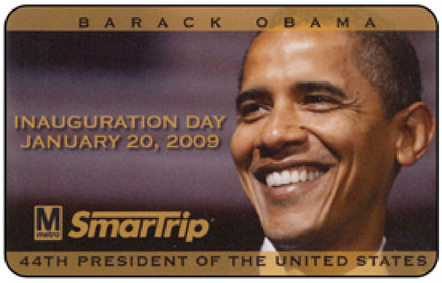
January 2009

Volume 18 • Number 1

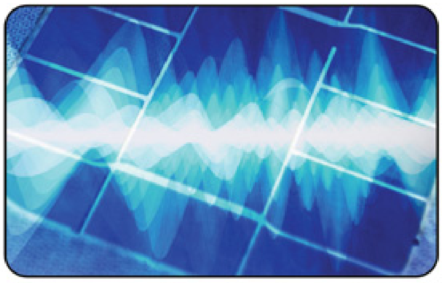
# Smart Card & Identity News

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

www.smartcard.co.uk


BARACK OBAMA
INAUGURATION DAY JANUARY 20, 2009
SmarTrip
44TH PRESIDENT OF THE UNITED STATES

*6 • Obama Inaugural SmarTrip Cards*



*10 • Safe-Guarding Products Against Power Analysis Attacks*

*16 • "Mobile World" - Meeting of the Smart Card Club*

*18 • Barclays launches NFC Debit Card*

# Heartland Credit/Debit Card Data Loss Greatest in World History?

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 in 2007.

The company handles more than 100 million credit/debit card transactions every month for their 250,000 business clients. These customers cover every branch of industry from retailers to restaurants (about 40% of their business transactions) and suggestions are that people in just about every state in the USA are affected by this fraud.

In the case of TJX the fraudsters intercepted wireless payment card transactions made within the stores over several years. At that time (and still in some cases today) these businesses were only using the weak and deprecated security of WEP (Wireless Equivalent Privacy) used by the early adopters of IEEE 802.11 Wi-Fi. In the Heartland case the fraudsters introduced sniffing malware into the data centres that intercepted the data captured from the credit and debit card magnetic stripes from their clients.

**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 -** Lesley Dann, John Owen

**Contributors to this Issue** – David Everett, Tom Tainton, Peter Hawkes, Ken Warren, Jean-Pierre Delesse,

**Photos** - Julián Rovagnati (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.

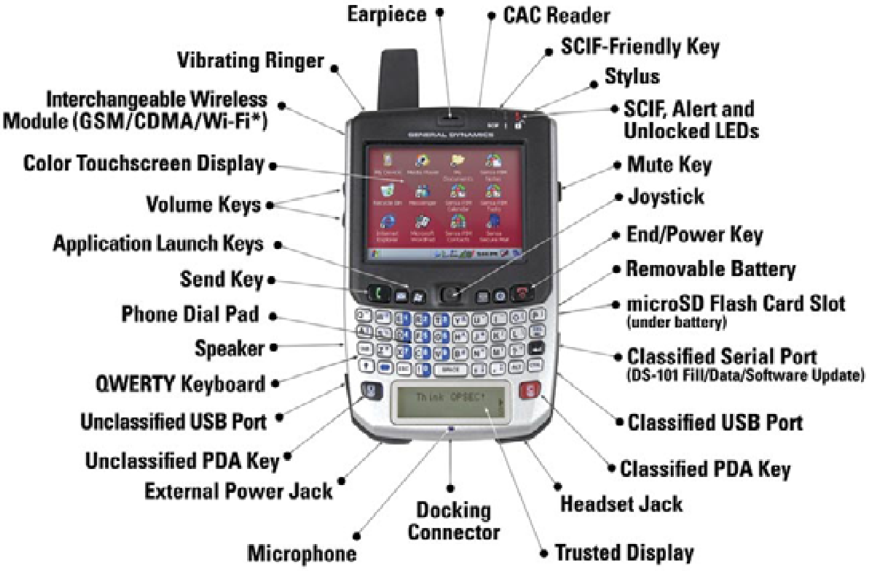
# Our Comments

***Patsy Everett***

Dear Subscribers

It's difficult to let this month go by without commenting on the Presidential Inauguration of Barack Obama in the USA. Well perhaps not so much the ceremony but how about some of the technical implications. The new president is reputed to be the most technocratic of any major power and arguably the USA leads the field. So will we see smart cards dangling from his pocket?

First things first, that Blackberry which the President has said would have to be prised out of his hands. It hasn't taken long but we have already heard that its going to be replaced by a General Dynamics Sectera Edge PDA and knowing how you guys out there want the latest gadget information here is a picture of the mighty beast,



*The Sectéra® Edge™ smartphone converges secure wireless voice and data by combining the functionality of a wireless phone and PDA — all in one easy-to-use handheld device. Developed for the National Security Agency's Secure Mobile Environment Portable Electronic Device (SME PED) program, the Sectéra Edge is certified to protect wireless voice communications classified Top Secret and below as well as access e-mail and websites classified Secret and below.*

*The Sectéra Edge is the only SME PED that switches between an integrated classified and unclassified PDA with a single key press.*

I couldn't resist it, straight from the General Dynamics web site and clearly some very serious PDA indeed if it can handle voice at Top Secret and data at Secret and all this with a Microsoft Mobile operating system. Note also the Classified USB port which could be a good place to connect your smart card or USB cryptographic token. Perhaps I'm getting cynical in my old age but I don't see this device as a replacement for the friendly Blackberry, I'll have a little bet that he doesn't use it and somehow get's his Blackberry back but I just wanted to share with you what the NSA deems to be a secure mobile phone/PDA. Oh and by the way guys just in case you wanted to keep up this little PDA will set you back well over $3,000. We

probably are all well aware that standard mobile phones and PDA are lacking security functionality and yet it has become an everyday tool in Government, NHS and all the other places you can imagine that handle sensitive citizen data.

And just to put all this in perspective the Computer Security Institute's 2008 Computer Crime & Security Survey in the USA found that information breaches cost companies an average of nearly $300,000 a year. The Institute also estimated that the average major corporation loses (lost or stolen) 640 laptops, 1,985 USB memory sticks, 1,075 smart phones and 1,324 other data devices per year. The institute estimates that each year up to 800,000 memory devices (laptops, smart phones, memory sticks) are lost or stolen. Mind you I don't suppose Barack Obama is likely to lose his PDA, but just imagine a courtesy car in some foreign country and we all know how the phone can fall out of your coat, trousers, bag or purse, doesn't bear thinking about.

And that watch, well according to Washington insiders Barack's political advisors weren't to happy with his watch, a $600 Tag Heuer Series 1500 divers watch that he bought in the early 90's so they all clubbed together to buy him a new watch.

It's a Jorg Gray 6500 chronometer selling for about $200 except this one is a little special in that it has a special logo for the United States Secret Service and can only be bought in their employee's shop. There were rumours that his advisors though the Tag Heuer looked too expensive but maybe he just wanted a new watch.

Anyway with all this technology going on behind the scenes I'm betting that we are going to be seeing more on electronic ID and perhaps at long last the USA will give up on magnetic stripe cards and start using chip & PIN like everybody else, see our lead article for more details on the latest financial card data loss.

Don't forget it's the GSMA Mobile World Congress in Barcelona February 16-19th, I hope to be meeting some of you there.

Patsy.

