

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

Email: 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, Holly Sacks, William
Holmes, Brian Berger, Stephane Fymat,
Suparna Sen

Photographic Images - Nejrion -
Dreamstime.com

Printers – Hastings Printing Company
Limited, UK

ISSN – 1755-1021

Disclaimer

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

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

© Smart Card News Ltd

Our Comments

Dear Subscribers



Patsy Everett

Well we are approaching that time of the year again when the rail strikes take over in Paris and of course that means it's time for Cartes (November 17/18/19th). I can't believe another year has gone by but just in case you have forgotten it's now pretty urgent to book the planes and hotels.

It's tempting to ramble on about the UK's indecision over the National ID Card, not to bore you but it's off again until the Labour party gets re-elected or the Tories replace them in which case we know the ID card is doomed. But really it's a long way from our day-to-day concerns and trips to Paris always remind me of the year I got mugged, my bag was stolen and in an instance my life came to a halt. No money, credit cards, mobile phone, driving licence, diary (PDA of course), keys, glasses, business cards, the list goes on. If it's happened to you you'll know what I mean but for everybody else please don't put all your eggs in one basket.

This is identity theft in one swoop and believe me the problems of closing and replacing credit cards and the like is not an experience you will want to repeat.

So the salesman told me and I'm sure I'll get more at Cartes, just put everything into your phone. You'll know your phone is missing in 20 minutes but the wallet takes 20 hours to spot. In my case it was seconds but let's ignore that, do I really want everything in one place?

Does this compare to the Fort Knox Paradox? Is it better to keep all your gold in one place or is it better to store it spatially distributed? Assuming we have the same total number of defenders in each scenario, which is the better game plan? Let's assume we have 1000 bars of gold and 1000 defenders. At the two extremes we have 1000 defenders at Fort Knox or 1 defender per bar if they are totally distributed. But of course to make the game more interesting we assume that there is a probability of knowing where the gold lies within the two extremes, totally certain for Fort Knox and highly uncertain for total distribution. In order to win a bar of gold you must have more attackers than defenders and know where to go, where would you keep the gold?

Normal human behaviour has answered this question in the sense that most of us store our money in the bank and remove it in little lumps as and when required. The duty of the bank then is to identify and authenticate us before handing over the cash. Here's where we break with the paradox in the 21st century, is it possible for a small number of attackers (perhaps just one) to hoodwink a large number of defenders (at the bank)?

In my bag there was two credit cards both EMV enabled for Chip and PIN. Just a note of caution here readers, the debit card is effectively providing access to your current bank account, if an attacker can hoodwink the bank then an attacker might empty your bank account. In the case of a credit card the attacker will be creating a liability on a post-paid account to be settled at the end of the month. Is it easier to get the bank to put money back into your current account or is it easier to refuse to pay a credit card bill in the event of an attack?





Having recovered from the mugging and found my way to the Police station in Paris, no mean feat when everything has been stolen, the time had come to start shutting down all those financial cards and of course the mobile phone SIM. How do you do that when you have lost everything? To cut a long story short friends and family came to the rescue, on my own it would have been impossible.

It took about an hour before I was able to start notifying the banks about my problem but even in this short time my card was used to make payments as it happens for petrol at a garage nearby. In those days the merchants didn't check the chip and PIN on foreign cards, they just used the magnetic stripe with a signature.

Now you are all probably feeling comfortable that these days everybody does Chip & PIN so if you lose your card it won't matter. Not so I'm afraid, the USA does not comply with EMV although curiously Visa and MasterCard are American companies. So any attacker stealing your card can have it being used (as a counterfeit) in the USA using a magnetic stripe probably within minutes. The internet is of course worse, all we need is the card number and the security code from the back of the card.

So what happens if all my cards are in the phone which has just been stolen? It's going to be down to the security of the phone and how the financial application is stored on the phone. I think I'll hang on to my physical cards a bit longer but I just won't keep them in one place. NFC still seems a long way off but if and when it comes what would I do with it? Enjoy our lead article on NFC this month.

Patsy.

Contents

Regular Features

Lead Story	1
Events Diary	3
World News In Brief	5,13

Industry Articles

The smart way to safer hospitals	6
One Time Password	
- NOT just another application on your cell phone	7
Safely Adding Smart Cards and Other Security Monitoring Devices	9
Privileged and Shared Accounts	
- Why You Must Close this Security Hole	12
India's UID Project to help the poorest	18

Events Diary

October 2009

6 – 8	ISSE 2009, The Hague, Netherlands - www.isse.eu.com
13 – 15	8th Asian High Security Printing Conference, Beijing, China - www.bccspc.com/2009/EN/
20 – 22	Biometrics 2009, London, UK - www.biometrics.elsevier.com
20 – 22	RSA Conference Europe 2009, London, UK - https://365.rsaconference.com/index.jspa
20 – 22	Urban Transport World Europe 2009, London, UK - www.terrapinn.com/2009/ute
26 – 27	Mobile Money Transfer 2009, Dubai - www.mobile-money-transfer.com
28 – 30	8th Annual Smart Cards in Government, Washington DC, USA - www.smartcardalliance.org/pages/activities-next-conference

Source: www.smartcard.co.uk/calendar/





.... Continued from page 1

chip embedded in the handset. This would provide control of secure chips and application processors and 'ensure that consumers can reap the benefits and of mobile payment services as soon as possible.'

Chief Marketing Officer of GSMA, Michael O' Hara said that by signing up to the 'Pay-Buy-Mobile' scheme, handset manufacturers would avoid fragmenting the market, and benefit from introducing a new attractive service for users – boosting sales at a time when the industry forecasts are looking increasingly bleak.

The 'Pay-Buy-Mobile' trials were conducted in many countries including Australia, Taiwan, USA, and France, all of whom enjoyed strong results and positive feedback. In South-east Asia, 80% of the users were satisfied with the security of the service, while in the 'Payez Mobile' trial in France, 90% of consumers found contactless mobile payments 'easy to use' while 80% merchants welcomed the 'speed and cutting edge appeal' of contactless payments.

The new payment channel is wholly dependent on the availability of NFC-enabled handsets and device manufacturers incorporating Single Wire Protocol and NFC features as standard. While the GSMA have suggested that collaboration with vendors would help speed up demand, and were confident that a set of minimum requirements will accelerate the delivery of these handsets to the marketplace, it's all gone a little bit flat. We're fast approaching autumn and there's barely a fully functioning NFC phone in the market. So what's happened to the GSMA 'Single Wire Protocol' dream?

No one doubts that NFC is a useful application. Wave your phone by a door and it opens, near a till and your bill is paid. But much of the technology requires a secure module that doesn't necessarily need to be the SIM. The capabilities of a SIM have greatly advanced in the last few years, with multi-megabyte capacities and fast processors crammed into the package. However, getting payment for this potential hasn't proved as simple. Even the emergence of a dynamic interface such as USB has done little to whet the appetite of the operator, despite USB adoption leaving one pin free on the SIM face, a single wire that allows the SIM to communicate with NFC hardware stored on the handset.

They're more than content to see the secure module embedded in the handset, much like Nokia's 6131 NFC mobile, one of few NFC-enabled handsets on the high streets. While GSMA claim that all and sundry have signed up to make Single Wire Protocol handsets, the reality is that until networks demand it, the manufacturers will be delighted to keep NFC under their full control.

