choice of contents on a single platform
- high level trainings

### Media & Press Partners



Attend Smart Event 12<sup>th</sup> edition and enjoy its multiple opportunities of knowledge-sharing, learning, and networking: 150 speakers, 700 participants, 40+ countries represented...

We look forward to welcoming you.

Detailed information and programs  
on [www.smart-event.eu](http://www.smart-event.eu)



organized by

