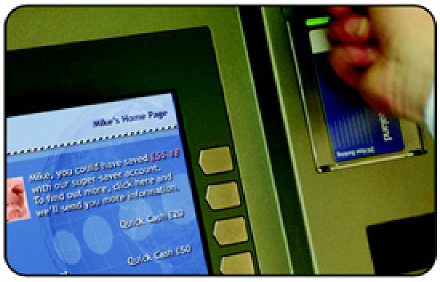
July 2009

Volume 18 • Number 7

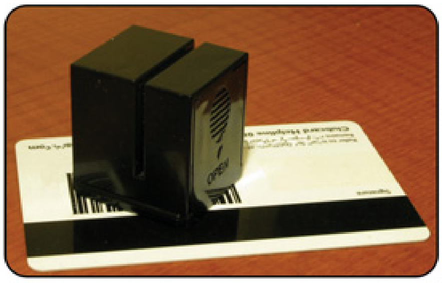
# Smart Card & Identity News

Smart Cards, SIM, Payment, Biometrics, NFC and RFID

www.smartcard.co.uk



*6 • ATM Malware Code Steals Bank Details*



*12 • Europe Eyes Banning Mag-Stripe*

*13 • TJX Companies, Settles Data Loss Fine*

*18 • Interview with Morten Landrock, UK Managing Director of Cryptomathic*

# 40 Million Stolen Identities

Attempted ID Theft
Your IDENTIFICATION - has been compromised. Your attention is required.
Action
Ignore
Help
SOCIAL SECURITY
CREDIT CA
PLATINUM

There is a new web site on the internet that has over 120 million records relating to at least 40 million unique identities from data that has been traded between criminals over the last 4 years. Lucid Intelligence (www.lucidintelligence.com) has gathered personal information including credit card details, bank account numbers, PINs and telephone numbers available to criminal elements prepared to pay the bill.

The web site is not there to sell this data but to give citizens the opportunity to find out whether they might be at risk to on-line identity theft. They can find out if they are on the database for free, but then it costs you $16 to find out exactly what data Lucid has captured about you over the internet. In some cases they may even tell you how it was obtained.

The Lucid web site lists the three people behind its incarnation, Colin Holder who retired from the Metropolitan Police as a detective sergeant after 30 years service. In later years Colin specialised in fraud and identity theft. Jack Richardson is the data base specialist who has worked his time in the healthcare, leisure and banking sectors. The third member of the founding team also comes from the Metropolitan Fraud Squad, Tim Harvey who became Detective Superintendent in charge of all operational fraud squad teams retired from his policing activities in 2006.

**Continued on page 4….**

*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.

**Contributors to this Issue** – David Everett, Tom Tainton, Torsten George, Kevin Gillick.

**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.

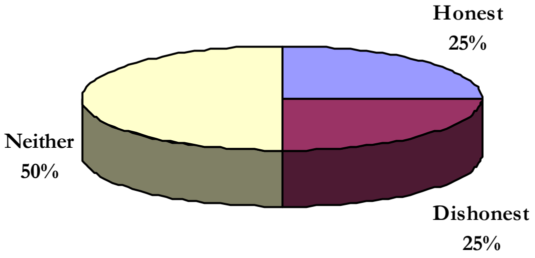
# Our Comments

***Patsy Everett***

Dear Subscribers

Where money is involved you will always find fraud. For years the 'Ring of Confidence' has been my guiding light although I always used to wonder if it's really true. The ring represents the total population and says that 25% of the population is totally honest, 25% is totally dishonest and 50% will take what's on the table. Could 75% of the population really be dishonest? But now I'm starting to worry about the existence of the 25% supposedly honest souls.

**Ring of Confidence**



This month I have been reading about the level of fraud attached to eBay and PayPal, well not these organisations who incidentally have a common ownership but the people who use their services. It's not just the selling of goods that are a little misrepresented, like new when really they are pretty worn but the number of instances where people set out to commit open fraud. There are sellers who are blatantly just trying to get your money for goods they never intend to send and buyers who never intend to pay. The list is endless, in fact there are books on the subject such as 'Scams and Scoundrels' by Michael Ford which would almost put you off ever wanting to use eBay.

The really interesting thing is the way that the internet has interwoven the concept of a transaction between two parties and the payment mechanism. If somebody sells you rubbish on eBay then the general assumption is that PayPal should reimburse you. We have got used to this with credit cards where consumer laws protect the use of credit cards but not necessarily in the same way for charge cards or even debit cards. eBay is of course the auction site and PayPal the payment mechanism but the fraud in most cases  is clearly nothing to do with the payment mechanism itself. So the question has to be about whether we are looking at internet transactions in the right way. In fact it's no different to the old fashioned way of buying things from a newspaper or magazine advertisement. You would send in your order enclosing perhaps a postal order, cheque or even cash and wait for your goods to arrive. What happens if they don't appear or they do not match the advertisement? Well then you would get on the phone and try and resolve the dispute, there was little hope of cancelling a postal order or cash. The money is already irrevocably in the other person's hands.

I'll bet you have forgotten all about it, Cash on Delivery better known as COD. When the goods arrive you would have a quick look and hand over the cash. Both parties are at least partially protected and it would certainly avoid the majority of scams monopolising the internet today. In the business world we still have escrow accounts, some third party such as a bank who everybody (used to) trusts would hold the buyers funds on behalf of the seller until the buyer confirms the goods are received and all is well.

You are probably wondering where this is going? It's not that I have some burning desire to rewrite the credit card charters only to point out that most internet fraud scenarios are really nothing to do with smart card payment systems such as EMV but are due to the fraudulent behaviour of the people involved. Improving the security of the payment system does not in itself stop the problem, the security has to be applied as part of the transaction protocol.

Ah you might say well surely eBay offers escrow services? Well not exactly because as I understand it, such services are provided by 3rd parties outside of the eBay umbrella. But what's wrong with that? Yes, we've eventually got there, it's all a matter of trust because a quick search on Google will show you that there's plenty of fraud in the world of escrow.

And my thought for this month, it's really all about identity. If I could trust the seller or buyer as the case may be then I probably don't need an escrow system. eBay provides me with a seller or buyer's history but the problem is that this is too easy for the fraudulent amongst us to manipulate, what I really want is an electronic on-line system that gives me the modern day equivalent of a 'Bankers Reference' on you! Any suggestions?

Patsy.