## Contents

### Regular Features

### Industry Articles

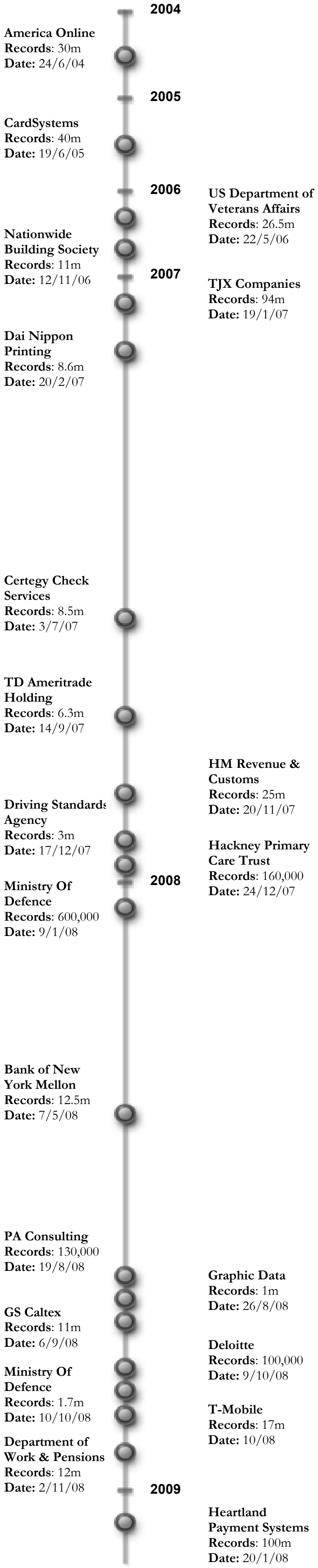
## Events Diary

**February 2009**

| | |
|---|---|
| 16-19 | GSMA Mobile World Congress, Barcelona, Spain - www.mobileworldcongress.com |
| 24-26 | NFC Congress, Hagenberg, Austria - www.nfc-research.at |
| 26-27 | Global Commercial Cards & Payments Summit - www.commercialpaymentsinternational.com |

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

…. Continued from page 1



This data is of course sufficient to create counterfeit magnetic stripe credit and debit cards that could be used to plunder the bank accounts of the innocent card holders. Worse than that of course is that the more intelligent fraudsters might just take a little bit here and there which in many cases will probably go undetected.

Apparently the fraudsters introduced the malware about May 2008 but Heartland weren't aware of the problem until late autumn 2008 and then only after Visa and Mastercard started reporting fraudulent activity reports that resulted from payments made by merchants whose transactions were processed by Heartland. As we mentioned previously Heartland saved up the day of confession until Inauguration day, one where the eyes of the world were looking elsewhere. Robert Baldwin Jr, Heartland's President and Chief Financial Officer has said that it is too early to estimate how many people have been affected and that comparison with TJX is premature. The TJX total losses have been estimated at up to $1 billion and pro-rata we might expect this to be twice as much.

Where do you start on something almost unbelievable on this scale, how on earth can consumers and citizens ever trust those organisations that handle their private data in whatever form?

In the first instance one has to wonder what has happened to the PCI-DSS (Payment Card Industry – Data Security Standard) which is designed to provide the necessary assurance that frauds of this ilk should not happen. Every organisation that stores or processes consumer credit and debit card information is subject to the fairly stringent requirements of the DSS and should have been evaluated and certified to be meeting the requirements. One doesn't want to speculate without full knowledge of the facts but it does seem as though the company was guilty of lax protective monitoring controls and more to the point that it escaped audit detection by 3rd parties.

The other interesting point is that given Visa and Mastercard were aware that something was amiss as early as autumn 2008 why did nothing happen in the interim months?

And then you have to ask, why is the USA not pursuing a chip & PIN strategy? Mastercard and Visa are forcing its adoption in most other major countries (the UK back in 2002) by moving liability for the charge back of fraudulent payments to the party not using chip & PIN. As long as magnetic stripe payment cards are in widespread use there is a simple fraud attack path for the crooks. It is easy to counterfeit a magnetic stripe card it is extremely difficult to counterfeit a modern smart card chip that can exhibit the necessary cryptographic functionality, assuming it is of course tested as part of the transaction authorisation but that is another matter.

This data loss seems to set the scene for another year of problems which is clearly escalating year by year as shown in the timeline for data loss aside

The problem is that consumers are going to lose confidence in payment systems and the management of citizen data by government departments. It is really surprising that these frauds are taking place using well known attack paths and that large enterprises have such totally inadequate controls in place.

David Everett

# World News In Brief

## Smart Card News Obituary - Jack Smith

As many of our long term readers may remember, Jack Smith was the editor of our newsletter until 2002. Sadly Jack passed away earlier this month in his beloved country of France.

I have known Jack since the early 1980's when he was a hack with the local paper. Jack joined David's (my husband)security company as our PR consultant working along side me. Although a Scott from Glasgow, Jack hated the cold, damp climate of the UK and decided to move to the South of France in the early 1990's where he could enjoy the wine and sunshine. When David and I decided there was a need for a newsletter for the smart card industry we immediately thought of Jack and he jumped at the idea as long as he could work from France.

I am sad to say we lost touch a few years ago but he will be remembered for his many stories about working on a Scottish paper, his Navy days as a PR officer and when he owned and ran a wine bar in Brighton. I hope where ever he is now there is plenty of sunshine and good wine.

Patsy

## UK Information Commissioner's Office ICO Takes Action against Home Office and NHS for Serious Data Breaches

The Information Commissioner's Office (ICO) has found the Home Office in breach of the Data Protection Act after a contractor, PA Consulting, lost an unencrypted memory stick holding sensitive personal details of thousands of individuals in August 2008. Details lost included information about individuals serving custodial sentences and those who had previously been convicted of criminal offences.

ICO has also found Abertawe Bro Morgannwg University NHS Trust and Tees, Esk and Wear Valleys NHS Foundation Trust in breach of the Data Protection Act.

An unencrypted laptop containing the sensitive personal data of approximately 5,000 patients, including some health records, was stolen from the Abertawe Bro Morgannwg University NHS Trust.

An unencrypted memory stick had been lost containing sensitive personal information relating to patients and Trust staff from Tees, Esk and Wear Valleys NHS Foundation.

The ICO has required the Home Office and both NHS trusts to sign a formal Undertaking outlining that they will process personal information in line with the Data Protection Act.

Both organisations will implement a number of security measures to protect personal information more effectively. With immediate effect, all portable and mobile devices, which are used to store and transmit personal information, must be encrypted. Any organisation processing personal information on behalf of the data controlling company must also use encryption software, a requirement, which must be clearly stated in all contracts.

The Trusts will also implement a number of security measures to protect personal information more effectively.

Mick Gorrill, Assistant Information Commissioner at the ICO, said: "We are investigating a number of the most serious reported data breaches. The Data Protection Act clearly states that organisations must take appropriate measures to ensure that personal information is kept secure. Failure to meet the terms of the Undertaking is likely to lead to further enforcement action by the ICO."

## EU Schengen Border Control Database in Crisis

EU ministers met up in Prague on the 15th for an Informal Meeting on EU Home Affairs.
At the afternoon part of the meeting the Ministers discussed the issue of development of the second-generation Schengen Information System.

The common Schengen Information System is a database used primarily to search for persons and property in the Schengen area). The Schengen area comprises of EU states where border controls are not conducted at their internal borders. This Schengen Information System replaces the abolished EU internal border controls.