The availability of handsets is minimal, with exceptions such as the LG KU380 and the Apple iPhone, a handset that harnesses RFID to indulge in bizarre activities like knocking over small objects when the device is swung in near-proximity. For Swedish telecom giants, Ericsson, it's a year later than expected. The company's Vice-President, Håkan Djuphammar promised that by next year (2010) every new handset that's sold by Ericsson will possess NFC capabilities.

It's the industry to decide as to how much control the mobile operators should hold over the secure element of the process. SIM manufacturers and mobile operators are pushing for the SIM to play a part in all areas of communication that the NFC chip has with other chips in the phone, to the extent of giving the SIM the authority to reject unfamiliar applications. Subsequently, they're urging the European Telecommunications Standards Institute (ETSI) committee to adopt this particular model.

On the other hand, the handset manufacturers aren't so enthusiastic. Nokia, a key player in the market, only wants communication between the SIM and the NFC chip, and rejects suggestions that the SIM should be involved in applications stored on other secure chips. And while mobile operators rush to ETSI to fight their corner, Nokia has turned to the NFC Forum, an organisation that it helped to create. If Nokia continues to stand its ground (which it inevitably will), the squabbling within the industry will only serve to cause further delays to widespread usage, bump up prices, and dramatically impact the time to market of NFC handsets. The inability to agree on standards, and the lack of a solid business case to justify expenses have contributed to the limited availability of NFC handsets, and the continuing struggle for control of different parts of the supply chain. In the short term, vendors such as INSIDE Contactless have developed a stick-on NFC device that can be attached to a mobile phone thus enabling access to GPS, transit and smart postering solutions. In the longer term, SIM manufacturers may be forced to offer their services as a trusted third party. In the mean time, the rollout of mobile payments is edging ever closer. The specifications are completed; the trial results are in and the outcome is successful. All we're waiting on now is the handsets. But that's easier said than done, no doubt.

By Tom Tainton, Smartcard & Identity News



World News In Brief

Google working on Micropayments System to help News Media charge for Content

Google confirmed it's planning to roll out a system of micropayments within the next year for the Newspaper Association of America. The revelation was made in a Google document, which was first publicised by the Nieman Journalism Lab, indicating that the micropayment system will be an extension of Google Checkout, a payment system that Google rolled out in 2006 and positioned as a competitor to eBay's PayPal service. The document was forwarded by Google to the Newspaper Association of America in response to the association's request for paid-content proposals to several technology companies.

The micropayment system would enable payments from pennies to several dollars by aggregating purchases across merchants. Google, which has long relied on advertising for the over-whelming majority of its revenue, said that it believed that paid content could be a good complement to advertising. Google said: "While we believe that advertising will likely remain the main source of revenue for most news content, a paid model can serve as an important source of additional revenue." They believe that a successful paid content model can enhance advertising opportunities, rather than replace them. The micropayment system, which is still in the planning stages, could be available on Google and non-Google properties in 2010.

However, The Guardian Newspaper (UK) has taken a poll on preference of subscriptions to micropayments in September, and the poll revealed that a long-term subscription and not micropayments is the most attractive option to consumers.

BIO-key Biometric Technology selected as part of the Next Generation FBI AFIS System

BIO-key International, Inc. announced a contract awarded to them by Lockheed Martin to provide fingerprint identification technology for the FBI's Next Generation Identification (NGI) system. The technology will be based on the fusion of BIO-key and MorphoTrak biometric algorithms.

As Mike Depasquale, the CEO of BIO-key said: "This is the most important award the company has ever received and it may be the most important biometric contract ever awarded.

Mira LaCous, Vice President of Technology and Development has also said that BIO-key's core algorithm accuracy and image enhancement/correction solutions will bring in major improvements to the FBI's current system.

ZK Software launches "The first MultiBio Face and Fingerprint Embedded Device in the World"

ZK Software, a China based leading manufacturer of fingerprint biometric readers, released their new product line of multi-modal biometric identification devices called the iFace series. With the help of this MultiBio Face and Fingerprint Embedded reader, users can be identified by their Face and/or Fingerprint and/or RFID and/or PIN.

iFace provides both Time & Attendance and Access Control functionality and it includes:

- Fingerprint sensor
- Infrared, night-vision camera for facial recognition
- Large colour touch-screen display
- TCP/IP
- Wi-Fi communication
- An internal battery-backup

In addition, this biometric reader can detect the same face with 15 different facial expressions and is unaffected by varying light intensity. iFace can be used in high-security situations, which require more than one mode of biometric authentication (i.e. in airports, banks, prisons, schools and hospitals).

NFC Mobile Payments to Exceed \$30bn by 2012

An analysis from Juniper Research of the NFC opportunity forecasts that the application of NFC as a mobile retail-marketing tool via coupons and smart posters will support the growth of NFC mobile payment transaction values from \$8bn in 2009 to \$30bn within three years.

NFC report author Howard Wilcox stated: "Many people focus on the use of NFC for payments but in fact it is poised to revolutionise the way many people shop too." He also said that the ability to tap smart posters and receive coupons and product information also presents new channels to market for merchants. Even vendors see widespread availability of NFC phones in future.





The smart way to safer hospitals

By Holly Sacks, Senior VP, Marketing and Corporate Strategy, HID Global



Holly Sacks

Over the past few years, the healthcare sector has become increasingly dependent on information technology. Contactless smart card technology has been used many years in other industries, and is now helping to solve some longstanding thorny issues in the healthcare sector: safeguarding patients and staff and protecting confidential patient information.

Hospitals in Scandinavia were early adopters of this technology, and Germany has recently issued healthcare smart cards to its entire 80 million-strong population. In the UK, many hospitals are now waking up to the benefits of using contactless smart cards to control physical access to their buildings and logical access to the IT systems that house confidential patient data.

In the past, it was relatively easy for an intruder to walk unchallenged around a hospital, accessing areas meant only for authorised staff. In rare cases, this led to security breaches where babies were removed from paediatric wards. Contactless smart cards are addressing this physical access problem by using encryption to offer differing levels of building access to certain staff. For example, a cardio-thoracic surgeon would require access to the operating theatre, while a registrar might need access to all the wards in the hospital.

Medical professionals can also use their smart card to access sensitive patient data on a network. Thus, using a smart card for logical access can also create efficiencies in terms of time. If a doctor can access crucial IT systems with just a smart card, this saves on time wasted in remembering and entering usernames and passwords and frees up more time for patient care. It also helps healthcare professionals to demonstrate that they are storing and managing patient details in a safe and secure way to comply with the Data Protection Act.

Smart cards can come in contact or contactless form, and can offer three levels of security: single, dual or three-factor authentication. With single-factor authentication, using the card on its own will give access to a system or open a door. Dual-factor authentication - the most common level of smart card authentication in UK hospitals - adds on an extra level of security in the form of a PIN code. Three-factor authentication goes a step further, using a PIN and an extra security measure such as a biometric scan. Contactless smart cards are traditionally used for physical access control and are now being adopted for logical access control as well.

One surprising area where this technology is making an impact is infection control. We've all seen the bottles of antibacterial hand gel that now stand at the doorway to every hospital ward, and no one can have missed the government swine flu posters that landed on every doormat across the country. Contactless smart cards - where the card is passed in front of a reader device, are playing a key role in limiting this spread of infection. After all, if your pass card never touches the reader, it can't spread germs.

With this many advantages, adopting contactless smart technology seems like a no-brainer. But some hospitals are still using the most basic form of secure access control: the magnetic stripe - or 'mag-stripe' - card, where magnetic data is stored on the back of the card.