## Contents

### Regular Features

### Industry Articles

## Events Diary

### August 2009

| | |
|---|---|
| 16 – 20 | CRYPTO 2009, California, USA - www.iacr.org/conferences/crypto2009/ |
| 20 – 21 | Card Ex Conference 7 Exhibition, Johannesburg, South Africa - www.card-x.co.za |
| 27 – 29 | RFID India 2009, New Delhi, India - www.electronicstoday.org/rfid |

### September 2009

| | |
|---|---|
| 1 – 3 | Mobile Payments World Asia 2009, Singapore -www.terrapinn.com/2009/mpayments |
| 2 – 3 | Mobile NFC, London, UK -www.mobilepaycom.com/newt/l/mpayments/mobilenfc |

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

## September 2009

| | |
|---|---|
| 6 – 9 | Cryptographic Hardware and Embedded Systems 2009, Lausanne, Switzerland - www.chesworkshop.org/ches2009/start.html |
| 9 – 11 | Cards & Payments 2009, Paris, France - www.efma.com |
| 10 – 12 | E-payments India 2009, New Delhi - www.electronicstoday.org/epayments2009.htm |
| 10 – 12 | Smart Card Expo 2009, New Delhi - www.electronicstoday.org/smartcardsexpo2009 |
| 15 – 16 | Prepaid Cards & e-money CEE, Warsaw, Poland - www.prepaid-conference.com/cee |
| 15 | The 5th ISG Smart Card Centre Open-Day, Royal Holloway, University of London, Surrey, UK - www.scc.rhul.ac.uk/events.php |
| 22 – 24 | 5th Symposium on ICAO MRTDs, Biometrics & Security, Montreal, Canada - www2.icao.int/en/mrtd/Pages/ |
| 22 – 24 | The Biometric Consortium Conference, Florida, USA - www.biometrics.org/bc2009/ |
| 22 – 25 | Smart Event 09, Sophia Antipolis, France - www.strategiestm.com/conferences/smart-event/09/ |
| 29 – 30 | RFID Europe 2009, Cambridge, UK - www.idtechex.com/rfideurope09/en/ |

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

## …. Continued from page 1 - *40 Million Stolen Identities*

So first there are two questions, where did the data come from and for what is it going to be used, for $16 can I get the info on my chosen target? Of course some information such as credit card numbers is reported to be openly available for less than $1. Then one has to ask about the site itself, should the Information Commissioner (in the UK for example) allow a database with 120 million stolen records? Apparently about 4 million UK citizens are on identity risk from this data.

According to Lucid all the data on their site has been in criminal hands and has been put up for sale on the internet. Apparently files are sometimes made available from web sites posing as 'marketing sites', these sites are like a one stop shop for spammers and phishing perpetrators. The owners of the site have been collecting the data from sites such as bulletin boards and chat rooms. In addition the data has been obtained from black market FTP sites, which are apparently the virtual street corners of the cyberspace world.

The shear size of the data base makes you want to draw breath, 120 million records, gathered presumably over the last 4 years. But then you really need to know the sensitivity of the data in relation to what people freely make available. Facebook and other social sites for example carry an unbelievable amount of what can only be described as personal information. Just last month MI5 made it be known that candidates for jobs in intelligence will be disqualified if they have a Facebook or similar presence. Perhaps just a little confusing to hear the new boss of MI6 Sir John Sawers was starring on Facebook courtesy of his wife's profile on the site.

As for the matter of phishing where a perpetrator persuades you to link to a bogus site representing your bank or eBay or something similar to get your user name and password, well I would have to say that in my opinion it is easy to get caught. Some of these phishing sites are unbelievably smart and even the brightest may be lulled into the web of deceit. In the world of the internet you always need to be on guard and who can honestly say that they never slip up?

Dr David Everett

# World News In Brief

## 3M Considers Legal Action over Award of UK Biometric Passport Contract

Reports in July have revealed that 3M are considering a legal challenge over the Governments decision to award De La Rue the contract to produce the UK's Biometric Passport.

De La Rue Identity Systems, announced on the 11th June that it had been selected as preferred bidder to design and produce the UK's Biometric Passport. The 10-year contract is valued in the region of £400million.

3M are "furious that its bid was rejected," and is in discussions with the Identity and Passport Service (IPS) for an explanation of their decision.

There is a potential conflict of interest, as Gill Rider is Head of the Civil Service Capability Group, and a board member De La Rue which she temporally stepped-down during the bidding period and subsequently re-joined on the day the contract which awarded.

Gill Rider is responsible for recruitment and ‘Capability Reviews’, to ensure the Civil Service has the right capabilities to deliver Government's future requirements. She recruited two former colleagues to the top positions in the Identity and Passport Service team.

Gill Rider worked with James Hall Chief Executive of the Identity and Passport Service at Accenture for 27 years.

## UK IPS and IBM sign 7-year National Biometric Identity Service Contract

IBM will provide a replacement for the UK Border Agency's (UKBA) Immigration and Asylum Fingerprint System (IAFS), which holds biometrics collected from visa applicants.

James Hall, Chief Executive of the Identity and Passport Service, said: "This contract will provide a secure database for storing facial and fingerprint images for the next generation of biometric passports and will support the delivery of the National Identity card."

As the prime contractor, IBM will integrate and operate the solution, the majority of which will be built with IBM hardware and software. IBM will obtain integration and operations support from Atos Origin and will obtain biometric services and software from Sagem Sécurité (SAFRAN Group).

## CA Certificate Deleted for German e-Heath Card

The German e-Health Card scheme has suffered a serious set back after the root Certificate Authority (root CA) was deleted by the Hardware Security Module (HSM).

The company in charge of the project Gematik commissioned D-Trust, to provide the root CA as a service to the operation of the health card PKI. The incident is being blamed on a 'voltage drop' during testing; the HSM deleted the data independently as it thought it was being attacked. Restoring the data is an embarrassing problem as there is no backup of the root CA.

Gematik spokesman Daniel Poeschkens in a statement to heise online - poured scorn on the statement that Gematik had insisted on the service provider carrying out a test without backing up the root CA private keys. "We did not decide against a back-up service. The fact of the matter is that the service provider took over the running of the test system, so it also has to warrant its continuous operation. How it fulfils this obligation is its own responsibility."

The test system can continue to run providing no new cards need to be issued.

## India's 1.2 Billion Citizens to get Biometric ID Cards

India is taking on the largest Biometric ID Card program ever conceived. All 1.2 billion citizens will be issued with new biometrics ID cards.

The project will be lead by Nandan Nilekani who recently left Infosys to take control of the project. Nilekani said "It is a humongous mind boggling challenge, but we have the opportunity to give every Indian citizen for the first time a unique identity, we can transform the country".

Mr Nilekani has a huge task ahead, he has to get 60 government departments to co-operate, A new state department will be responsible for gathering and

storing personal details, which will make this one of the worlds' largest databases. The first cards are expected to be issued within 18 months.

Experts have warned that a database of this size will prove irresistible to identity thieves. Guru Malladi a partner at Ernst & Young said, "It will have to be impregnable".

## ATM Malware Code Steals Bank Details

We are all warned about covering our PIN codes with our hands whilst using the ATM machines. Now, there is no defence against the new malware targeting ATMs that has appeared in Ukraine and Russia. No matter how much a customer may try to cover their hands over their PIN at the ATM, the malware can still steal all the account details with relative ease. This scam goes far beyond that of an amateur's method of using PIN cameras and false keyboards at the cash box.

An ATM based malware script has been discovered with the potential to sit invisibly within ATM machines and record all sensitive data contained on the card, without being detected. The malware records card transactions, including the details for the PIN, security number and the account details, and remains very difficult to detect because it appears to look like any ordinary piece of the ATM coding.

The malware has been reported as being hidden as executable code in the ATM framework. It is believed to be the work of an insider at the bank or ATM, as the coding is required to be installed inside the actual machine. According to the report, given by NewScientist.com, virus checkers are said to be useless against the malware, with the criminal network behind the attacks camouflaging the malware within various Windows utilities inside the machine.

Security experts are concerned about the ATM malware as they are alarmed at just how easy and audacious it appears to be. It has the ability to record customers PIN and their 3-digit security number; a security detail often thought to be one of the last defences against fraud.