"We have just addressed the present situation in the development of SIS II with all EU and Schengen Ministers and we have agreed that this project is, in fact, in a crisis that needs to be solved immediately. The Czech Presidency determined the solution of the crisis of this project as one of its priorities and it will make maximum effort to revive it and transfer it to the Swedish Presidency in a healthy state", stated Minister of the Interior Ivan Langer.

The Ministers supported the plan of the Czech Presidency that consists of a series of interconnected measures. Beside the revival of the current project, preparation of a back-up solution is also part of this plan. The final decision on the direction of the SIS will be adopted no later than June 2009. The Schengen information system is one of the most important tools of cooperation for states that have cancelled internal border checks and the Czech Presidency feels that its modernisation and inclusion of new functions is a key issue.

"I hope that three or four months is enough to be able to find a solution," continued Langer.

## EU Officials Raid Smartcard Chipmakers

It has recently been revealed that European Union antitrust officials carried out unannounced inspections at the premises of several smart card chips producers in several member states on the 21st October 2008.

"The commission has reason to believe that the companies concerned may have violated EC treaty rules prohibiting practices such as price fixing, customer allocation and the exchange of commercially sensitive information," the statement read.

The companies involved are STMicroelectronics, Infineon Technologies, NXP, and Renesas Technology have received surprise visits from investigators.

The Commission, competition watchdog of the 27-nation European Union, said it was not prejudging the outcome of its investigation. "The Commission respects the rights of defence, in particular the right of companies to be heard in antitrust proceedings," the statement said.

It said it had no strict deadline to complete its investigation.

## Obama Inaugural SmarTrip Cards

Giesecke & Devrient (G&D) has delivered 200,000 limited edition SmarTrip cards to the Washington Metropolitan Area Transit Authority (WMATA) in order to commemorate the historic occasion of President Obama's inauguration.

The new gold-trimmed cards feature a picture of President Barack Obama and the words "Inauguration Day January 20, 2009, the 44th President of the United States."

The card body was made from a PVC/PET composite material, making them more durable and more eco-friendly. Public transit passengers are able to buy these commemorative cards for $10 each online or at Metro sales centres.

As with other SmarTrip cards, passengers will be able to add value to the cards so they can use them indefinitely. SmarTrip cards are used by millions of commuters in Washington, D.C.

## NXP SmartMX Choosen to Power German Transport Ticketing

NXP, announced that its secure contactless microcontroller chip - SmartMX, has been selected by the VDV-Kernapplikations GmbH & Co. KG, to power future electronic transport ticketing schemes in Germany. Alongside card and inlay-manufacturer Cardag, NXP will provide SmartMX ICs for around eight million contactless cards to be issued throughout Germany by 2012. The aim of the scheme is to provide a single ticketing solution that will be used across all nationwide transport networks.

NXP's contactless microcontroller technology will be integrated in smart cards created and personalised by Cardag, and is fully compliant with the VDV-Kernapplikation (Core Application), the national data and interface standard defined for contactless ticketing and automatic fare collection in Germany. The development of the standard was driven by the German Federal Ministry of Transport, Building and Urban Affairs to ensure standardised electronic tickets in a range of formats such as smart cards, bank cards and mobile devices would be fully interoperable for use within public transport schemes throughout the country and internationally.

## Qimonda files for Bankruptcy

Global memory supplier Qimonda on the 23rd January filed an application with the local court in Munich to open insolvency proceedings. Their goal is to reorganise the companies as part of the ongoing restructuring program. The court has appointed insolvency administrator Dr. Michael Jaffé.

The insolvency petition is the result of the massive drop in prices in the DRAM industry and dramatically decreased access to financing on the capital markets, both of which have led to the deterioration of the financial position of Qimonda in recent months. A financing package involving the Free State of Saxony, parent company Infineon, a leading Portuguese financial institution and additional banks could not be completed in time, despite intensive but also very complex negotiations and financial support committed by customers over the past days and weeks. Furthermore, an increased need for financing for the current financial year recently became apparent as a consequence of the price decline in the December quarter and the fact that important investments needed for productivity improvements could not be made due to the delay in negotiations.

The temporary insolvency administrator will analyze the situation at Qimonda in the coming days. “We assume we will be able to continue our business within the context of our restructuring program with the support of the temporary insolvency administrator and our employees,” Loh said. “We are especially counting on the excellent relationships with our customers and suppliers, with whom we have made significant progress in developing our Buried Wordline technology during the last months.”

## Nexus Seeks Government funding for Smart Card Pilot Projects

Nexus (UK) is the Tyne and Wear Passenger Transport Executive and fund administrators. Nexus has announced it hopes for approval from the Passenger Transport Authority at its January 2009 meeting to submit a bid for Government funding for pilot projects.

Nexus is to work together with bus operators across North East England to develop the region's first smart ticketing technology for public transport. The plans would see passengers able to travel anywhere from the Scottish border to the Tees Valley, using a single 'intelligent' card in place of cash.

If pilot projects are successful next year then a full scheme could be ready to start in three years time.

## NXP Announced Appointment of Richard L. Clemmer as CEO

NXP Semiconductors, announced the appointment of Richard L. Clemmer as President and Chief Executive Officer. Mr. Clemmer succeeds Frans van Houten who is leaving NXP.

Sir Peter Bonfield, Chairman of the Supervisory Board of NXP, said: "I am pleased to welcome Richard Clemmer as the new CEO. Rick has extensive executive leadership experience in the high tech industry, including semiconductor, storage, e-Commerce, and software companies. He is very familiar with NXP and well suited to bring NXP to the next level."

## Standardised Coding on all EU Pharmaceutical Packaging

Honeywell have announced that its full line of area-imaging scanners meet the requirements of healthcare customers preparing for the planned EU initiative that will require 2D bar codes on all pharmaceutical packaging within Europe. The regulation aims to provide transparency and full trace-ability within the complex European supply chain.

The European Association of Hospital Pharmacists (EAHP) and the European Federation of Pharmaceutical Industries and Associations (EFPIA) have both called for a regulation that requires pharmaceuticals to carry a 2D bar code on their packaging. After an extensive study by the EFPIA, 2D bar codes were selected as the technology of choice due to their ability to store large amounts of information in limited amounts of space.

The pending legislation is designed to improve patient safety by reducing the level of counterfeit medicine within the European pharmaceutical supply chain. EU statistics released on 19 May 2008 confirm that 4.1 million medicinal articles were detained at EU customs borders in 2007, a 51% increase over the previous year.

## Gemalto Formally Terminates its Offer for Wavecom

Gemalto has announced that it has terminated its French tender offer for Wavecom, in accordance with Article 232 - 11 of the French Financial Markets Authority (AMF) General Regulations. The U.S. tender offer has also been formally withdrawn and terminated.

## Contract with BT for the NHS National Data Spine

Intercede announced this month that it has signed a contract with British Telecom (BT) for the supply of the MyID Identity and Credential Management System in support of the National Health Service (NHS) National Data Spine. BT had previously been supplied with Intercede's MyID software and services indirectly through an Intercede business partner. All new orders will now be placed directly with Intercede.

The National Programme for IT in the NHS is the largest civilian IT programme in the world. Intercede is midway through supplying MyID software licences to enable the issuance of up to 1.2 million smart cards to healthcare staff throughout the United Kingdom. Over the last 4 years, more than 500,000 smart cards have been issued.