While mag-stripe cards are cheap to produce, they can end up more expensive in terms of maintenance. Magnetic stripe cards are contact cards that can collect any debris and inevitably ends up inside the reader and on its contact pins. They are also susceptible to magnetic interference and wear and tear. This type of card is also very restricted in terms of its data storage capacity compared to a smart card, some of which now have up to 164K of memory. But perhaps their biggest disadvantage is that they are very easy to clone. You can even buy a mag-stripe reader from a high-street store and use it to create an unlimited number of clones.

It's fair to say that the cost of upgrading to contactless smart cards can be a barrier to deployment for some hospitals, where funding priorities can mean that management has to choose between upgrading physical and logical access systems and having another 30 patient beds. On the other hand, is it really possible to put a price on effective infection control or security in a maternity ward?

Thus, contactless smart card technology can offer outstanding value to the healthcare sector, saving time and money, protecting patients and staff and safeguarding their personal data. Portable and secure, contactless smart cards are fast becoming a valuable tool for safeguarding physical security and guaranteeing the privacy of sensitive electronic information.





One Time Password – NOT just another application on your cell phone

By William Holmes, Consultant to GO-Trust



William Holmes

Suddenly there has been a rush to add numerous applications to Cell Phones and PDA's. These applications are most frequently social or inconsequential and are also most never business 'Mission Critical'. Mission Critical applications need something more than a software applet that runs on the cell phone (in the open), they need special secure hardware so that critical keys, seeds and calculations are never accessible and certainly never in the open.

But let's start at the beginning and briefly describe the One Time Password (OTP) concept. Static (user generated) passwords are vulnerable. The vulnerability could be something as simple as someone looking over your shoulder or a more sophisticated method like keyboard logging. Passwords may be left inside memory after logout and can easily be found by scavenger bots. Deduction based on the users preference and personal records (birthdates, pets' names etc.) and brute-force attacks are just a couple more of the methods to find out fixed passwords.

Then the almost obvious idea arrived, if you use a password only once it does not matter if it has been copied or deduced, the previous password has no value – One Time Passwords were born. As they are only valid for a single session or a single transaction they are not vulnerable to replay attacks. There are three common types of OTP algorithms:-

HOTP – Where the H stands for HMAC, which in turn stands for Hashed Message Authentication Code. This is a seeded algorithm that generates a series of unique passwords. The sign-on server is always looking for the next password in the series. As the algorithm uses a crypto hash function it is believed to be impossible to reverse engineer the series to calculate the next password.

TOTP – Where the T stands for Time-based. In this algorithm the real-time clock is an additional parameter. Generated passwords are only valid at a specific time and only for a defined time period.

OCRA – Where the acronym stands for Onetime Challenge Response Algorithm. In this algorithm the addition factor is a challenge code from the logon server.

Great idea, but there is an obvious snag; OTPs cannot be memorized by human beings and preprinted sheets of future passwords defeat the whole concept of unpredictable password series. The next obvious step was the development of standalone key generators. These key fobs and less frequently smart cards became very popular with financial institutions and multinational corporations. Simple to use and many times more secure than personnel remembering (weak) passwords.



Looks like a good solution but there are some downsides. The key fob is yet another thing to carry but more seriously it only has a two to three year battery life. Before that time is up there needs to be a total redeployment, the replacement of every key fob in the field! Smart cards are easier to carry, do not have batteries, but do require either a portable reader or a conventional smart card reader on a PC or notebook.

To recap, OTP is many times better than static passwords, but extra hardware is required to generate secure passwords, the current key-fobs and smart cards are not the ideal solution.





Last year in June 2008's SCN newsletter (<http://www.smartcard.co.uk/archive/>). I wrote about 'Smart Card Security for People and Applications on the Go' which detailed the latest technology to embed smart card chips in MicroSD memory modules delivering smart card, hardware based, security for applications on cell phones and PDA's.

This technology has moved on very quickly in the twelve months since that article with many new smart cards being available in the microSD form factor delivering new smart chip, hardware based, security to cell phones and PDA's. One chipset that has caused particular interest is the microSD JAVA, with EMV, Common Criteria compliance and FIPs certification. The flexibility of such a secure environment lends itself to an array of secure applications on mobile phones and PDA's, some of the more interesting include mobile TV, banking and secure VPNs.

Back to OTP, the microSD JAVA is the perfect platform for secure one time password generation. It is fast, easy to install in any phone or PDA with a microSD memory slot and it is completely secure. Unbelievably the microSD with the embedded JAVA chip still has up to 4 GB of flash memory most available to the user only a small amount is used to store the phone side display application. Installing the OTP application on your phone is simple:-

1. Insert OTP microSD into mobile phone SD slot.
2. Use the file explorer or a similar tool to locate the memory card.
3. Select the correct folder for the platform (Blackberry, Symbian, Mobile, Android) in the memory card.
4. Execute the file in the selected folder.
5. The Mobile phone will install OTP application and will be ready to run.
6. And running the application is even easier:
7. Select the OTP application from the main menu.
8. Select Generate OTP Value.
9. Input the PIN for the smart card chip embedded in the microSD.
10. The OTP is generated.



OTP Application Menu



The OTP Value

So why does it make sense to move the OTP generation to a Mobile Phone or PDA? Firstly the security is as good as it gets. Smart Card hardware security with EMV, Common Criteria compliance and FIPs certification. It is always right next to you, nothing else to carry or remember. There is no need to change your OTP system every two to three years as part of a mammoth redeployment of units. It follows your lifestyle, change your phone and the OTP application on the microSD moves with you. You can even use a full size SD adapter and run the OTP application on your desktop or notebook. The OTP application has not robbed you of your extra memory; the 4Gb of flash memory is still there on your phone for music, photos or data.

OPT will be the most secure, most valuable and most important applications on your cell phone!



Safely Adding Smart Cards and Other Security Monitoring Devices to Enterprise Networks

By Brian Berger, Trusted Computing Group, and executive vice president, Wave Systems



Brian Berger

With security being among the highest concerns for enterprises of all sizes, users need to be aware and take advantage of the latest technologies. This is especially important when a combination can either improve or degrade security. From a computer perspective, the hardware technology developed by the Trusted Computing Group (TCG), a not-for-profit industry standards organization, provides a basis for establishing trust in portable and desktop PCs. This technology is also used in servers and other computer hardware including portable hard drives.

Called a Trusted Platform Module (TPM), the TPM is typically a microcontroller or application specific integrated circuit (ASIC) similar to the chip in smart cards. The TPM can provide strong authentication for remote access, handle Public Key Infrastructure (PKI) key management and exchange, work in cooperation with smart cards and fingerprint scanners and more. IDC data in 2008 showed that over 150 million notebooks and desktop PCs had a TPM. The market research firm predicts the TPM market will increase to more than 250 million pieces shipped in 2010 indicating an attach rate of more than 90 percent for notebooks and desktop PCs.

Working with smart cards and other security monitoring devices, the TPM has a defined role in multi-factor security. For a typical multi-factor security consisting of what I know, what I have and who I am, the ubiquitous TPM provides a more secure and simplified approach to passwords and PINs that the user knows.

The TPM, Smart Cards and Biometrics

From the improved security perspective, the linkage between smart cards and biometric and other security monitoring devices to the TPM has been possible for many years. As shown in Figure 1, this is the second level of improvement beyond simple user ID /passwords and PKI/ token access in data and network security. The TPM provides a foundation for more advanced security features.