This type of malware has the potential to make the amateur skimming practices obsolete. Other unconventional skimming attacks have been looked at in university investigations, but this attack is the first time that malicious code has been found in public.

Through the use of a trigger card, scammers are able to 'tell' the malware to trigger a screen that will enable the attacker to either release the cash box, or print the encrypted details of customer accounts, thereby making it easier for criminals to employ mules to pick up the information for them, virtually undetected.

Although the malware has only been found in Russian and Ukraine ATMs, security experts are worried that the practice will quickly spread to areas such as East Asia and Eastern European localities. In these regions, security around ATM machines may be just as negligent, creating an opportunity to spread the malware globally. Banks in Australia have recently been targeted for an increase in ATM fraud, but the existence of this malware may fuel the requirements for a new strategy to combat these types of attacks at the local level, including different approaches to physical ATM designs.

## ATM Cracking Presentation Postponed

An upcoming Black Hat Conference was to be the stage for a live demonstration of an ATM cracking operation.

Juniper Networks has withdrawn the presentation and demo by Barnaby Jack after a request by the cash machine manufacturer, to allow them time to fix the problems before the details are made public.

A statement issued by Juniper stated "The affected ATM vendor has expressed to us concern about publicly disclosing the research findings before its constituents were fully protected. Considering the scope and possible exposure of this issue on other vendors, Juniper decided to postpone Jack's presentation until all affected vendors have sufficiently addressed the issues found in his research."

## TPG Capital Sells 8% of their Stake in Gemalto

Reports are emerging that TPG Capital has sold 8% of their 12.5% stake in Gemalto.

FSI (Fonds Strategique d'Investissement) purchased 8% in Gemalto for approx. Euro 160 million from TPG Capital, and has said it wants one representative on the board of Gemalto to help back the group's profitable growth strategy. TPG intends to retain the 4.5% stake at this present time.

# Ken Warren of Cryptographic Research explains CryptoFirewall

By Tom Tainton, Smartcard & Identity News

*Tom Tainton*

### What is CryptoFirewall and how does it work?

CryptoFirewall is an embedded silicon core designed only to protect keys and crypto-algorithm, it doesn't burden itself with additional functionality, and it can be implemented on its own or embedded. If you take the example of the pay-tv system and its conditional access module, a crypto-firewall would be embedded and that would be responsible for the components of the control contribution. It's essentially responsible for one part and doesn't get involved with all the various permissions. The application compliments the existing system by securing that specific part of the control world so if the system is compromised the overall pay TV system isn't. We can apply this in other anti -counterfeiting applications such as printers.

### How much of a problem is piracy to the pay-tv industry?

Traditionally it's been huge and continues to be so. There's an estimate that if piracy was eliminated the suppliers would gain an extra £6bn in revenue worldwide, it's staggering. Of course, some territories are better than others, and in instances where our CryptoFirewall technology is being deployed we have an unblemished security record. The first deployment was seven years ago and for something to survive in the field for that length of time is almost unheard of. The CryptoFirewall's design goals were to be as highly tamper-resistant as possible and in the pay TV industry a lot of the attackers are well funded and well equipped. We see it as quite a compliment to our technology that it has survived the test of time. However, we're not complacent. We recognize that things move along which is one of the reasons that we design CryptoFirewall with overlapping or complimentary systems. We accept that certain elements may be compromised but the whole thing won't be, because it's not a single point of sale.

### What sort of threats are companies at risk from?

One of the big issues in the pay-TV space is that set top boxes are sold at a loss or subsidized so the attacker will compromise the conditional access security. Thus, the attacker will receive the access for free and can bypass the subscription and payment mechanisms as well as re-programming the devices to work in the general case. Regularly, on EBay, people offer to sell conditional access cards or pay subscription cards, which will get you access to programmes at the fraction of legitimate cost. In the counterfeit goods area, someone will clone copy a component such as printer ink cartridges, usually be refilling the tank. Technology has begun to be deployed whereby authorization is required to verify that the correct ink supplier is correctly validated. That's another area for technology like CryptoFirewall where you would have a cryptographic handshake between the cartridge and the printer head to ensure it's the legitimate procedure and it's ok to continue. Cloning is a potentially attractive market as goods are sold significantly in excess of the raw manufacturing cost. Another type of attack, remanufacturing, is when the device is worked upon so it can be re-used such as modifying set-top boxes. The final area is repurposing devices where cell phones, limited to a handset provider, are made available for general use by cracking the security.

### How does CryptoFirewall provide the solution to these risks?

What CryptoFirewall is doing is providing a cryptographic authentification of the legitimacy of the product. There are a number of other application areas, such as medical devices. The potential vulnerability goes beyond purely financial, because there are life-threatening consequences of people using dodgy sensors. Another area is the aircraft industry. There are huge financial issues and the temptation to use ordinary bolts as opposed to specialist components so there's a growing requirement to ensure that legitimate products are used. In general terms, the impact overall globally of counterfeit goods is something like £200 billion, that ranges from bags and perfumes to all sorts. There are legal remedies to catch the perpetrators but the other solution is to use technology to ensure that only legitimate products and parts will be used.

**What challenges or competition does CryptoFirewall face in the industry?**

It is undoubtedly a change to the existing legacy, and there's no doubt there is a cost implication. However, if someone is losing a certain amount of money then it becomes an economic decision to cover the cost of deploying what is essentially a chip solution to solve that problem. There are other approaches that aren't so rigorous. In the ink cartridge market, there are several manufacturers that provide chip solutions to authenticate the ink. In most part, these are simple and easy to bypass and in some cases it might just be picking a chip off one product and putting it on another. We believe that with the CryptoFirewall we have a very robust and cost-effective solution. We're keeping the design solely security focused and not burdening it with additional non-necessary functionalities.

**Currently, what sort of take-up has CryptoFirewall had?**

Currently 75 million CryptoFirewall devices are deployed globally, predominantly in the pay-TV space. To date, as far as we're aware it hasn't been compromised. We work in industries where if they have been compromised we'd know about it pretty quickly!

**What does the future hold for CRI and CryptoFirewall?**

We're working with a number of customers to design CryptoFirewall into their products. We've announced initiatives in the pay-tv space and we're working in other industries as well. The CryptoFirewall is quite a design intensive process and there's an awful lot of work involved. One of the difficulties in designing something which is secure and tamper proof is that it has an impact on everything because you're explicitly taking out the testing features that would help you. The verification process is time consuming and we put a lot of effort into that. One of the longer term objectives that we're looking to achieve is to get a generic CryptoFirewall product supported by major manufacturers and we announced collaboration with Infineon to develop CryptoFirewall products. Ultimately, CRI's objectives are to increase our capability to be able to relay CryptoFirewall solutions to those that would benefit from it, particularly anti-counterfeiting protection.

# World News In Brief

## Giesecke & Devrient Holds Off Challenge from Oberthur Technologies

Number three smart card manufacturer Oberthur Technologies (up 1.4% YOY in 2008) closed the gap on Giesecke & Devrient in second place last year to less than one percent market share difference following its acquisition of XPonCard. However, the latest market analysis from IMS Research shows that the German company, after reporting record turnover and profits in 2008, maintained its position as the second largest manufacturer of smart cards globally, behind market leader Gemalto. Sagem Orga (up 1.3%) and Watchdata Systems (up 1.5%) were the other two companies calculated to have made the biggest gains last year.