# Smart Government Forum

## London, December 11th 2008

**By Peter Hawkes, Smart card & Identity News.**

***Peter Hawkes***

Smartex has been running this forum for some years. The emphasis is smart card enabled services, which are or may be provided by the UK Government and Local Authorities such as Town and County Councils. At this meeting there were three main presentations, which all led to lively discussions from an enthusiastic and well-informed audience.

### Talk 1

Richard Poynder, the Founder of Smartex, gave the first talk. His topic was "Local Authority smart cards: do they have a future?" He described himself as "The grumpy old man of the Smart Card Industry". He outlined the state of play with local authority smart cards as already issued to residents in Scotland, Wales and England. This was followed by his radical suggestions to ensure wider benefits for cardholders.

Of the three regions Scotland has achieved the most. Wales comes last. Apparently the devolved Government of Wales has no budget to build on the initiatives already started. Across all three Regions many Local Authorities (LAs) have now issued concessionary travel cards to the Elderly and disabled persons. However only a few schemes allow free travel outside the cardholder's home LA area.

Cards for other purposes are limited to "boring" applications such as library, schools facilities and leisure centres. Richard is pessimistic about further prospects if the LA's are left to enlarge the market by their own efforts. The whole initiative could die.

His suggestions for the future would involve sweeping changes from the status quo. Card issuance and ownership would not be left to the LA's. The Banks, Transport operators and Retailers are considered to be the best organisations to introduce cards for citizens with truly useful "primary" applications. The LA applications would be accommodated as secondary applications sharing space on the card. It has been technically possible to produce such multi-application smart cards for at least a decade. However there have been few examples of successful deployment. An obvious difficulty is in deciding which organisation takes responsibility for the various functions of the card system. Security is one example of a function where responsibility is hard to allocate.

### Talk2

David Rennie, Independent Consultant, followed Richard with a talk on "Access to Public Services". David has been a consultant to the Treasury where he was in the support team for the Public and Private Partnership on Identity Management. This resulted in the Crosby Report on Identity Assurance.

David has also consulted to the Identity and Passport Service (IPS) on Identity services. Currently he advises on the Direct Government Web site- www.directgov.gov.uk

This site was new to me and perhaps to others at the meeting. The stated aim is for it to be the official government web site for citizens. It is intended to provide easy access to "the public services you use and the information you need, delivered by the UK government". LA services are included.

Of the services available so far one of the most used is for renewal of the annual car tax. The mandate of Directgov was set by the Varney Review of 2006. This was that "by 2012 Directgov is the primary electronic channel to citizens for government and is a place citizens can turn to for the latest and widest range of public services". The Directgov initiative is matched by Businesslink.gov for businesses. "…the aim is almost all online information and transactions will be easily available through these two sites". David summarised the strategic aim of Directgov as "Directgov will be at the heart of the relationship between government and citizen in the digital space".

To this end he showed a plot of the total number of central government web sites against time from March 2007. At that date there were about 770. The forecast for March 2011 is around 50. Usability is seen as key to the forecast growth in traffic. Besides inquiries transactions are often necessary-paying for car tax is an example.

Many transactions require Identity authentication.
David divided the requirements for authentication of transactions in to 4 levels:-

- Level 0 – No identity data required
- Level 1 – balance of probabilities
- Level 2 – substantial assurance
- Level 3 – beyond reasonable doubt

He pointed out that currently a wide variety of methods are used. "Government Gateway" is the method chosen by many public service providers.  The Web site for this is www.gateway.gov.uk

Unsurprisingly he sees Registration as a deterrent to customer engagement. Registration can be anonymous. Multiple Government Gateway accounts can be created. The specific (Government) service provider determines the enrolment process. This is because different identity attributes are required for some services. The basic authentication method is considered to be Level 1.

A user ID and password thereafter provide the mechanism across all services i.e. the aim is "single sign-on". Usage has two peaks per year. These are for HM Revenue & Customs for income tax returns. Work in progress to achieve "single sign-on" was outlined. Sensibly this distinguishes between proof of (personal) identity and possession of credentials. Obtaining Level 3 registration would, he said, necessitate the same sort of personal information as is soon to be required for an e-passport. That is :-

- Provision of validated (biographical) data
- Authentication of this Identity
- Authentication of that person's biometric data (to bind it to the Identity).

So level 3 registration is going to need an initial face to face interview procedure plus a biometric enrolment (face and fingerprints).
Level 2 can rely on the postal loop. The User ID and any necessary activation code are sent through the post to the person registering. Level 1 can proceed remotely. I was impressed with the progress made with the Directgov channel for the supply of information to citizens.

The transactional side via Government Direct strikes me as a much tougher challenge. Identity fraud may become rife. If it does the Government will need to issue every citizen with a two-factor authentication device.

## Talk 3

The last of the main presentations was by Andrew Henderson. He is Sales Director of Giesecke & Devrient GB Ltd. He gave an overview of smart card opportunities in the UK public sector. For convenience these opportunities were divided in to Large Scale and Small Scale opportunities. The Large scale opportunities in the Public Sector are dominated by ID related ones. These include the e-passport and the proposed National ID card. The latter is likely to function additionally as an intra-EU travel document. This need for pan- European inter-operability raises the question of conformance to ECC standards. Such Standards require consensus between States. They therefore take time to evolve. This is at odds with the rapid prototyping and implementation achievable with proprietary designs.

Technology providers like G&D tend to work with System integrators in Europe. In other markets they have to take on the System Integrator's role. There are some quite big opportunities in UK at the local level. One of the largest ones so far in the UK is the Centro National Concessionary travel pass. This is issued by Centro to the over-60's, blind and disabled persons for free travel on any local bus service at off-peak times. 430,000 persons living in the West Midlands now have such cards. It is part of the English National Concessionary Travel Scheme (ENCTS).

On a completely different tack Andrew reminded us that some future opportunities might be based on alternative card formats. An example he cited is a version of the Micro SD card. Called the StarSign® Micro SD card it is based on the G&D Secure Micro SD token with a USB Adaptor. Helixion of Edinburgh uses the StarSign card as the basis of a security system for mobile data communicating devices including GSM to be connected to a remote server. See lok-Id on www.helixion.com

**Conclusion -** This was an excellent meeting fully up to the high standards set by Smartex.

# Safe-Guarding Products Against Power Analysis Attacks

By Ken Warren, Cryptography Research Inc.

*Ken Warren*

In order to provide confidence that tamper resistant cryptographic devices are secure, it is important that they are adequately tested for resistance to side channel vulnerabilities such as Simple Power Analysis (SPA) and Differential Power Analysis (DPA).

It is widely recognized that expert Independent testing is essential for validating the presence and effectiveness of countermeasures for power analysis attacks. However, not all independent reviews are equal. Gaining confidence in a security evaluation depends on many factors including the comprehensiveness of the evaluation, the expertise of the evaluator, the design of the device and the level of access the evaluator has to design information. Whilst insecurity in a vulnerable device can be clearly revealed, demonstrating that a device is secure can be less straightforward.

Cryptography Research Inc (CRI) developed its DPA Countermeasure Validation Program in response to comments and observations from security experts that many existing evaluation schemes are inadequate when it comes to testing for side channel vulnerabilities – particularly SPA and DPA. Testing for these vulnerabilities requires a certain amount of creativity for the tester, so static evaluation models in particular tend to produce inconsistent results.