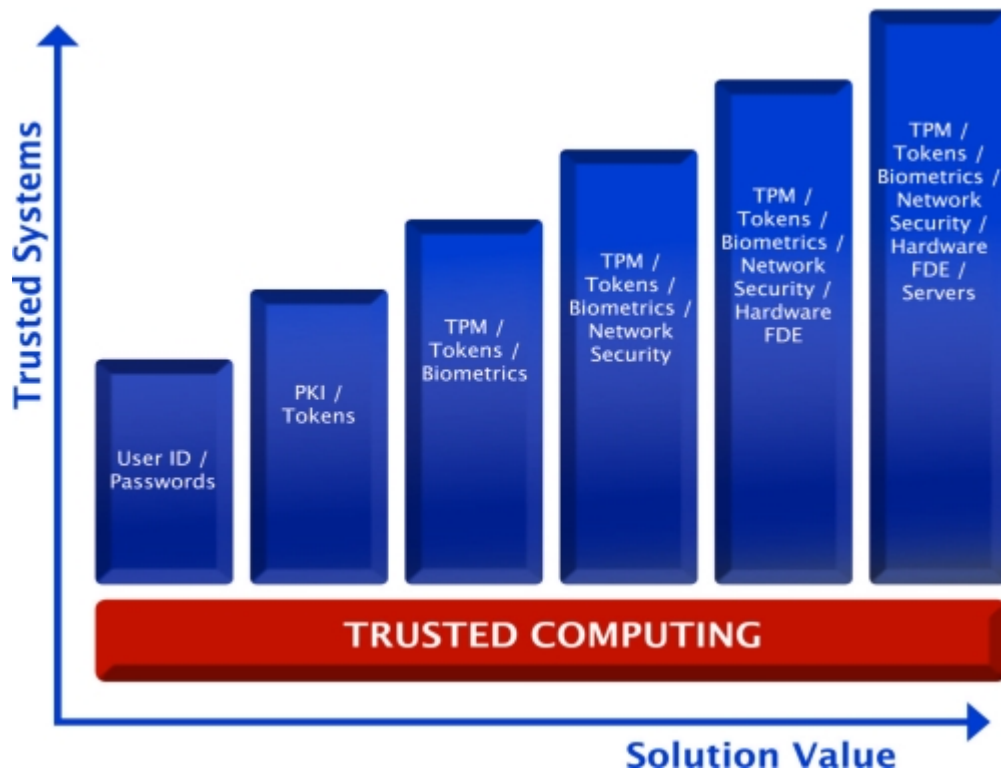


Figure 1. System trust and its inherent solution value increase with added security functions enabled by the TPM.





Both hardware and software have been developed by biometric security suppliers that link to the computer's TPM. For example, AuthenTec's AES1610 slide sensor (Figure 2) takes advantage of the computer's TPM for protection from startup to sign off. One option is to enable the TPM to protect the user credential encrypted and persistently protected by the TPM. The fingerprint sensor works with the TPM, to enable TPM protected pre-boot authentication that provides authorized access in both fingerprint and user ID/Password mode. The TPM securely "locks" biometric data to the user's PC. In addition, the sensor's flash memory provides flexible storage options for a TPM signed matcher and encrypted fingerprint templates.

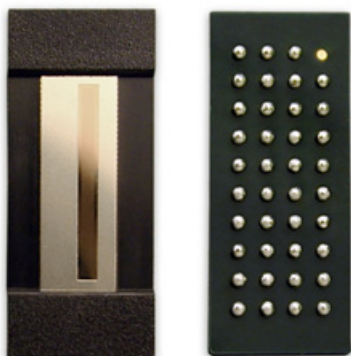


Figure 2. The 12 x 5-mm AES1610 fingerprint sensor can easily be designed into laptop and other PCs. Source: AuthenTec.



Figure 3. Working with the TPM in enterprise class laptop PCs, UPEK's USB-connected Eikon To Go provides a fingerprint biometric solution for improved data security. Source: UPEK.

Other biometric security suppliers have also leveraged the TPM's capabilities for improved security. UPEK's biometric fingerprint security technology complements the multi-factor authentication possibilities offered by the TPM. With its Digital Identity Engine, UPEK provides a secure environment for processing biometric operations for additional security. UPEK's Secure Endpoint solution (See Figure 3) supports multiple tokens with multiple RSA SecurID seeds or factory-encoded random keys.

In 2009, Dell Computer in conjunction with WaveSystems developed software to support their Universal Security Hub (USH) for enhanced security. The USH uses the TPMs capabilities and Dell's ControlVault (CV) for storing a variety of authentication data including passwords, and enrolled BIO templates, enrolled HID card serial number, enrolled SC/CSC data and more. Instead of password only preboot, the USH/CV allows users to add biometrics, smart card and contactless smart cards including the Dell Java Smart Card for single sign-on into Windows that includes a self-encrypting drive (SED) enabled and locked. Wave System's provides single sign-on (SSO) software support for the USH, CV, TPM and SED capabilities in a seamless multi-factor authentication solution.

The Dell ControlPoint Security Manager, a collaborated effort between WaveSystems and Dell, simplifies access to mobile security features and data management by collecting hardware and security settings using a single user interface. In addition, an embedded multi-technology contactless smart card reader allows users to carry a single card that can be used for both logical and physical access control.

For Dell computers without the USH, the EMBASSY Trust Suite for Dell from WaveSystems simplifies preboot authentication for fingerprint, smart card and contactless smart cards as well as automated secure password management and PKI support for smart card and TPM cryptographic services and more.

A Security Protocol for Security Monitoring Devices

From the potential for a degraded security situation, as smart cards and other personal identification hardware are connected to the network through remote entry points or unmanaged endpoints, the likelihood of the complex node being the entry point for malicious software increases. To address the associated connectivity and security issues, TCG's Trusted Network Connect (TNC) workgroup extended its network access control. Using an interface (IF) protocol called IF-MAP, physical security devices can safely be connected to networks and avoid unmanaged endpoint problems. IF-MAP helps security systems share information.

With IF-MAP, security monitoring and classifying devices or sensors and flow controllers that make and enforce decisions through a Metadata Access Point (MAP) or central database enable secure connectivity. Normally, unmanaged endpoints do not have any security software like antivirus, anti-malware and others to verify the safety and status of the device. An unmanaged endpoint can be connected easily and securely to the enterprise intranet with IF-MAP providing automated access and monitoring throughout the device's lifetime.



An example of an unmanaged endpoint provides real world context to the potential problem that IF-MAP prevents. In 2008, digital picture frames with a network connection were shipped from China with a virus embedded in the ROM software. The embedded device problem resulted from the lack of secure IT processes at the supplier. A virus attached to the frame's memory contained four malicious files with an autorun file to execute them. As a result, Windows based systems were at risk for attack from the malware.

The embedded memory virus problem can occur in any device with embedded memory. If a security device with an embedded problem is connected to the enterprise network, it could infect the entire network. To date, these endpoint products have not been a concern but it only takes a single problem to generate a lot of bad publicity and serious damage to a company. The IF-MAP can prevent connecting an endpoint with this problem to the enterprise network.