"Overall the smart card market grew 16.7% in 2008 in terms of volumes and all manufacturers saw plenty of upside", commented John Devlin, author of IMS Research's Smart Card Annual Review & Market Share Update. "This meant that there was plenty of room for companies to manoeuvre and try to gain some initiative with regards to developing new opportunities."

Gemalto continued to be far and away the market leader, accounting for more than the next three companies combined, and its growth into service areas is one that others are keen to follow. Only in March did Gemalto announce its pending acquisition of NXP Semiconductors' Mobile Services Business, giving it an extension of its contactless/NFC business and combining it with NXP's MiFare knowledge. Other companies have also built out the service side of their businesses, announcing partnerships and acquisitions, such as Giesecke & Devrient's purchase of SmartTrust this April. Much of this development focuses on the mobile market since half of the smart cards in use last year were SIM cards.

Devlin continued; "There continues to be an erosion of standard smart card ASPs, particularly in the SIM arena, as increased competition (particularly from China), economies of scale and a slight slowdown in growth rates means that price pressure continues to grow. However, a number of companies are innovating with higher-end products in this area in order to increase margins. Added-value features, such as A-GPS, accelerometers, smart card web-servers, personalisation techniques, green credentials, increased security and multi-application cards are being released."

## Watchdata provides over 10million Smart Cards to Singapore Card Issuers

Watchdata is the first vendor to comply fully with the Singapore Standard for Contactless ePurse Application (CEPAS), winning contracts to supply smart cards for a nationwide application in Singapore. Watchdata has already issued more than ten million multi-application smart cards to various card issuers in Singapore. Currently, Watchdata is the only card vendor capable of supplying fully CEPAS-compliant cards.

Michael Yu, President of Watchdata's International Business Operations said, "We are delighted to be a key supplier of secure payment technology in Singapore. Through hard work and a strong commitment to excellence, we have played a major role in helping our Singapore customers realise their goal of issuing a single multi-application card in no time."

The TimeCOS contactless smart card uses Watchdata's CEPAS-compliant technology.

## Infineon not to be Asset Stripped

Concerns arose this month by news that Infineon could be asset stripped by an American private equity firm has been dampened by an interview with CEO Peter Bauer in the German newspaper 'Frankfurter Allgemeine Zeitung'.

To raise funds Infineon Technologies in mid-July launched a rights of issue for up to 337 million shares with a subscription price of 2.15 Euros per share. Apollo will guarantee the rights issue by buying any remaining shares at the subscription price, up to approximately 326 million shares not subscribed for by existing shareholders. Apollo will be paid 21 million euros fee for its reassurance.

Electronics Weekly E-zine reported that once Apollo owns a 30% share in Infineon, it is obliged by German law to bid for the whole company. This led to concerns that Infineon would by bought on the cheap and asset stripped by Apollo.

Peter Bauer explained to the German Newspaper; "It is important to have an anchor shareholder in the background. The issuance of new shares without a guarantor would have been too high risk at this time. When questioned about the breaking of Infineon, Bauer answered; No, I do not see this scenario, besides the market is not at all receptive to such transactions.

# The Threat from Within

## *- Tools to Fight Insider Security Problems*

**By Torsten George, Vice President, Worldwide Marketing at ActivIdentity**

*Torsten George*

Organizations have long faced persistent cyber attacks in form of Malware such as Trojans, computer viruses and spyware that can result in the potential loss of corporate data and intellectual property. As a result, many organizations focused their IT security spending on addressing external threats rather than implementing multi-layered security approaches across networks, applications facilities, intellectual property and other information assets. Such a strategy protects against threats from both outside and inside an organization.

This focus on security spending is natural givern the obvious requirement to protect the organizations perimeter Insider attacks originate, in many cases, with the very people who are tasked with keeping the information technology working. Keeping insider threats at bay is difficult due to the ubiquity of CD and USB drives, or even user access to printers that are often not secured or controlled.

According to a survey of more than 200 organizations globally conducted by Deloitte Touche Tohmatsu, only 28 percent of respondents rated themselves as “very confident” or “extremely confident” with regard to internal threats, which is down from 51 percent in 2008. The shift in the assessment of internal threat preparedness can be tied to the change in the business environment and the large number of layoffs. As the survey outlined, often IT was unprepared to denying employee access to critical systems in the event of mass layoffs.

Another study, conducted by Symantec and the Ponemon Institute, revealed that 24 percent of former employees retain access to their employers’ computer systems or networks after their termination. This illustrates not only the increased internal threat levels, but also emphasizes the need for a more sophisticated approach to access control.

### High-Risk Targets

Although enterprises in nearly every industry are susceptible to insider threats and data theft, some are naturally more prone to this danger than others. Any organization that is in a highly competitive market or that produces valuable intellectual property must be more concerned about insider threats. For instance, aerospace and defense companies are at high risk, considering the type of products and services they produce. Furthermore, public companies have more at stake than privately held companies that are not traded on stock exchanges.

### Threat Vectors

Whereas hackers have built sophisticated tools to infiltrate networks, privileged insiders already have been granted access to data that can be sold or exploited outside the company. The most common method employees use to steal information is also the least technical method—they simply cart off printed reports. Data can also be placed on CDs, DVDs, or USB key drives, as a legitimate attempt to backup data and later can be exploited if the employee becomes disgruntled. .

Insiders can access data in other ways, as well. Business applications (internal and hosted) and Intranets have become a common repository for competitive information, pricing, RFP guidelines, and other sensitive data. Many organizations put themselves at risk by using only username and password authentication for these areas instead of implementing a strong authentication system.

## Tools to Fight Insider Security Problems

If an employee is a threat to their employer, protecting the access to this data becomes critical. Organizations trying to address the increased internal threat risk should consider a multi-layered security approach across networks, applications facilities, intellectual property and other information assets.

The foundation of this approach lies in creating corporate policies that determine who requires access to sensitive data and subsequently deploy the proper controls to allow or disallow access. It is recommended that organizations lock down USB ports and Internet protocols to reduce malicious transfer of data, as well as deploy controls that define how data can be copied and transmitted. Many security-minded organizations today lock down their employees computers completely, disabling the use of any external media drives. Some go even a step further and deploy access control mechanism to their corporate printers, allowing only a selected group of personnel to print out pre-defined data.

The next security layer deals with data access control in form of strong authentication. While many organizations still rely on user name and password as the primary identity credential to control access to sensitive data, we all are aware that this methodology represents the weakest form of authentication. User names within organizations normally follow corporate standards and are therefore easy to predict and the passwords are often accessible to co-workers from the sticky notes that are tucked to the colleagues computer screen; strong authentication methods are therefore highly recommended.

The strong authentication technology has made major advancements over the years and standardization has driven down the cost of deployment. Thus, organizations should consider relying on methodologies such as adaptive authentication, (lightweight) one-time-password authentication, out-of-band authentication, biometrics, or Public Key Infrastructure-based authentication when controlling the access to networks, workstation, and data across the IT infrastructure.

Larger organizations should consider leveraging a credential management system in addition to a strong authentication platform, as in today's business environment it becomes essential to find cost-effective and efficient ways to streamline the decommissioning of user credentials, so that disgruntled ex-employees cannot continue to gain access to sensitive data by using their old access credentials.