CRI's DPA certification program builds on the testing procedures used in Common Criteria, and adds additional testing requirements. These enhancements embrace a more comprehensive and fluid testing procedure that is designed to ensure high quality security testing of products against SPA and DPA attacks. Products which successfully pass the tests earn the right to use CRI's trademarked DPA Security Logo in association with the certified product. Thus, companies that buy products bearing the DPA Security Logo will have a high level of confidence that the products have been thoroughly tested.

This article provides an overview of the CRI DPA Countermeasure Validation Program, including a description of the scheme's testing methodology and a summary of the relationship and confidentiality between the vendor and the testing lab.

## DPA Countermeasure Validation Program

The DPA Countermeasure Validation Program has been designed to leverage the best elements of both validation and evaluation methodologies, maximizing the strengths of the respective approaches. Testing is based on the clear box model, where the evaluation lab has access to comprehensive design information and countermeasure rational. Well documented and designed products will thrive under such an approach, where presence and effectiveness of strong countermeasures are confirmed by the testing lab, and resources devoted to penetration testing can be focused on the key elements of the product's operational environment. This approach also gives the accredited labs the flexibility to deploy their expertise in the most efficient and effective manner. This means that the testing labs are not being constrained by overly rigid and dogmatic requirements that are often recognized as adding limited value in highly formal evaluation methodologies.

## Testing Process Overview

The product vendor provides the evaluation laboratory with samples and comprehensive product documentation and details of the design. This includes describing the side channel countermeasures that have been incorporated, the threat models that they address, and the rationale for their being appropriate and effective in the context of the usage model of the product.

The first phase of the lab evaluation is to study the vendor documentation and usage model, followed by initial testing to confirm understanding and the function of the product. The lab will then conduct a validation of the countermeasure rationale & effectiveness, including selected testing to confirm the presence and effectiveness of the countermeasures.

The second phase involves conducting leakage testing of selected functions identified as being the key elements of core function and cryptographic processing. The lab will use its expertise in selecting the appropriate analysis techniques to conduct penetration testing based upon the product configuration and usage model.

Finally at the conclusion of the testing, the lab will prepare an analysis report and provide feedback to the vendor. After addressing any issues identified in the evaluation and testing the lab will then send a brief conclusion statement to CRI confirming the outcome of the evaluation. CRI will then provide the formal notification to the product vendor that the identified products are licensed and have successfully passed the tests demonstrating resistance against side channel attacks. Such products are awarded the right to use the DPA Security Logo.

### The Product Vendor and Testing Lab Relationship

Any company that has a valid DPA countermeasures license with CRI may contact an accredited lab to arrange for their products to be evaluated for the right to display the DPA Security Logo. CRI is currently evaluating the capabilities of several testing labs. Thus far, Brightsight is the only lab we have accredited. We intend to accredit only a small number of the very best evaluation laboratories who have demonstrated outstanding expertise in the area of side channel analysis.

Contractual details of the evaluation are negotiated in strict confidence between the product vendor and the lab directly, and without Cryptography Research's involvement. Furthermore, the sharing of any confidential information relevant to the evaluation is also strictly limited to the laboratory and vendor relationship. No confidential information provided by the vendor to the evaluation laboratory is shared or made available to Cryptography Research at any time.

The laboratory conducts the testing and evaluation, and provides its detailed results and feedback only to the vendor. When the evaluation is successfully completed, a conclusion summary is given to CRI confirming that the product has satisfied the necessary criteria required by the DPA Countermeasure Validation Program. CRI will formally notify the vendor that the identified products have been awarded the right to use the DPA Security Logo.

The DPA Countermeasure Validation Program augments and complements existing testing and evaluation methodologies, providing a consistent and coherent framework for side channel evaluations. For example, when conducted as part of a Common Criteria evaluation that addresses side channel vulnerabilities, the additional overhead for CRI's scheme is minimized.

### Conclusion

The ability to resist power analysis attacks is an essential requirement for cryptographic devices operating in an open and potentially hostile environment. Providing assurance that the countermeasures against such attacks are effective can only be achieved by testing conducted by expert independent laboratories. The DPA Countermeasure Validation Program has been designed to address these requirements by combining the best elements of existing testing approaches into a comprehensive methodology which is compatible and consistent with existing industry evaluation schemes. The DPA Security Logo enables product vendors to differentiate their products which deploy effective licensed and tested countermeasures against power analysis attacks.

## World News In Brief

### Hackers exploit MD5 Flaw to forge SSL Certificate

A group of hackers announced that they'd beaten SSL, using a cluster of 200 PS3s.

By exploiting a flaw in the MD5 cryptographic algorithm, they managed to create rogue SSL certificates, which would appear to be issued from Verisign's certificate authority RapidSSL. The task takes 1-2 days to calculate using the 200 PlayStations.

This means the authenticated web sites you're visiting could be counterfeit and you'd have no way of knowing. Vendors using MD5 are going to have to use less predictable variables and upgrade to a more robust algorithm.

URL:http://www.win.tue.nl/hashclash/rogue-ca/

# The Smart Security Industry is well prepared for a rapid deployment of M2M

By Jean-Pierre Delesse, Renesas Technology Europe

### How to define M2M?

M2M stands for Machine to Machine communication; it can be defined as an eco-system allowing the communication between 2 pieces of equipment by exchanging data over a mobile network (wireless M2M) or by direct connection (wired M2M) without human intervention. When at least one piece of equipment includes a Smart Devices (tamper resistant), it can be defined as a Smart M2M eco-system enabling identification, control or transaction.

## M2M: a huge market potential…..

As of today, M2M has a relatively low penetration and it is too early to say how big it will ultimately be; it is likely that M2M will represent a huge market potential because it will offer the opportunity to connect several billion of intelligent devices. As far as wireless M2M is concerned, the expected growth will be facilitated by the expansion of the GSM network and by the increase of broadband connectivity (like 3G).
Eurosmart estimates in 2007 there were more than 20 millions units of wireless M2M sold, increasing to 100 million units by 2012.

Berg Insight reports that Europe represents a potential for more than 600 million wireless connections with different levels of security, while IDATE and ABI Research estimate that by 2010, there will be about 2 billion machines that will have the ability to communicate with each other. There is no more doubt that the market potential will be huge.

### ….and extremely fragmented

The M2M market is it is extremely fragmented, covering a wide range of wireless and wired applications and consequently forecasting the current and future market size can be difficult.

Among the wireless M2M applications, automotive telematics and metering are seen as the most promising, although other applications like vending machines or fleet tracking will also offer hope for further growth. In the wired sector, applications like anti-cloning or usage control are already deployed by some OEM's.
Some M2M emerging applications are driven by new regulations for emergency car safety, like the eCall initiative in Europe, or by programs for energy saving like remote metering. For instance, in France, EDF is working on the next generation of electricity meters, which could generate a potential of more than 30 millions of M2M modules.

### M2M will offer new opportunities for SIM and for MNO's

The value chain of the M2M eco-system remains complex as it involves different players and activities, such as silicon vendors, SIM producers, SIM personalization, Module Makers, Mobile Network Operators, Integrators and Services providers.

As most of the wireless M2M applications are SIM centric, it is not a surprise to see Mobile Network Operators (MNO's) willing to be at the heart of the eco-system; clearly M2M will offer opportunities for MNO's to generate new revenues trough new applications and new services.

All major MNO's in Europe are defining their strategy to address the M2M market, raising technical and economical expectations to the Smart Security industry.