RFID and the Enterprise Network

Radio frequency identification (RFID) technology is a physical security technique that will increasingly connect to enterprise networks. RFID tags have been extensively used to track shipments in the supply chain, monitor inventory in warehouses, and as anti-theft devices on goods in the retail sector. The technology is predicted to be used increasingly in health care to locate and protect expensive diagnostic equipment. The world's largest RFID network is the U.S. Department of Defense's In-Transit Visibility network. This network tracks about 35,000 items daily across more than 4,000 locations and 40 countries. In most of the newer and many of the existing applications, data security and privacy are major concerns.

In their 2005 paper *Privacy For RFID Through Trusted Computing* researchers addressed the issue of providing privacy protection for RFID to comply with privacy regulations using the TPM. They concluded that remote attestation capability of the TPM enables any party to check that the reader will respect a particular privacy policy.

More recently, in the December 2007 white paper, *Trusted Networks: Design of an RFID Trusted Reader (D4.4.1)*, partially funded by the European Union, the authors developed a secure RFID reader that uses the TPM's capabilities for enforcement, attestation, secure storage, unique identity and open services platform. As a defined task in the BRIDGE (Building Radio frequency IDentification for the Global Environment) Project, the goal of the Trusted RFID reader development was the secure sharing of supply chain information among different parties in the supply chain. As shown in Figure 4, the Trusted RFID reader has similar elements to the 2005 Trusted RFID design including the TPM.

RFID technology, even Trusted RFID output linked to an enterprises network can benefit from the increased security that the IF-MAP network protocol can provide.

Conclusion

All of the increased security involving TCG's TPM, requires users to turn on the TPM in their computer. Since the TPM ships in the deactivated mode it must be activated. However, this is a rather straightforward process especially for IT administrators.

The TPM is a key building block in computing security that has help from an increasing number of other security technologies such as the TNC IF-MAP protocol. As security tools increase, the standards developed by TCG will allow the integration and safe use in both physical and data security applications.

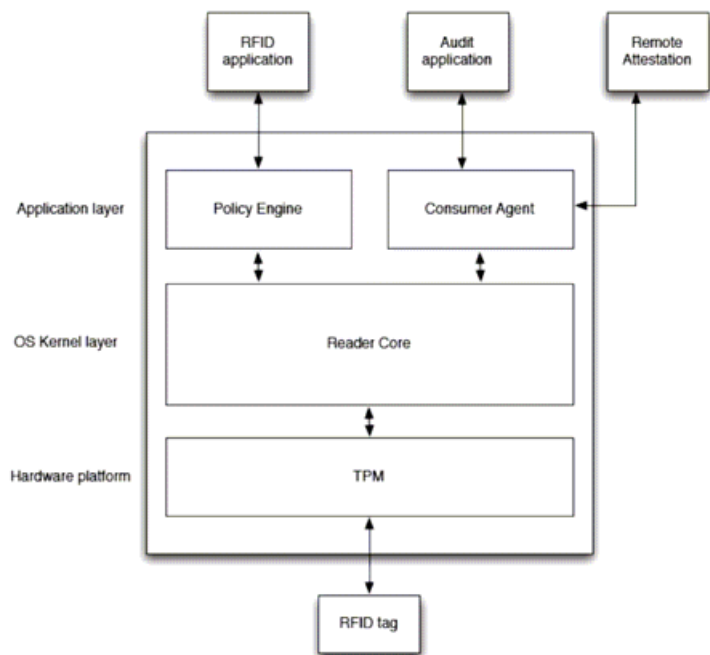


Figure 4. The TPM is an essential technology in a standalone Trusted RFID reader.



Privileged and Shared Accounts – Why You Must Close this Security Hole

By Stephane Fymat VP of Strategy and Product Management, Passlogix



Stephane Fymat

One only has to consider the case of Jérôme Kerviel, the rogue trader at French bank Société Générale, who used multiple shared passwords and accounts to execute fraudulent trades, to appreciate the risks shared account logons pose to the modern organisation. Kerviel's actions cost the bank €4.9bn and serious ramifications were felt across the global financial markets.

The City of San Francisco found itself in a similar situation last year when a disgruntled network administrator, Terry Childs reset all administrative passwords to the routers for the city's wide area network. His actions prevented administrators from managing the system as he essentially held the City to ransom.

What these two stories demonstrate is that failing to manage shared passwords adequately can expose organisations to serious vulnerabilities, particularly in the case of privileged accounts where a disgruntled employee could potentially have the power to hold an entire network hostage.

Keeping track of privileged user and shared access accounts is also important for accountability. Unfortunately, however, many organisations simply don't know for sure who has access to shared passwords. Far too often, the entire IT department knows the details of what is supposed to be a limited-access password. According to a 2008 survey of its members by the Independent Oracle Users Group, nearly 40 per cent of organisations had no way of monitoring the abuse of data by privileged account users.

As a result of high-profile incidents like those at the City of San Francisco and Société Générale, legislation and industry regulations such as PCI DSS are increasingly prohibiting the sharing of accounts between users. But this causes big headaches for many IT managers in both the public and the private sector, as shared and privileged accounts have become a necessary component of today's enterprise IT infrastructure.

All kinds of employees, from office administrators and temporary workers to nurses and civil servants require access to shared account logons for enterprise applications and systems for all kinds of reasons. IT managers therefore need to strike a balance between providing the flexibility required to meet end users' needs and ensuring security and compliance with corporate policy and the latest industry regulations and legislation.

So, how do they protect themselves from the risks in a cost-effective manner?

To make certain of compliance - and to ensure that IT applications and systems are secure - organisations need to know who is using what shared account and when. They need absolute certainty, so they can identify the culprit if data is stolen, changed or deleted. They also need to be able to demonstrate this information in a clear audit trail.

The first step is to put in place a scalable and flexible method for regularly changing passwords, as well as a reliable way of ensuring that all passwords generated are unique on every system and suitably complex.

The second step is to centralise shared account storage and control so that a user must make a request to use a shared password. This can then be approved or denied based on pre-established policies set by the organisation. This ensures that the organisation has visibility and hence control each time a privileged credential is accessed or used.

The more people who know a password the greater the threat it poses to an organisation. So the next step is to ensure that all passwords for shared accounts are concealed so that a user never actually knows the password of an account that is checked out. This prevents the inadvertent or malicious sharing of passwords, as well as sabotage by rogue administrators. To facilitate regulatory compliance it is also important to tie





shared account usage to the user within the organisation's identity management system so that the actual user of a shared password is known at all times.

For some particularly sensitive accounts organisations might also want to consider controlling the usage of privileged or shared password by policy. For example, by setting a limited time window for their use, or prescribing maximum number of logons. A further security measure could be to introduce two-factor authentication at the point of logon to ensure that the person using the account is actually the person authorised to check it out.

The loss of revenue and the damage to their reputations suffered by the City of San Francisco administration and Société Générale could so easily have been avoided if they had put these relatively low cost security measures in place. Solutions for managing shared credentials can provide a simple, secure and audit-ready approach to providing system and application access for administrators, temporary workers and others who must share account passwords. They dramatically reduce the risk that enterprise systems will be compromised by the unauthorised use of privileged accounts.

Not only does this close the security gaps associated with shared password management but it also provides a cost efficient way for organisations to comply with data protection and PCI DSS regulations that prohibit the sharing of accounts between users.

World News In Brief

Eight Million Chip and PIN Pals At Risk of ID Fraud

New research from LV= home insurance has revealed that in the past 12 months, over eight million adults have given their chip and pin details to someone else to make a purchase on their behalf or get money from a cash machine for them - with a quarter (24%) of these falling victim to fraud.

Experts warn that by sharing pin numbers with others, card users are exposing themselves to fraud and seriously weakening the security of the chip and pin system.