## Smart Card-Based Access Control as Best Practice

Smart cards represent the best practice approach for a multi-layered security approach across networks, applications facilities, intellectual property and other information assets. A smart card-based employee identification badge represents tremendous cost-efficiencies for organizations, as it functions as a photo ID and a proximity badge for facility access, as well as an IT security device for digital identification and authentication. Such a "smart employee ID solution" is much more than a multi-function smart card – it is a solution that allows organizations to converge user identification and improve facility and IT security by integrating processes and back-end systems. The result is a single card for each person across facilities and IT domains, providing increased security and accountability.

This is the reason why many government agencies as well as commercial enterprises that deal with government entities have rolled out strong authentication and credential management programs that are solely based on smart cards.

# World News In Brief

## Visa and MasterCard European Dominance to be Tested

The European Central Bank has called again for the industry to construct a rival scheme to challenge Visa and MasterCard dominance in the Single Euro Payments Area.

French and German banks are increasing their efforts to create a new European Debit Card Scheme. At EBAday (an annual payment industry conference), Wiebe Ruttenberg Head of Market Infrastructure Division, European Central Bank told delegates "We need at least one alternative card scheme in Europe to become a credible challenge to the duopoly".

Banks have been a little hesitant to commit due to the uncertainty surrounding 'Interchange Fees'. Interchange fee is a term used in the payment card industry to describe a fee that a merchant's bank (the "acquiring bank") pays a customer's bank (the "issuing bank") when merchants accept cards using card networks.

A group is to be set up in September to accelerate the scheme, and it is hoped that other European counties will join to create a solid European System.

## Europe Eyes Banning Mag-Stripe

According to the chairman of the European Payments Council, Gerard Hartsink, European banks are considering banning the use of magnetic stripe credit and debit cards.

Hartsink, who is also senior executive vice president of ABN Amro in Holland, said that European financial companies would have largely completed the transition to the EMV Integrated Circuit Card Specification by 2011. Hartsink also added that the council, which is pushing the transition to the Single Euro Payments Area (SEPA), would be able to advise its members to stop accepting magnetic stripe cards, which are considered less secure than those that use EMV.

At London's Contactless Cards and Payments conference, the European Payments Council Chairman stated, "My feeling is, although it has not yet been decided, the council will take a decision in 2011, maybe 2010, to only use chip cards."

If the European banks went along with such a decision, US cardholders could be left in the lurch, if they were to travel to Europe, when attempting to use their cards for purchases or ATM withdrawals.

According Dave Birch, director at the UK research company Consult Hyperion, Hartsink is not the only person suggesting a ban on the magnetic stripe cards. In a recent blog post, Birch cited comments from a financial regulator in Singapore pressing for a "concerted, global effort to phase out magnetic stripe technology entirely."

## INTERAC Partners with INSIDE to bring Contactless Debit to Canada

Interac Association, Canada's leading payment network, announced this month a partnership with INSIDE Contactless, to develop chips containing the specifications for Interac's contactless payment service, thus enabling Interac Association and its members to offer their debit card users a "next generation" retail payments solution.

"By partnering with INSIDE, we will be able to incorporate fundamental policies, strong consumer protections, which is a vital tenet for the Canadian market, and key features, all of which are unique to Interac." said Mark O'Connell, President & CEO.

"The small-ticket purchase segment in Canada, which is still dominated by cash and coin, represents green field territory for card payments, and although this market has been targeted time and again, it has been difficult to penetrate due to the lack of the right technology solution delivered at the right cost" said Shyam Krishnan, Industry Analyst at Frost & Sullivan. "The partnership between Interac Association and INSIDE Contactless goes a long way towards creating a viable solution, providing the technology and value proposition necessary to break the barriers to this market."

## Microsoft Unveils New Biometric Games Controller

Microsoft has unveiled its new control system for the Xbox 360 console at the Electronic Entertainment Expo (E3) Gaming Conference in Los Angeles. Project Natal is a fully hands-free control system that will use biometrics, face recognition software and motion sensors to allow users to play games.

During the demonstration, British developer Peter Molyneux showed how the Natal could not only recognise faces, it could recognise facial expressions to determine what mood a player was in and react accordingly.

Videos 'Project NATAL' in action are available on You-Tube.

## O2 Expands into Personal Finance with Launch of O2 Money

O2 has partnered with NatWest to make its debut in the personal finance market with the launch of O2 Money, a new business within O2. The first products from O2 Money, will be two cash cards

The O2 Money cash cards are two completely Fee Free pre-paid Visa cards, which will help people better manage their spending money by never going overdrawn and with real-time balance updates sent to their mobile phone.

The two pre-pay cards are powered through a partnership with NatWest and are called Cash Manager and Load & Go.

Ronan Dunne continued, "O2 has a strong and successful track record of innovation and O2 Money will represent a launch pad into a wide range of mobile banking services. We believe that we are at the start of a journey towards the coming together of phone and wallet".

## HSBC firms Fined over £3m for Information Security Failings

The UK Financial Services Authority (FSA) has fined three HSBC firms over £3 million for not having adequate systems and controls in place to protect their customers' confidential details from being lost or stolen. These failings contributed to customer data being lost on two occasions.

HSBC Life UK Limited (HSBC Life) was fined £1,610,000, HSBC Actuaries and Consultants Limited (HSBC Actuaries) was fined £875,000 and HSBC Insurance Brokers Limited (HSBC Insurance Brokers) was fined £700,000.

During its investigation into the firms' data security systems and controls, the FSA found that large amounts of unencrypted customer details had been sent via post or courier to third parties. Confidential information about customers was also left on open shelves or in unlocked cabinets and could have been lost or stolen. In addition, staff were not given sufficient training on how to identify and manage risks like identity theft.

Despite increasing awareness of the need to protect people's confidential details, all three firms failed to put in place adequate procedures to manage their financial crime risks.

Margaret Cole, director of enforcement at the FSA, said: "These breaches are very disappointing. All three firms failed their customers by being careless with personal details, which could have ended up in the hands of criminals. It is also worrying that increasing awareness around the importance of keeping personal information safe and the dangers of fraud did not prompt the firms to do more to protect their customers' details.

The firms have taken a number of remedial actions to address the concerns raised, including contacting the customers concerned, improving their staff training and requiring that all electronic data in transit is encrypted.

HSBC Insurance Brokers, HSBC Actuaries and HSBC Life co-operated fully with the FSA in the course of its investigation. All three firms agreed to settle at the early stage of the FSA's investigation and qualified for a 30% discount. Without the discount, the fines would have been £1m for HSBC Insurance Brokers, £1.25m for HSBC Actuaries and £2.3m for HSBC Life.

## TJX Companies, Settles Data Loss Fine

The TJX Companies, Inc. announced that it has settled with a multi-state group of 41 Attorneys General, resolving the States' investigations relating to the criminal intrusions into TJX's computer system announced by TJX over two years ago.

TJX revealed in March 2007 that its computer systems had been illegally accessed on several occasions. 45.6 million credit and debit card numbers were stolen from the system over a period of more than 18 months during 2005 & 2006.

TJX Companies, owns discount clothes retailers T.J. Maxx and T.K.Maxx.