## No compromise on Security!

It is likely that M2M will face the same kind of threats as any other applications requiring secure identification (hacking, SPAM, identity theft). For some applications like eCall or medical control, the consequences of a non tamper resistant eco-system could be huge as it involves human safety. What would happen for example if the server of a rescue organisation received corrupted data from a car emitting an emergency call? What would be the benefit of a security network based on M2M technology if a hacker takes full or partial control of the network?

It is important for each type of M2M applications to identify the real trigger: human safety, e-transaction, business model and then to ensure the proper level of security is implemented. Although M2M is a new market, there should be no compromise on security!

The Eurosmart association is currently preparing a study on M2M including recommendations of appropriate security levels for different applications.

The Smart Security industry has for many years been proposing a wide range of security levels which deliver the proper response against different levels of threat.

### Still some barriers….

The different players in the M2M value chain have already identified some common needs especially for the SIM: physical constraints (temperature, vibration, humidity, etc), data retention, life time….. Some silicon vendors are already enabling chips for the automotive or the consumer & industrial market, this experience is very useful to develop M2M silicon that can work in more severe environment.

For instance, Renesas has developed a new device, the AE470G, which has been successfully tested under the severe conditions required for M2M applications.

As it is often the case for new applications, standardisation and business model seems to be the remaining barriers that M2M will have to cope with.

For instance, there is an on going debate regarding the new form factor which should be used for the M2M SIM; soldered, removable, VQFN, SOP…?? . So far, the smart security industry has always been able to reach a consensus addressing the needs of the end users and there is no doubt it will be the case for the M2M.

### Conclusion

The Smart Security industry has demonstrated it has been able to deliver solutions ensuring a safer world for human to machine applications like SIM Card, Banking Card or e-Passport. In the near future, that legacy will be extended to machine to machine applications to make our life easier and safer.
In its 2020 vision paper, Eurosmart sees M2M as a dominant application of trusted hardware technology
There is no doubt that M2M will be part of our future.

## World News In Brief

### UK Rail agrees Open Mobile Ticketing Standard

The Rail Settlement Plan (RSP), the rail ticketing body jointly owned by UK train operating companies and the rail operators themselves, have been working with Masabi, a mobile applications company to develop a new standard for secure barcode rail ticketing. The new open standard allows all mobile ticketing schemes to use a common secure barcode system, and also to be able to start accepting a single mobile ticket on a journey involving multiple rail operators.

To date, all rail mobile ticketing systems have used the web to sell a restricted selection of advance tickets using proprietary standards. The approval of RSPS3001, the UK-wide standard is the first step toward being able to use mobile tickets and print-at-home tickets on many different rail operators for everyday walk-up tickets which represent the vast majority of sales.

The new barcodes contain enough ticket and security information to allow off-line systems to scan and validate tickets with similar security to the Oyster smart card system used in London. This allows the system to operate as an islanded system on vehicles or on hand held terminals in the event of system disconnection, and still process millions of tickets quickly and conveniently.

# Interview with Thomas Froschmeier – Head of Marketing and Communications at Giesecke & Devrient

By Tom Tainton, Smartcard & Identity News

*Tom Tainton*

Giesecke & Devrient (G&D) is a market leader in smart card systems and security solutions. Based in Munich, the group employs over nine thousand people and operates across the World. The company gives high priority to driving new technology innovations and holds more than 7,000 patents, adding well over 100 each year. In 2007 G&D spent roughly €100 million euros on basic research and product development and employs more than 800 specialists researching and developing new products and processes. I spoke to the Head of Marketing and Communications Thomas Froschmeier about their plans for the New Year.

**G&D is a global leader in e-commerce solutions and high-technology innovations. What are the key factors in the company's success?**

When it comes to smartcard technology and security we're market leaders dealing with global markets such as telecommunications and payment. We have over 150 years of experience in the security sector, and more recently in digital security. Over the years we've built a solid base of trust with our customers. We maintain a strong focus on innovations in new technology, such as Touch and Travel, an NFC ticketing project, which won a Sesame Award. We have also worked successfully in NFC and contactless trials with Barclays in the UK, and Garanti in Turkey.

**How important is the development of NFC to the industry and why do you think the technology is still yet to experience major take-up?**

NFC is a really important topic and crucial for the industry. This is because contact less technology allows us to open up new business models and application opportunities. This is why G&D established a joint venture with Nokia already back in 2006. Venyon provides a secure platform for implementing applications for NFC-enabled mobile phones. The problem with the new technology is its unfamiliarity. For wide take-up to occur the customer needs to realize the benefits of the technology and learn to trust it. It's an educational process that the industry can help to push. Commonly, an individual might worry that contactless technology will result in them losing money or having personal data stolen. Instead, we need to stress to the customer the convenience of such a solution. A good example is GSM (global system for mobile communications) which came around in the late nineties. At first take-up was minimal and some suggested the technology wasn't useful. However, over time people began to trust it and today it's a necessity for everyone.

**You mentioned receiving a Sesame Award for your mobile ticketing solution – Touch and Travel. Was this your most successful application or highlight in 2008?**

In terms of innovation, the Sesame Awards was a highlight of the year for us – it's undoubtedly a huge honour within the industry. Nevertheless, Touch and Travel is just one application that has been recognized. We have reached a couple of other innovation milestones including Garanti in Turkey where we have introduced secure payment solutions. I believe that we're on the forefront of contact less technology, and we're the NFC market leaders in North America.

**The Micro SD card is the first to offer contactless smart card security as well as data storage functions. Can you tell me more about the product and how it works?**

A Micro SD card is essentially a flash memory drive with no security. However, with this card we have added a crypto-controller onto the flash memory card, which enables data to be encrypted onto the secure flashcard.

The card still retains its smartcard functions as well. A customer can have secure applications on the card, as well as digital signatures, all of which is technologically done. In the very beginning the application was based upon a three chip solution, and today we talk about one microcontroller that controls everything.

What benefits will the user experience over standard security cards?

The benefits for the end-user are obvious. The opportunities for the Micro SD card are immense. It's important to remember mobile devices are not only mobile phones, but also devices such as Mp3 players. Most mobile phones today offer Micro SD cards and in the future ipods will also have Micro SD capabilities. The card also gives the consumer the freedom to choose the combination of network operator provider and to choose a device. It's a big step away from the conventional smartcard. The card gives the user and bank most suitable for him. So effectively, the card makes life easier and quicker for the user and the provider.

**What are the main challenges facing G&D, and the industry in 2009?**

The major challenge to the industry and to our company is the financial crisis. For the moment we see little or no impact because Giesecke & Devrient has a very balanced portfolio, we are remaining very positive. However, while we see no influence currently, we don't know what will happen in the following months. We will keep a close look on the market. Away from finances it's important to further drive all new technologies such as the Micro SD card and NFC including preparing the market and educating consumers. Finally we will be looking to complete our evolution to digital security service provider.

**Going into 2009, how different is the market in comparison with five years ago?**

Compared with the market around 4-5 years ago the biggest change is the competitor landscape. There are not as many international competitors as a result of a series of large mergers such as Axalto and Gemplus (Gemalto). The markets are globalised, with international providers and regional companies influencing the global competition. In 2005 pricing was of utmost importance, and the pressure to raise prices was huge. This peaked in 2006, which as I'm sure you are aware was a difficult year for the industry. Today price pressure is far more moderate – a positive signal for the industry. Instead quality of product takes precedence and is deemed way more important.

**Finally, what does the future hold for G&D, both short term and long term?**

I'm confident our future will be good. We have a solid structure and financial base and we aren't dependant on share market prices, an issue which affects other companies. We also have the confidence and trust of our customers which is really important.