The research shows that ID fraud 'hotspots' such as websites, petrol stations and cash points are among the most common locations for people to use friends' and families' cards, with the most popular 'pin pals' being spouses or partners

Businesses themselves need to pay closer attention as 98% of people who have used someone else's card said they were not caught, leaving retailers open to being targeted by fraudsters.

Banks may refuse any kind of refund if the card owner has shared their pin with others, as card users sharing details may be considered to have acted 'without reasonable care' by banks who will then refuse to pay out to cover stolen funds.

Sandwell Council Loses Personal Data on Children in its Protection

According to the ICO Press Release on 4th September 2009, Sandwell Metropolitan Borough Council has agreed to take action to comply with data protection principles. The council has signed an 'undertaking' to assure the Information Commissioner's Office (ICO) that personal data will be kept securely in future.

ICO has found Sandwell MBC in breach of the Data Protection Act after an unencrypted memory stick was lost by an employee. The memory stick was not password protected and it contained sensitive personal information relating to four families, including why children were taken into care or made subject to a Child Protection Plan.

Alison Fraser, Chief Executive of the Sandwell Metropolitan Borough Council has agreed to ensure that portable and mobile devices, including laptops, computers and such devices, used to store and transmit personal data are encrypted. The council staff will also be appropriately trained and made aware of the policy for the storage and use of personal information.

Head of Enforcement at ICO, Sally-Anne Poole said "It is vital that personal information, the loss of which could cause damage or distress to individuals, is handled securely, particularly in the case where the information is sensitive and relates to children. I am pleased that the council has taken remedial action to improve data security."





BlackBerry Fit for eBanking

certgate, a specialist for mobile and communication security, in cooperation with the informatics centre of the (mutual) savings bank organisation SIZ now extends secure mobile business transactions to BlackBerry devices.

certgate SmartCard microSD with its built-in cryptographic chip enables Distributed Electronic Signature (DES) with EBICS through a secure SSL connection. The technology had been introduced for Windows Mobile based devices earlier in 2008.

EBICS transactions with electronic signature over secure SSL connection "on the road": certgate SmartCard microSD, well known for their EBICS support on PDAs and smartphones, now brings this technology onto BlackBerry devices. As a result, more decision makers frequently travelling for business can now authorise urgent financial transactions in a secure fashion away from their desks.

EBICS (Electronic Banking Internet Communication Standard) is a standard in the German banking business supporting Internet-based product for electronic banking. EBICS transactions provide the basis for transfer of encrypted orders to the bank-specific target system. Transferred data must be signed by one or more authorised individuals according to a pre-defined signature category.

Sumikin Bussan is going to distribute Impinj RFID Products in Japan

Impinj, Inc. the provider of UHF Gen 2 radio frequency identification (RFID) technology and global trading company Sumikin Bussan announced that the latter will sell the Impinj Speedway family of RFID reader and antenna products throughout Japan. With the use of this special type of reader, Japanese RFID solution providers will now have easy access to the world's leading UHF Gen 2 technology for a wide variety of applications and markets.

The relationship between Impinj, Inc. and Sumikin Bussan signifies the growing importance and value of UHF RFID technology solutions. It is also believed to strengthen the presence of the Impinj brand in the world. Dick Yamauchi, General Manager of Supply Chain Management and Project Development Department for Sumikin Bussan said: "We are pleased to represent Impinj RFID products in Japan." He also said "We believe Impinj's products combined with our market knowledge and

expertise will accelerate the expansion of RFID adoption in Japan."

Mr. Larry Arnstein, Senior Director of Business Development for Impinj said "We are impressed with Sumikin Bussan's leadership in both working with the Japanese Government and internationally to promote the adoption of UHF Gen 2 solutions." Impinj looks forward to jointly supporting their mutual customers and helping the market grow.

Smart-card Proposal to Combat New Zealand Obesity

According to New Zealand Herald, the country's Ministry of Health is considering issuing a smart card that would offer subsidies for those on welfare to buy healthy food. The program would encourage healthy foods consumption in low and middle-income families with children to reduce New Zealand's high rate of obesity.

Health economist Des O'Dea and colleagues of Otago University at Wellington suggested the New Zealand government to set up a smart-card electronic subsidy system that would be similar to the food stamps now given to low-income families in USA. It would be aimed at reducing "food insecurity" and encouraging consumption of healthy foods over junk foods. In a research, financed by the ministry and the Health Research Council, Mr O'Dea evaluated removing GST (Goods and Services Tax) from basic healthy foods. He said that an electronic smart card could be targeted at those on lower incomes such as about 300,000 working-age beneficiaries, and those who receive the Working for Families tax credit.

O'Dea has estimated that the new subsidy system would cost the Government around \$100,000 a year. He further stated that the pensioners should be excluded from this new subsidy system since they do not face food insecurity.

Hygienic RFID Animal Ear Tags for Animal Tracking

A Chinese leading producer of animal tracking solutions, DAILY RFID has launched a series of hygienic RFID animal ear tags for livestock tracking such as cattle, pigs and sheep. The ear tags are constructed of polyurethane, which prevents the growth of bacteria and thereby decreases the chance of infection in tagged animals.

According to the producer, these user-friendly RFID animal ear tags include passive components (with no battery) that can be worn as ear tags to



enable automated livestock management in processes, such as feeding, immunity, disease management and breeding practices. The RFID animal tag can also help to track growth rates by recording the number of individual animals. In addition to these ear tags, DAILY has also released inject tag, hang tag, foot ring and tag princer to make animal tracking processes lot easier.

Suprema set to provide Biometric Solution to Brazil

Suprema Inc., a developer and supplier of biometric technology, is all set to provide the Brazilian government with a fingerprint solution. The solution comes as part to revamp the country's voting and voter registration systems. The decision to use RealScan-D fingerprint scanners from Suprema was made by the Brazilian Superior Electoral Court (TSE). Officials hope that the new system will streamline voting procedures, thereby preventing fraud and consolidating the rights of the citizens.

The FBI certified RealScan-D live scanner is a portable, USB-powered device, suitable for bundling with a mobile jump-kit when used at the voter registration and voting sites. With the introduction of these live scanners, the Brazilian government aims to implement uniform biometric voting system in the entire nation to enhance the strengthening of the rights of its people.

Imperva says UK Firms need to Tighten up on Web App Security

News that more than a quarter of all Web applications have a high risk of security vulnerabilities comes as no surprise, nor is the fact that the problem is getting worse, says Imperva, the data security specialist.

"The 2009 Web Application Security Report from NTA Monitor shows that the number of apps with at least one high risk vulnerability has soared from 17 to 27 per cent in the last year, whilst the medium risk category has risen from 78 to 90 per cent," said Brian Contos, Imperva's chief risk strategist.

"Although this comes as no surprise to us, it is an appalling indictment on the software audit and control operations in most companies. With NTA spotting an average of 13 vulnerabilities per test, it's clear that IT departments really do need to pull their socks up in terms of testing and auditing of their software development processes," he added.

According to Contos, NTA Monitor's report proves what Imperva has been telling its clients for some time - namely that few organisations have the in-house resources to perform regular software testing

and updating a clearly-stated set of application security policies.

Perhaps worse, he said, even fewer companies do as NTA Monitor suggests and include security service level agreements into their contracts with Internet or managed service providers.

Staff training, he explained, is central to application auditing and testing, and, since few organisations have the time or skills required, the key to the problem is effective outsourcing.