Jeffrey Naylor, Chief Financial and Administrative Officer of The TJX Companies, Inc., stated, "The sheer number of attacks by cyber criminals demonstrates the challenges facing the U.S. payment card system in protecting sensitive consumer data. This settlement furthers TJX's efforts to unite retailers, law enforcement, banks, and payment card companies to consider installing in the U.S. the proven card security measures that are already in use throughout much of the world."

TJX firmly believes that it did not violate any consumer protection or data security laws. The decision to enter into this settlement reflects TJX's desire to concentrate on its core business without distraction and to promote cyber security measures that will benefit all consumers.

Under the settlement, TJX has agreed to:

Provide $2.5 million to establish a new Data Security Fund for use by the States to advance effective data

security and technology.

Provide a settlement amount of $5.5 million together with $1.75 million to cover expenses related to the States' investigations.

Certify that TJX's computer system meets detailed data security requirements specified by the States.

Encourage the development of new technologies to address systemic vulnerabilities in the United States payment card system.

## Heartland Successfully Completes First Phase of End-to-End Encryption Pilot

Heartland Payment Systems during the last days of June successfully completed the first phase of its end-to-end encryption pilot project. This first step involved the transmission of live AES (Advanced Encryption Standard)-encrypted card transactions from a merchant to Heartland's processing platform. AES is the highest level of encryption and is currently on track to replace DES (Data Encryption Standard) and Triple DES as the desired standard for sensitive data.

According to Robert O. Carr, Heartland's chairman and chief executive officer, to his knowledge, this is the first time encrypted transactions have been sent from a merchant's card reader to and through a major processor's payments network.

The transactions involved a Texas-based merchant and multiple credit card, prepaid and signature debit card transactions testing each of the major card brands," Carr explained. "These cards were read by our newly developed pilot tamper-resistant security module (TRSM) terminal. The data was encrypted as the electronic digits left the magnetic stripe and entered the TRSM hardware device. The data was then successfully transmitted to and through our processing platform for authorisation and settlement.

"Typically, cardholder data is unencrypted as it leaves a merchant's terminal and is not encrypted until it is either tokenised in a gateway or at rest in the processing platform's data warehouse," Carr explains. "This means cardholder data in transit is at risk of being compromised should it get in the hands of cyber criminals or hackers via such methods as network or memory sniffer malware. To protect data throughout the lifecycle of a credit, debit or prepaid card transaction, Heartland is developing end-to-end encryption technology we call E3(TM) that is designed to encrypt the transaction from the card read through our network and ultimately through transmission to the card brands."

On Barack Obama's inauguration day (20th January 2009) Heartland Payment Systems Inc., reported a data breach of more than 100 million credit and debit card account details which seems likely to be the largest such fraud in payment card history dwarfing the TJX data breach of 45 million credit and debit card numbers stolen.

## Researchers Find Social Security Numbers can be Predicted from Publicly Available Information

Carnegie Mellon University researchers have shown that public information readily gleaned from governmental sources, commercial data bases, or online social networks can be used to routinely predict most - and sometimes all - of an individual's nine-digit Social Security number.

Project lead Alessandro Acquisti, associate professor of information technology and public policy at Carnegie Mellon's H. John Heinz III College, and Ralph Gross, a post-doctoral researcher at the Heinz College, have found that an individual's date and state of birth are sufficient to guess his or her Social Security number with great accuracy. The study findings will appear this week in the online Early Edition of the Proceedings of the National Academy of Science, and will be presented on July 29 at the BlackHat 2009 information security conference in Las Vegas. Additional information about the study and some of the issues it raises is available at http://www.ssnstudy.org.

The predictability of Social Security numbers is an unexpected consequence of seemingly unrelated policies and technological developments that, in combination, make Social Security numbers obsolete for authentication purposes, according to Acquisti and Gross. Because many businesses use Social Security numbers as passwords or for other forms of authentication - a use not anticipated when Social Security was devised in the 1930s - the predictability of the numbers increases the risk of identity theft. ID theft cost Americans almost $50 billion in 2007 alone. The Social Security Administration could mitigate this vulnerability by assigning numbers to people based on a randomised scheme, but ultimately an alternative means of authenticating identities must be adopted, the authors conclude.

"Given the inherent vulnerability of Social Security numbers, it is time to stop using them for verifying identities and redirect our efforts toward implementing secure, privacy-preserving authentication methods," Acquisti said. Methods to

consider include two-factor authentication, similar to the PIN number/card combinations used for bank accounts, and digital certificates.

## UK e-Borders Scheme Teeters

Reports this month revealed that the UK, "Government plans to force millions of travellers to hand over personal details were in chaos last night after it was claimed that the anti-terror initiative breaches European laws".

The UK's £750 million e-boarder scheme could be left in tatters after the European Commission has indicated that the scheme breaches EU law, guaranteeing the free movement of its citizens.

The scheme, which was due to be fully operational by December 2010, was to act as an early warning system for immigration officials regarding terrorists and organised criminal gangs.

Implementation of the scheme appears to be fraught with problems as it is not compatible with Belgium and French law. Ferry operators have also found it impossible to implement due to the EU Data Protection law restricting transfer of passenger data.

Chris Grayling Shadow Home Secretary said: 'It seems the Home Office is spending hundreds of millions of pounds on a system it can't legally enforce and it represents a scandalous waste of taxpayers' money.'

The UK Border Agency says it is talking with the European Commission to resolve these issues before next year.

## BT U-turn on Phorm

BT has withdrawn plans to use Phorm. "Phorm" is a behavioural advertising service that monitors a users browsing and search terms, to build an advertising profile of the user.

Since trials were conducted over a year ago Privacy issues have never been far from the news.
The European Commission said Phorm "intercepted" user data without clear consent and the UK needed to look again at its online privacy laws, which prompted an investigation by the EU. In a statement BT commented, "We continue to believe the interest based advertising category offers major benefits for consumers and publishers alike. However, given our public commitment to developing next generation broadband and television services in the UK, we have decided to weigh up the balance of resources devoted to other opportunities,"

The result of BT's decision has resulted in a sharp drop of share prices for Phorm.

## BT wins Metropolitan Police Identity Contract

BT is helping London's police force keep its buildings and computer systems secure. At the beginning of July BT announced that it had won a contract to provide Metropolitan Police officers and staff with new identity and access management services.

BT Global Services says the deal - signed with the Metropolitan Police Authority (MPA) - will help the force improve the security of its buildings and computer systems.

Mike Blackburn, BT Global Services director for central government and home affairs, said: "Integrated physical and IT security is becoming ever more important in today's society.

"By converging both physical and logical security, organisations have the ability to tighten security, audit users for compliance and deliver operational efficiencies."

Under the contract, BT will integrate elements from existing systems to create a comprehensive identity and access management system.

## RFID - a Surge in Orders

As forecasted by IDTechEx, there has been a surge in orders for RFID in 2009. Despite the world's largest RFID project, the $6 billion China National ID card scheme, being completed a year earlier, the global RFID market is rising 5% this year to $5.56 billion, in the face of the global financial meltdown which has caused some car production, for example, to plummet by 50%. In many applicational sectors, RFID orders are up 10%.

Most of the action has been in the USA, where the largest orders continue to be placed, in the UK, China and Japan.