## World News In Brief

### G&D Release microSD Card Smart Card Contactless Functions

Giesecke & Devrient (G&D) has developed a mobile security card offering contactless smart-card security in addition to the usual data storage functions. The new security feature is provided by a cryptography controller with an NFC-compatible interface integrated in the microSD card along with the flash memory. The Mobile Security Card CL thus serves as an ideal basis for implementing security and payment functions in cell phones and for many other mobile applications.

"The holder of a Mobile Security Card CL can now use one and the same card for authenticated access to all services requiring a digital identity, both from their home PC and when out and about from their mobile phone." points out Dr. Kai Grassie, Head of G&D's New Business division.

### Gemalto provides Kingdom of Bahrain with additional One Million e-ID Cards

Gemalto will deliver an additional one million of its electronic ID cards for citizens and residents of the Kingdom of Bahrain. This new program extends the country's original electronic ID system, which saw Gemalto documents distributed since September 2007. This new high-end identity card combines built-in biometrics and serves as official ID and travel document. The card can store medical information of the cardholder (including URL's pointing to the cardholder electronic medical files).

# "Mobile World"

## - Meeting of the Smart Card Club, London, January 13

### By Peter Hawkes, Smart card & Identity News.

*Peter Hawkes*

Six talks were given at this meeting. Collectively they covered many current and proposed aspects of mobile communications technology and applications.

Dr Fred Preston of Motorola Identity and Security gave the first talk. His topic was "A handset manufacturer's point of view-rapid mobile fingerprint identification - a case study". Motorola's customer was the Swiss Federal Department of Justice and Police. In 2007 the various Swiss police forces and the border guard organisation needed a mobile fingerprint capture and matching system. This was to be for use in the field by the guards and police. On the basis of the Officer collecting the subject person's thumbprints a positive identification was needed. This was assuming his prints were on record. The response time from the central fingerprint database had to be 2-5 minutes.

Dr Preston took us step-by-step through Motorola's design and development stages. These began with gaining an understanding of the Department's needs in the European context. There followed the selection of the components, assembling a first fingerprint solution, pilot trials and then an administrative trial. Deployment throughout the country was achieved last summer. Dr Preston gave us an initial report on the first results achieved during the autumn.

In the initial 3 months of use 253 searches were carried out for the police forces. These resulted in 101 hits in the AFIS and other linked databases. Border guard searches gave slightly lower hit rates. The combined average of about 33% was, he reminded us, quite typical of fingerprint searches carried out since fingerprint identification began to be deployed over 100 years ago.

This trend continued when manual database searching was supplemented by Automatic Fingerprint Identification Systems (AFIS) in the 1980's. Human Factors have been carefully considered in the Swiss mobile system. For example if a sample of two thumb scans from a subject person leads to his identification as a dangerous person, the "hit" details may be sent to another Officials rather than the Officer making the AFIS enquiry. A Swiss proverb was cited by the Executive in the Department when reporting his satisfaction with the new mobile system:- "The egg-producing-wool-milk-pig does not exist". Translated it means that one should beware of seeking all-embracing, over-ambitious solutions to the problems of human identification. Instead simpler, more practical designs that work should be adopted.

The high standard of presentation set by Dr Preston was maintained by the later speakers. The first of these was Mr Nick Ogden of the Voice Commerce Group. He spoke on his company's current products led by the Voice Pay technology. This uses sampled speech data sent over the public telephone networks to a Voice Commerce Group server. Server software is used to help identify the caller seeking to prove his access rights. These rights might, for example, be to use a telephone banking system to carry out a transaction or to consult his bank account.

The "Voice signature" devised for ID checking is considered to be an ideal biometric replacement for "Chip & PIN" in mobile commerce and banking. The emphasis is on mobile telephone users. 2.3 billion mobile handsets are already in service worldwide. The number of users of such devices now far exceeds the number of users of networked PC's. 80 % of all MNO (Mobile Network Operator) users are Pay-as-you go. So they are (currently) anonymous to the MNO. Accordingly Voice Commerce Group has to carry out it's own checking of callers' ID claims.

The Group's system assumes that existing payment instruments will be used. User convenience comes from basing his "signature" on samples of his speech, as spoken in to a standard telephone microphone and digitally encoded. Noisy backgrounds result in the identity checking software at the remote Server refusing a transaction. Given a quiet environment the system deploys an array of proprietary authentication techniques. These are combined with the results of voice matching to create an adequately secure authorisation environment for authentication decisions. The residual risk of this decision being incorrect is borne by the Company. So perhaps we can say the company is putting its money where it's ear is rather than it's mouth.

The next talk reminded me of the one of the key commercial aspects of new mobile services- Consumer trust in a well-respected Brand. Mike Greening of Analysys Mason gave us an erudite account of Branding issues in "The battle for competitive advantage in the mobile world." This started with an illustration of the spectrum of Brands now deployed in the Mobile network domains of Europe. On one extreme the MNO's deploy their products as "sub-brands". They own these. Orange is a good example, being owned by France Telecom.

At the other extreme there are Mobile Virtual Network Operators (MVNO's). Very successful examples of these include Tesco Mobile and Virgin Mobile. So now in the UK 12% of all mobile subscribers are with MVNO's. However only a few of the MVNO's are flourishing. Seeking increased profits the others are exploring new business models. Analysys has observed some winning strategies for sub-brands and wholesale. Several MVNO's focus on basic "no frills" services, available to all. Others focus on the special needs of minorities e.g. expatriates calling home.

The fourth presentation involved a double act. The two speakers were Leonard Carey from Business Services at Orange and Philip Ayles of Parkeon. The Parkeon Group took over Wayfarer, the UK maker of bus ticketing machines in 2007. Their topic was "NFC trials- a case study of payment, access and authentication using mobile technology". The actual trial was a collaborative project with the Bus operating company in Reading, Berks. This company is owned by the local authority, Reading Council. Orange participation followed from a trial of NFC phones for access to Manchester City's football ground at the end of 2007.

The NFC trial at Reading Buses is part of a much larger ITS (integrated transport system) project run by a consortium including Orange. See :-www.reading.gov.uk/search/Search.aspx?TextID=65725. Orange provided the Sony-Ericsson NFC enabled mobile phones. Oberthur supplied the NFC SIM's. These emulated ISO 14443 compliant contactless cards.
Only a small number of phones were involved. They were used by season ticket holders on a single route. Some searching questions from members of the audience were deflected as too commercially sensitive.

Tony Birk Jensen of Oberthur Technologies spoke next. His talk differed from the abstract in the programme. The focus was on Oberthur's activities in supporting its customers with card personalisation services. These customers include 250 MNO's and 5000 banks. National governments and public transport operators are also served. Personalisation services are provided by a network of service bureaus operating from 30 sites world-wide. The trust of both card issuers and their customers needs to be maintained at all times. Applications often need to be loaded remotely. The same applies to blocking and re-activation.

The last talk was billed as a debate "Cards vs Phones". It was to be led by Dr Neil Garner of Proxama Ltd. In the event it was essentially a comprehensive presentation by Dr Garner with no time for the debate. Whilst there are obvious differences in form and function between cards and mobiles he pointed out that they have more in common than it may appear on the surface. For example both are portable personalised electronic devices. Both may now be used for making payments or storing account details. In consequence both record sensitive data and security information. Both contain a secure chip. The two technologies are converging. Cards are becoming more like Phones by supporting an LCD display. Phones are becoming smaller e,g. the Samsung P520 phone which is credit card size.