RFID Cocoon Cooker Wins Electrolux Award

Rickard Hederstierna from Lund Institute of Technology in Sweden is the winner of the Electrolux Design Lab 2009 competition for inventing the Cocoon, the meat and fish maker. The winner was announced at finals in London on September 24, at 100% Design London, the UK's leading architecture and design event.

"Cocoon" is a sustainable response to the world's growing population and its desire to consume meat and fish. Similar to heating popcorn in a microwave, Cocoon prepares pre-packaged meat and fish dishes by heating muscle cells identified by radio frequency identification (RFID) signals. The signals detect the specific dish and then suggest the required cooking time. This process uses science to create food, lifting a burden on the planet by reducing the need for further intensive farming and fishing.

Precise Biometrics Targets Bank Market in Africa

Precise Biometrics has entered into a strategic partnership with Interswitch - one of the leading African financial solution providers based in Nigeria. The aim is to supply fingerprint recognition with Precise Match-on-Card(TM) to bank applications. The partnership is already engaged in a first project, which will provide license sales at a minimum of € 200,000 in 2009.

The partnership between Precise Biometrics and Interswitch aims at building and promoting biometric Match-on-Card solutions for the bank segment in Africa. The solutions will initially target Nigeria, which is the largest populated country on the continent with more than 150 million inhabitants.

Nigeria recently decided to replace magstripe bankcards with more secure chip cards, so called smart cards, in order to gradually eliminate fraud related to less secure magstripe cards. The new cards comply with the EMV (Europay, Mastercard, VISA)





standard used in the bank industry and the government deadline to replace all magstripe cards with chip-based smart cards is December 31, 2009.

To enable banks to migrate faster, Interswitch has introduced the Verve card into the market. The Verve card has both international and local security features, and through Interswitch's partnership with Precise Biometrics, it also includes fingerprint recognition and Match-on-Card features. These features are used to control a cardholder's physical presence at the moment of a transaction. With fingerprint recognition and Match-on-Card, banks, governments and organisations increase security internally as well as for customers through personal verification and KYE (Know Your Employee).

Mitchell Elegbe, Managing Director and Chief Executive Officer of Interswitch states: "We are pleased to enter into this partnership, as Precise Biometrics is the leading provider of biometric Match-on-Card solutions. We believe that our joint efforts and technological know-how will have great commercial potential in the West African region. The capabilities, security and reliability of the Match-on-Card solution give us a positive differentiation from biometric solutions that are relying on databases or external servers."

Thales Launches SafeSign Single Sign On

Thales announces SafeSign Single Sign On, the latest addition to the SafeSign strong authentication and ID management product line. SafeSign Single Sign On delivers simplified strong authentication for organisations concerned with ever increasing security threats, rising help-desk costs and frustration with managing multiple and complex passwords.

SafeSign Single Sign On provides simplified secure access to sensitive applications through strong authentication, requiring the user to identify himself only once at the start of a session. It enables suitable authentication logon policies to be enforced in order to meet a diverse set of business requirements.

ENISA Warns of Alarming Increase in ATM Crime

Annual cash machine losses in Europe approach EUR 500 million: ENISA provides advice for consumers

With the annual cost of ATM crime in Europe approaching half a billion Euros, ENISA, the European Network and Information Security Agency, is urging consumers to be more aware of

the risks and take precautions to avoid personal loss. The rapid growth in the number of ATMs combined with more sophisticated attacks and fraud has resulted in an alarming 149% rise in ATM attacks in 2008.

The number of ATMs in Europe increased 6% last year to almost 400,000, with many now found in remote site locations such as convenience stores, airports and petrol stations. Seventy-two percent of European ATMs are located in just five countries: UK, Spain, Germany, France and Italy.

Cash taken illegally from ATMs is still the preferred method for criminals who obtain pin numbers using a wide range of techniques from 'shoulder surfing' to complex skimming techniques. This can involve the use of a small spy camera, a false PIN overlay and even fake machines; while increasingly Blue Tooth wireless technology is used to transmit card and PIN details to a nearby laptop computer.

During 2008 alone, a total of 10,302 skimming incidents were reported in Europe. Other methods used to extract money include trapping and then retrieving users' cards, stopping withdrawals in the middle of a transaction only to complete them when the victim has left and even trapping cash in the machine. Organised criminal gangs are also using sophisticated phishing techniques and hacking into bank computer systems and web sites to obtain PIN and account information.

ATM burglaries and physical attacks have also seen an increase by 32% over the last 12 months from ram raids and explosions to the use of rotary saws, thermal lances and diamond drills.

"ATMs are attractive to criminals because they contain bank notes, while the bank cards themselves give thieves access to customers' bank accounts," said Mr. Andrea Pirotti, Executive Director at ENISA. "Looking ahead, ATM crime is likely to become even more attractive as the latest generation of ATMs is designed to dispense other services and products such as phone top ups and stamps. The first line of defence against ATM crime is increasing awareness of the risks so that users can take simple precautions such as shielding their PIN when entering it and by keeping alert to any signs of tampering or suspicious activity at an ATM."

LaserCard Corporation appoints Secure ID Solutions Expert Ismael Dykman

LaserCard Corporation, a leading provider of secure ID solutions, has appointed Ismael Dykman, an





expert in this field, as their new sales and business development manager. He, along with his team of professionals will work together in providing secure ID solutions to governments throughout Latin America.

Bell ID Upgrades National ID Management System of Macao SAR

Bell ID, the leading smartcard technology management firm, has announced the successful upgrade of its ANDiS Management System at the Macao Special Administrative Region (SAR) to further enhance the security and life cycle management capabilities of the Resident Identity Cards.

The Macao SAR Resident Identity Card is an official identity card valid in the region. The recent upgrade of the national card by Bell ID extended ANDiS to include the personalisation of Secure Access Modules and the provision of additional digital certificates on the ID cards. In addition, Bell ID implemented a SOAP-based web service for cryptographic key management and key exchange, further enhancing the operational efficiency of the management system.

Oberthur Technologies to Provide Easy Contactless Cards for Montreal's Public Transport System

Oberthur Technologies has been selected by STM (Société de Transport de Montréal) to supply contactless cards for use in public transport throughout Montreal region.

As the sole supplier to STM, Oberthur Technologies will deliver the e-ticketing smart cards over the next four years, which can be used on buses, the subway and commuter trains throughout the Greater Montreal area and Quebec City, and can be recharged at automated fare vending machines or points of sale. To use this easy, highly durable plastic card, the passenger simply needs to hold it above the card reader at the turnstile or fare box on the bus.

Starbucks right at your Fingertips

The myStarbucks App is the first official Starbucks Apps for iPhone and iPod touch customers' on-the-go. The myStarbucks tab allows you to easily find and store your favourite stores, espresso beverages, Starbucks whole bean coffees, and food items for quick reference or to share with friends and family. The myStarbucks App also offers the unique ability to filter stores and conduct location searches based on a store's amenities, including store hours and

whether they have a drive-thru, oven-warmed food, or wireless internet access.

Powerful Encryption Technology to Protect Critical Data Applications

Revere Security, a company specialising in cryptographic data security solutions, has developed an encryption engine that's small, efficient, affordable and powerful enough to unlock a world of security opportunities in pervasive and ubiquitous computing and a host of critical data applications.