This year, the Chinese are putting RFID where it is not encountered in the West such as in cheques and on fast fishing boats to prevent collisions. However, China is also making the world's largest investment in installing RFID throughout its factories and supply chain in order to underpin the nation's pre-eminence in manufacturing. An order for $8 million of RFID enabled casino chips has been placed by establishments in Macao and the Philippines. Hong Kong is particularly active in RFID. Japan continues to buy over 90% of the world's RFID enabled mobile phones.

# THE IMPORTANCE OF STANDARDS

## By Kevin Gillick, Executive Director of GlobalPlatform

Throughout the last few years, there have been a number of successful and high profile trials of mobile payments deployments based on Near Field Communication (NFC) technology. Thanks to these trials, the significant growth opportunities associated with enabling payments via mobile handsets have been clearly highlighted and globally understood.

These trials have also, however, illustrated that further development work is required. A sustainable, interoperable technical platform, capable of supporting NFC-enabled mobile payment applications both now and in the future, must be defined and accepted in order to achieve mass-market adoption and to realize the full potential of NFC-enabled mobile payments.

### The Need for Collaboration

The challenges involved in developing this common and neutral infrastructure become clear when the level of inter-industry interest in NFC payments is considered. New and complex business models – potentially involving banks, handset and SIM manufacturers, mobile network operators and application developers – result in the needs of all of these stakeholders having to be met. Add to this the need for the technical platform to be flexible enough to support evolving usage scenarios - despite future business models, requirements and technology being unknown - and the technical development task becomes increasingly complicated.

To support the integration of the payment and mobile technical landscapes, and to ensure that a common technical infrastructure for NFC-enabled mobile payments is defined and delivered, inter-industry collaboration is already underway. Several technical industry bodies - each with its own standards, security and business requirements - have recognized the need to cooperate and are sharing industry knowledge, technical skills and resources, in order to mitigate the risks of standards fracturing as markets converge.

### The Role of GlobalPlatform

Celebrating its 10th anniversary this year, GlobalPlatform is the leading international association focused on establishing and maintaining an interoperable and sustainable infrastructure for smart card deployments. Its technical specifications for smart cards, devices and systems are already widely adopted; as of October 2008, GlobalPlatform conservatively estimated that there were 305.7 million GlobalPlatform compliant cards deployed globally and an additional two billion mid range USIM/SIM cards worldwide using GlobalPlatform card technology to enable over-the-air (OTA) application downloads for 3G and GSM mobile networks.

In recognition of the potential role its open technical specifications could play in delivering a neutral ecosystem for the delivery of mobile services, including NFC-enabled mobile payments, GlobalPlatform established a Mobile Task Force in 2006. One of the key roles of the Task Force was, and still is, to identify, and form alliances with, technical development and standards bodies across a variety of sectors connected to mobile services. By initiating inter-industry cooperation in this way, GlobalPlatform ensures that its specifications align with the technical work of other industry bodies and take into account the requirements of various market sectors. Additionally, by pooling knowledge and resources with other technical development organizations, GlobalPlatform ensures that work efforts are streamlined; the result is the development of non-conflicting technical standards.

GlobalPlatform's current collaborations involve liaisons with a number of technical bodies to develop different components of, or address various issues associated with, an interoperable ecosystem for NFC-enabled mobile payments. Below is a summary of recent / intended outputs from those liaisons:

- GlobalPlatform and the Association Européenne Payez Mobile (AEPM): In July 2009, GlobalPlatform signed a Memorandum of Understanding (MoU) with the AEPM, which develops specifications and facilitates trials to promote and accelerate the deployment of contactless mobile payment in Europe. GlobalPlatform and the AEPM will align their future development work to assist the market in bringing convenient, secure and user-friendly mobile payment services to European citizens. The organizations will also work together to further detail revolutionary mobile payment business models that will encourage end-user adoption.

- GlobalPlatform and EMVCo: GlobalPlatform has been formally working with EMVCo's Mobile Payments Working Group since 2008. EMVCo is the body responsible for developing and maintaining the EMV Specifications for the global payments industry. The aim of this relationship is to advance GlobalPlatform's Specifications relative to secure content management on mobile devices, ensuring that the technology meets EMVCo's application management requirements – including over-the-air (OTA) download and personalization – for mobile devices.

- GlobalPlatform and the European Payments Council (EPC): In May 2009, GlobalPlatform signed a MoU with the EPC – the decision making body of the European payments industry. This formal collaboration between the organizations aims to ensure that the bodies develop compatible mobile contactless technical specifications and use cases which adhere to pre-defined common requirements for mobile payments.

- GlobalPlatform and the European Telecommunications Standards Institute (ETSI): GlobalPlatform's collaborations with established telecom standards organization ETSI have been ongoing since 1999. Most recently, GlobalPlatform has addressed an ETSI requirement for the confidential loading of applications on USIM cards with Amendment A to GlobalPlatform Card Specification v2.2. Both organizations are currently working on contactless application selection and installation.
- GlobalPlatform and the Open Mobile Terminal Platform (OMTP): GlobalPlatform has been collaborating with the OMTP, a forum created by mobile network operators to discuss requirements for mobile devices, since 2005. GlobalPlatform has addressed an OMTP requirement for the trusted execution environment by publishing an extension to its device technology as well as the Device and Application Management Security (DASM) Specification.
- GlobalPlatform and StoLPaN: In February 2009, GlobalPlatform announced it would be aligning its development work with the activities of StoLPaN, a Pan-European consortium which aims to identify the technical and commercial frameworks required to securely deliver NFC applications to mobile devices. This collaboration will ensure the long-term compatibility between each body's respective approach to the development of NFC deployment.

GlobalPlatform's collaboration efforts, throughout the mobile payments and all other market sectors, are central to ensuring that GlobalPlatform Specifications offer a resulting technology platform which is truly interoperable and universally relevant. To safeguard the integrity of the GlobalPlatform Specifications and provide a method of 'quality control' to the global marketplace, GlobalPlatform has invested significant time and resources over recent years in developing a compliance program to ensure that GlobalPlatform compliant products do in fact conform to the requirements defined by the specifications. This compliance program, which is scheduled for completion in Q1 2010, comprises significant input from various industry bodies across sectors and in terms of mobile payments will play a significant role in expediting the process of developers and bringing products to market.

**The GlobalPlatform UICC Configuration**

One of GlobalPlatform's most significant outputs in the past twelve months has been the publication, in October 2008, of its UICC Configuration – a technical document which outlines a common and neutral environment to facilitate the secure delivery, over-the-air, of new and creative mobile services to consumers. It is the implementation guide for deploying GlobalPlatform Card Specification v2.2 within the mobile services sector and managing the secure delivery over-the-air of new services.

Utilizing its cross-industry representation and collaboration with other technical industry bodies, including EMVCo, ETSI, GSM Association and the Mobey Forum, GlobalPlatform combined mobile telecom and financial market knowledge with its technology experience to develop a configuration which outlines the behaviour of each and every actor involved within a UICC implementation, how they should be represented, and a summary of their role / responsibilities in a variety of business models. Cross industry contributions were vital to ensure that the document addressed the security requirements of all mobile services stakeholders and to secure universal acceptance of this document.

The GlobalPlatform UICC Configuration stands as a fine example of the significant, market-enhancing development work that can be achieved through inter-industry collaboration. For further information on the UICC Configuration, visit www.globalplatform.org.