Some phones emulate the card e.g. the Nokia 6212.NFC phone. NFC represents a convergence of card and phone. Additionally the phone can become a mobile POS and an e-commerce device. He suggested that, "An NFC Phone is to cards, what an MP3 player is to CD's".

In summary he suggested that for phones to truly take over from the wallet full of cards a complex multi-party ecosystem needs to be developed for the issuance and management of any device.
The convergence aspects of this talk gave me a sense of déjà vu. In the mid-1980's I worked on a smart card project with the late Donald Davies FRS and his team at the National Physical Laboratory. One of several pioneering results was a set of working prototypes of the NPL Token. This was a smart card with keyboard and display. It was battery powered. It communicated encryption keys and other data wirelessly to a secure reader. Some details are outlined in the specification of US Patent 4799258 (first filed in UK on February 13, 1984). A summary of the project is given on page 3 of Smart Card News for March 2001.

# Barclays launches NFC – enabled payment card – but what are the 'cons' of contactless?

### By Tom Tainton, Smartcard & Identity News

*Tom Tainton*

It's fair to say that contactless technology hasn't exactly been accepted with open arms by the British public. With that in mind, the announcement by Barclays that it will be the first UK bank to issue contactless payment cards to all its customers from March is great news for NFC enthusiasts and a significant boost to a technology that until now, has struggled to break into mainstream markets. However, the introduction of contactless payment raises as many questions for Barclays customers as it answers.

This is far from a snap decision by the bank. In fact, the group have been trialling contactless technology in the UK, (well London at least) for two years. In late 2007, Barclays introduced 'OnePulse' through its subsidiary Barclaycard. OnePulse combined an Oyster card, a credit card and a contactless payment card. According to their research, Barclays discovered that 95% of respondents said they made at least one contactless purchase a day. How accurately these results reflect user opinion is anybody's guess. The bank declined to divulge what percentage of OnePulse cardholders actually used the contactless technology. After all, there are only six thousand terminals in the country that can accept the card.

Nonetheless, Barclays is following bravely in the footsteps of Hong Kong's Octopus scheme, another contactless debit card that has fast become a must-have for travel and low-value payment in the Chinese city. Barclays will be hoping for the same success in Britain when it replaces its entire fleet of debit cards with new plastic cards embedded with NFC-enabled chips. The group said that debit cards issued would enable payment of low-value items up to £10 without consumers needing to sign or enter a PIN. The cash is then debited from the individual's account just as it would be from a standard purchase. More than eight thousand retailers already accept contactless payments, many of whom are based in London. These include Yo Sushi! Pret A Manger, Coffee Republic as well as news agents and dry cleaners.

The cards will still have chip and pin functions, enabling them to be used for transactions of more than £10 or to withdraw money from cash machines. But Barclays estimate that by 2011 its entire debit card estate will be cashless, and five million cards are set to be issued by the end of this year alone, with an extra hundred thousand merchant locations, capable of accepting the technology, to follow. One thing is for sure, this is a huge milestone for contactless transactions but what about security? If there is no PIN and no receipt print for a transaction, then how can a user be sure about when and how much the card has been debited?

Nowadays it's common to experience systems failures and human error in many of our services. Is it risky to carry a credit card which can be inadvertently debited without any further notice? The advantage for the credited party is clear, but the benefits to the customer are less obvious. The problem is that for successful transactions in a secure system there needs to be both a secure transaction conduit and a unique transaction validation. Neither of which are present in a standard contactless transaction, all that occurs is the reading of an RFID. The result is that the card companies are balancing the risk of fraud on low value transactions versus the chance of card RFID skimming. The real test will be whether RFID in every card will result in an acceptable balance of risk and reward. However, APACS (UK Payments Association), Visa and MasterCard have insisted the technology is safe and secure citing the fact that there hasn't been a single report of fraud loss in any pilots conducted by Barclays.

APACS has admitted that it is possible for a fraudster to read data from a contactless card, but it stresses the limited information available on the card would not be enough to clone it. Barclays have also added a security mechanism whereby the customer is required to enter their PIN on random occasions, as an added measure to prevent misuse. Besides, with all contactless transactions limited to £10 or below its unlikely fraudsters will be interested in the cost of a sandwich and a cup of tea.

The lack of contactless- enabled terminals is another concern for Barclays. Retailers who have recently spent a whole chunk of change on Chip and PIN will be reluctant to cough up for more new terminals or bank EMV

accreditation. For contactless technology to flourish, the vast majority of commercially available handsets have to incorporate NFC as standard. Currently, this is far from the case. Granted - the technology has yet to be compromised, but that's probably because the cards can hardly be used anywhere. If they can't be used, they can't be compromised. Barclays has failed to live up to the initial target of twenty-thousand outlets and while contactless technology remains limited to the capital, retailers in other parts of the UK have no incentive to adopt it. It makes sense to introduce terminals to areas that currently don't have them. Apparently, this is an area Barclays is 'addressing.'

Where Barclays have led, others are sure to follow. It's not certain that we'll ever become a cashless society but the bank is certainly taking steps in the right direction. Contactless technology is here to stay, whether Barclays customers welcome the changes is another matter.

# World News In Brief

## Is Cash Safe with a Flu Pandemic

As may of us know only too well, the flu season is here again. Research published last May, revealed that the human flu virus can survive on banknotes for up to 17 days.

Yves Thomas, head of the National Influenza Research Centre at Geneva University Hospital, told Reuters that employees who handle large quantities of notes daily could be at risk: "This could be reduced if they wear gloves, or even a mask for those who have to examine currency closely."

Researchers pointed out: "The unexpected stability of influenza virus in this non-biological environment suggests that unusual environmental contamination should be considered in the setting of pandemic preparedness."

Is it time to bid farewell to our paper notes and embrace e-money with open arms, and a healthier outlook?

## Motorola Planning Restructuring of Handset Division

According to unconfirmed reports in on-line publications, Motorola's handset division is preparing to layoff anywhere up to half of its Handset Division workforce.

An article by Phone Scoop suggests the US vendor is set to announce the cuts as early as this week.

The Phone Scoop article also claims that Motorola are not planning to have a booth at CTIA Wireless trade show this April, and will reduce the number of new phones it brings to market to 12, and the only smartphones it will produce will be based on Google's Android platform.

## EU to create New Payment Systems Market Expert Group

The European Commission is to create a Payment Systems Market Expert Group (PSMEG). The group will be composed of experts competent in the area of payments. It will aim to gain inputs on payment issues, including fraud prevention, from a range of stakeholders, in particular the payment industry and users.

Internal Market and Services Commissioner Charlie McCreevy said: "It is important to have sound, efficient and secure payment systems in order to ensure a proper functioning of the internal market. With the development of our policies in the area of payments, in particular in the context of the Single Euro Payments Area (SEPA), we have a growing need for regular and high-level stakeholder input at the earliest stage of our policy-making. New and complex areas of activity, such as the prevention of payment fraud or the development of innovative payments, will also mean new needs for specialist expertise."

The PSMEG's tasks will be: to assist the Commission in the preparation of legislative acts or policy initiatives regarding payment systems, including fraud prevention issues related to payment industry and users; to provide insight concerning the practical implementation of that policy; and to exchange views on up-to-date best practices and ensure monitoring of potential issues of concern for the market. The group will meet in Brussels and will be chaired by the Internal Market and Services DG of the European Commission.

A maximum of 50 experts will be selected.