The company is powered by its unique algorithm that delivers a multitude of benefits across audiences and applications, including the industry's smallest footprint resulting in smaller chips that require less power at a reduced cost. Revere Security's algorithm has been rigorously tested, analysed and proven successful through an independent study by ISSI, a company consisting of 30 scientists, engineers and mathematicians recruited primarily from the National Security Agency (NSA).

Gemalto's First Payment Card Personalisation Facility in Indonesia

Gemalto announced about inaugurating its first personalisation centre in Indonesia before the end of 2009. The new facility will enable Gemalto to locally support financial institutions in their EMV migration. Gemalto will act as an end-to-end service provider, from card manufacturing through to fulfilment. Value-added services include inventory management and express card personalisation with same day shipment. The personalisation centre achieved MasterCard and Visa certifications in less than six months.

INTERPOL to set Global Standard with first-ever E-Passport

INTERPOL's Secretary General Ronald K. Noble has announced that the EDAPS Consortium had been chosen to design and produce the world's largest police organisation's first-ever e-passport. Incorporating state-of-the-art technology, the e-passport will be issued to the Heads of INTERPOL's 187 National Central Bureaus (NCBs), Executive Committee members and staff from its General Secretariat headquarters.

Delivering the keynote address to the 5th Symposium and Exhibition on International Civil Aviation Organisation MRTDs, the INTERPOL chief said that the provision of a secure, globally recognised INTERPOL e-passport is aimed at ensuring that they can travel freely internationally in order to assist in the apprehension or transfer of fugitives.





India's UID Project to help the poorest

By Suparna Sen, Smartcard & Identity News

Like that of the USA social security number and UK smartcard, the Indian government is all set to introduce its own version of "Unique Identification Number" for all Indian citizens above and below the age of 18 years. To lead this ambitious ID card project, on 23rd July, 2009 Prime Minister Manmohan Singh chose Nandan M. Nilekani, a founder and former chief executive of Infosys Technologies as the chairperson of The Unique Identification Authority of India (UIDAI). As the head of this authority, Nilekani is enjoying the rank of a cabinet minister and has ceased to be the board member of Infosys.

The Unique Identification number will be backed by biometric authentication. Fingerprints and photographs of more than a billion people will be taken at the time of registration for the identity number. The biometric evidence will be stored online and as Nilekani has said it will be the biggest such national database in the world.

It is predicted that at least 60 crore (600 million) people would get their Unique Identification Numbers (UIDs) in the next 4 to 5 years. The Union Home Minister P Chidambaram said in Chennai on 21st of September that the proposed unique multi-purpose National Identity Cards would be issued to all citizens by 2010-2011. The process has already been started, with Delhi been the first Indian city to get such unique numbers in next 3 to 4 years.



Nandan M. Nilekani

Speaking in New Delhi on 2nd September, Nilekani appreciated the Delhi city government for its full cooperation towards the newly created body. He met Chief Minister Sheila Dikshit at her office where he gave a presentation on all aspects of the project. His team will make use of a database prepared by the Mission Convergence project of the Delhi city government to create a comprehensive database of 9 lakh (900,000) households and 42 lakh people, based on detailed biometric information of the residents.



Unidentified children having a roadside dinner in Delhi

Nilekani said the initiative would help in providing transparent, effective and transformational governance in the entire country. Speaking at a FICCI-IBA Banking summit, Nilekani said banks would be a key partner in the project and UIDAI would publish standards and protocols for the project in the next six months.

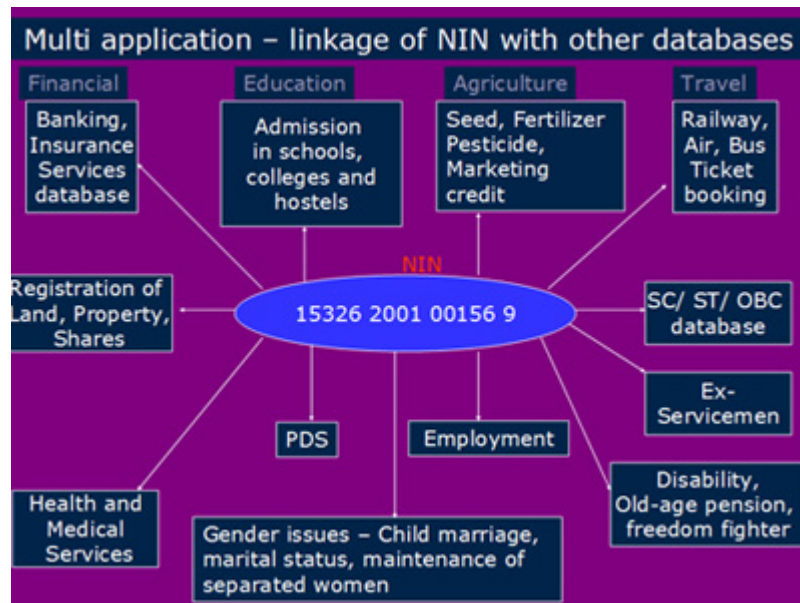
Now the question comes in as to how to make use of biometrics to make the Identification Numbers, unique in the true sense of the term. The chairman thinks that checks will have to be done carefully because there are high chances of the "phenomenon of duplicates" or fraudulent numbers.

As Mr Nilekani added, "it is clear that a large number of poor people have no identification at all, making it doubly difficult for them to gain access to social welfare schemes. This project is pro-poor and primarily targeted towards the poor. The middle class and the rich have some form of identity, but people on the margins are getting lost because of lack of identity." It is also hoped that the number should help tackle identity theft and fraud in India.





One important point to note is that the unique number will not be an identity card; instead, the number of each citizen will be included in documents like the election identity cards, PAN cards and bank account numbers, as said by Nilekani and the United Progressive Alliance (UPA) government.



The above figure shows Government proposal to link databases

However, just like every coin has two sides, doubts have been raised regarding the success of the UID project. Intellectuals and common people alike have questioned on the huge cost (estimates of £3 billion) technological challenge, volume of work to be finished within the stipulated time period and on the final outcome of the project.

According to the Arjun Sen Gupta Committee Report, in India, about 80% of people live under 20 Rupees a day (26 pence GBP). In such circumstances, spending so much money on a time-consuming project seems less feasible. It is suggested that the government could invest more on the welfare of the poor, on education and healthcare.

In an interview taken this month, Karan Thapar of the CNN-IBN fame questioned UIDAI Chairman Nandan Nilekani on the issue of technology. What technology will be used to make these ID cards? Thapar brought forth the analysis made by the London School of Economics on a similar project that was being considered by the British Government. They have concluded that the technology envisioned for this scheme is to a large extent untested and unreliable. No scheme on this scale has ever been undertaken anywhere in the world.

Then question crop up here as well as to how far Nilekani and his team will succeed in using advanced Biometrics Technology in making the ID cards really unique and authentic? According to Nilekani, there is absolutely nothing to worry about this project going into uncharted territories. He admitted, "There is the technological challenge, there is a challenge of the scale of work, and there is a complex governance challenge, working with so many departments and states". However, he believes that over time, all these problems will be addressed properly and handled with care.

Asked on how it could be ensured that the database would not be misused and result in an invasion of privacy, Nilekani said that "in every system there would be people who would try to hack on it. Some are impenetrable, some are not. We will have to design it as good as possible. We can certainly create checks and balances".

Thus keeping in mind the significant benefits of the project in making the poor inclusive and in giving them a chance to participate in the country's progress; it is now up to the Indian government and the UIDAI to make the ID numbers successful and really worthwhile.