**Evolving Demands**

A second role of GlobalPlatform's Mobile Task Force is to determine whether it is necessary to update the GlobalPlatform Specifications in line with emerging market or application requirements from the mobile services sector. The ultimate goal is to ensure synergy between the organization's technical output and evolving industry demands.

As part of this remit, the GlobalPlatform Mobile Task Force has recently identified the value GlobalPlatform technology can offer the transport sector by enabling contactless fare collection and ticketing. A GlobalPlatform Transportation sub-Task Force is subsequently soon to be launched under the GlobalPlatform Mobile Task Force, with the aim of educating the transit sector about the benefits of deploying a neutral, scalable and interoperable infrastructure for mobile fare collection and ticketing services. One of the group's first work items will be to develop a white paper explaining how GlobalPlatform Specifications provide an environment where cross-industry applications can coexist on a common platform in a secure and standardized way and to ultimately outline GlobalPlatform's value proposition to the transit sector.

Over the next few years, the GlobalPlatform Transportation sub-Task Force will reach out to actors within the transit sector to raise awareness of GlobalPlatform's proven technology and demonstrate the value it can add to new implementations. Through its outreach efforts and increasing relevance to the transportation industry, GlobalPlatform hopes to engage more transit organizations globally in its technical development work, to ensure that GlobalPlatform continues to align its technology to meet the mobile payments and wider mobile services requirements of the transport community.

# Interview with Morten Landrock, UK Managing Director of Cryptomathic

By Tom Tainton, Smartcard & Identity News

*Tom Tainton*

### What is Cryptomathic?

Founded in 1986, Cryptomathic's origin is contained in the company's name: cryptology and mathematics. Initially, our core area of business was to deliver cryptographic algorithms to banks, which in turn were integrated into their own solutions. Technology has advanced significantly and now a rising number of new markets require complex and highly secure systems and procedures to maintain the confidentiality and integrity of data.

We capitalised on this trend and today Cryptomathic is a leading provider of bespoke security solutions to organisations operating across a wide range of sectors including finance, smart card, digital rights management and government. We offer systems for e-banking, two-factor authentication (2FA), public key infrastructure (PKI) initiatives, EMV card issuing, ePassport and advanced key management, which contribute directly to our customers' core business activities. Essentially, we specialise in areas where cryptographic security is an essential and critical requirement.

### In what sectors has Cryptomathic experienced the most success?

Cryptomathic has been successful across a number of different industry sectors, in particular banking, government and digital rights management:

### Banking:

Although the migration to EMV and the banking sector's continued use of the internet to deliver services has created new opportunities for banks and improved convenience for customers, such advances have also resulted in increasingly sophisticated financial attacks from fraudsters. It is a continuing and complex process to ensure banking networks are successfully protecting sensitive data from existing and future threats, as most banks are operating a legacy IT system which was originally created for functionality and not security.

This is made even more challenging by the pace at which technology has advanced over the last decade, which would have been unimaginable when these IT systems were first introduced. With the 2008 APACS fraud figures (published in March 2009) revealing an ongoing increase in card-not-present fraud and a startling rise in identity theft – up by a third from six to eight per cent of total fraud - it is without doubt that Cryptomathic's expertise will continue to be in strong demand from this market.

### Government:

By transferring our knowledge from securing highly sensitive data within the banking sector into the progressive ePassport landscape, we have developed and implemented solutions which guarantee the security of the biometrics data held within a machine readable travel document or eID card. Taking this one step further, Cryptomathic has designed the technology required to 'speed up' the ability of border controllers to access biometric details without impacting the integrity of the infrastructure or application. Due to our work with the UK Identity and Passport Service to deliver a public key infrastructure (PKI) solution in 2006, our consultancy, product offering and visibility in this area has gone from strength to strength. This skill-set has also been used to support the delivery of government ID initiatives.

### Digital Rights Management (DRM):

As technology becomes increasing mobile, so does data, which raises new concerns regarding the protection of copyright information and its management. Interest has grown considerably in the creation of a trusted environment for protecting data, which will still enable access by authorised users. PKI is mostly known for electronic commerce and personalised digital signatures with the aim of preventing illegal use of digital contents by unauthorised users. However, there are currently a number of very large, 'transparent' PKI solutions for DRM in mobile phones and Trusted Platform Modules in PCs. Cryptomathic has witnessed an increase in demand for these specialised large scale solutions.

### Who would you say to date is Cryptomathic's main competition?

As one of the first companies to commercialise cryptographic algorithms, Cryptomathic has used its academic base to pre-empt new security requirements brought about by emerging technologies or regulatory decisions. This enables us to react to specific and individual client and industry needs in a timely manner. Our biggest competition comes from organisations that decide to develop solutions in-house rather than use an outside agency, which is usually a commercial decision.

### What are the benefits of Cryptomathic products over those of its competitors?

All of Cryptomathic's products are designed and built to specifically meet customer requirements today and are adaptable to future needs. Ensuring a solution is sustainable in the long-term is core in all our services, but is something that many systems developed in-house fail to acknowledge or accommodate, resulting in expensive amendments and time intensive upgrades.

### Despite the current economic circumstances do you still see a significant demand for your products in the industry?

Not only is there still a strong demand for our offering, but we have also witnessed new business growth, particularly from the financial sector. Although banks are under increasing pressure to economise without compromising levels of security, fraud costs the industry millions of pounds each year and implementing e-security solutions can eliminate this criminal exposure and the associated losses. Such systems are automated, which can also reduce demand on internal resources and human error; all of which save banks money.

### What security products do you see as having the greatest potential for adoption?

Due to the convergence of industry sectors, and the fast pace at which innovative multiple-partnership solutions are coming to market, scalable, reliable, flexible and secure server solutions have the greatest potential for adoption. Products that span payments and mobile in particular are currently experiencing a rapid rise in demand.

### What are the main challenges facing the company in 2009?

Cryptomathic's main challenge at present is the management of our global expansion strategy. We have an established office network throughout Europe and last year opened a new office in Canada to provide our US and Canadian-based customers with local business and technical support. With a rising demand in North America, Middle East and Asia for security solutions, in particular orders for EMV data preparation solutions for contact and contact less payment cards, as well as automated key management systems, 2FA technologies and PKI expertise, it is logical for us to raise our global visibility.

### What does the future hold for Cryptomathic?

The security solutions market we address is likely to continue growing strongly for the foreseeable future, as there will always be a demand for cryptography-based products.

In the coming years, a key area of focus will be the integration of biometrics with cryptography based solutions. Both technologies are very effective and offer different benefits in a range of scenarios. Cryptographic solutions - particularly when combined with a Hardware Security Module (HSM) - are so robust that the only challenge that has arisen has been from other sources.

For example, a bank will never experience a threat on the cryptography of its systems. The weaknesses originate from connections to the customer/bank interface and are most commonly exploited by attacks based on trojan, phishing, pharming techniques. In this instance, and many others, cryptography and biometrics can work together advantageously to provide increased assurances of security.

In the long-term, we intend to grow our company and further extend our portfolio of proven solutions through a pre-determined acquisitions strategy. Our overarching aim is to continue to deliver functional solutions and support, with a real return on investment, to a portfolio of happy and loyal customers.