

Smart Card & Identity News

Is published monthly by
Smart Card News Ltd

Head Office: Smart Card Group,
Suite 3, Anchor Springs, Duke Street,
Littlehampton, BN17 6BP

Telephone: +44 (0) 1903 734677

Fax: +44 (0) 1903 734318

Website: www.smartcard.co.uk

Email: info@smartcard.co.uk

Editorial

Managing Director – Patsy Everett

Technical Advisor – Dr David Everett

Production Team - John Owen,
Lesley Dann, Suparna Sen

Contributors to this Issue –
Tom Tainton, David Everett, Peter
Tomlinson, Watchdata Systems,
Suparna Sen, Steve Brunswick

Photographic Images - Nejrion -
Dreamstime.com

Printers – Hastings Printing Company
Limited, UK

ISSN – 1755-1021

Disclaimer

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

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

© Smart Card News Ltd

Our Comments

Dear Subscribers



Patsy Everett

Our theme this month is very much about identity theft or more precisely the ability for an attacker to gain sensitive information about us that enables them to masquerade as us usually to our financial disadvantage. A bit of a mouthful I know but I have been much maligned for using the term identity theft on the grounds you can't steal somebody's identity without being them.

I'm sure science fiction would allow me to travel in this space with shared and borrowed identities but just for now lets stay in the real world.

The New Scientist this week was taking on the problems of losing sensitive data via your smart mobile phone, I think they actually said identity theft but I've resisted the temptation. So the problem is that if you lose your phone what sensitive information are you making available to the potential attacker? We need to bear in mind that many phones are not protected by a password but I'm pleased to hear you are one of the exceptions. However those that do use a password quite often use a deterministic password that is unlikely to be of a hurdle for the enthusiastic hacker. So just for the record when you lose your phone, misplace it or maybe lend it with or without permission, then you have an open phone with mobile and internet connectivity. Worried?

Now there are the obvious, text and email messages along with contact lists. You'd be surprised at how many people are keen to get their hands on their partner's phone just to make sure they are keeping up with their messages of course. However it can lead to problems, apparently those with illicit affairs don't always keep it secret on their phone which can lead to the break-up of many a partnership. Even worse there are cases where the aggrieved spouse has attacked their partner and in at least one case this has led to the early demise of the culprit. I can't believe it but in some cases people even carry photographs on their phone that you certainly wouldn't want to show the children!

Now in that address book, what would there be for the attacker to find? The New Scientist article helps out a little more by suggesting that entries for M and V might not be for Martin and Veronica, MasterCard and Visa more like, and those 4 digit telephone numbers, guess what they are, not your PIN of course. Apparently some people are really helpful in their address book and put in a full 16 digit telephone number along with a 3 digit security code, no, I mean extension number.

Then of course there are the passwords, let's face it you even have to have a password to do your shopping, on-line of course. Let's be honest when you've got so many passwords you have to write them down, it used to be on a piece of paper but today we use the trusty phone. I'm sure you remember all your passwords, but I've seen people do it, at their PC or even at the point of sale out comes the phone before they can enter their PIN or password. Now all this may not be exactly identity theft but it would allow an attacker to pretty well take over your life, this is worse than losing your purse or wallet.





According to Lostmobile.org.uk over 700,000 phones are lost or stolen in the UK every year, the London Metropolitan police report 120,000 stolen phones per year of which two thirds are from victims aged between 13 and 16. Staggering figures so make sure you are not a part of the statistics.

Every day you hear about somebody losing their laptop or memory stick but actually losing your phone could be far worse because it might enable an attacker to get at all the data you are authorised to access. Apparently the Apple iPhone, one of the cult smart phones has particularly poor security and can easily be hacked. It doesn't bear thinking about, so now that 3rd party apps on smart phones are all the rage how about something just to encrypt that valuable data? It's funny because smart phones seem to be miles behind the PC when it comes to security and yet this is where we store all our sensitive information. What does it take to bring this to people's attention?

Yes, November is nearly here and Cartes 2009 is just around the corner, hope to see you there.

Patsy.

Contents

Regular Features

Lead Story - £1Bn Guardian Newspapers Identity Hack	1
Events Diary	3
World News In Brief	5,8,10,13

Industry Articles

Identity theft – It's no fraud, we're ALL at risk	7
Greater Manchester Integrated Transport: - Delivering Achievable Transport Plans	9
Convergence on the Horizon	12
Macro move towards Micro-payments	15
Contactless Payments – Going Global?	18

Events Diary

November 2009

3 – 5	ID World International Congress, Milan, Italy - http://www.idworldonline.com/
3 – 5	NFC Academy, Milan, Italy - http://www.nfcacademy.com/
17 – 19	Cartes 2009, Paris, France - http://www.cartes.com/ExposiumCms/do/admin/visu?reqCode=accueil
18 – 19	Mobile Asia Congress, Hong Kong - http://www.mobileasiacongress.com/

December 2009

7 – 8	3G Middle East 2009, Dubai, UAE - http://me.comworldseries.com/
8 – 9	RFID 2009, Paris, France - http://www.rfid-show.com/

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





£1Bn Guardian Newspapers Identity Hack Continued from page 1

Guardian Jobs has about 1.4 million users per month and stores the details of largely professional and public sector workers. So potentially perhaps another 900,000 users are on risk.

Scotland Yard's new e-Crime unit is involved and the newspaper has not released any technical information relating to the attack. The information exposed relates to users names, email addresses, CVs and covering letters presumably with their addresses.

There has been much speculation about the attack with the finger of suspicion being pointed at some form of SQL attack. Other speculators point out that in every 1000 lines of code there will be at least one hidden vulnerability. I suspect they have a hole in their calculator because the vulnerability in some software components is probably far higher.

The reason that planes don't fall out of the sky on a daily basis is not because there aren't any vulnerabilities in the components but because of the security reliability of the system. This is an integrated set of processes, security controls, and their management that leads to an overall reliable system. That is a properly organised risk management system. You can't avoid risks, you manage them.

What we are seeing ever more in the commercial and financial world is the result of a failure in a component for which the system is unable to adequately compensate.



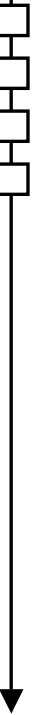
In this particular case the Guardian has provided the potentially vulnerable job seekers with a list of police endorsed steps to take as a precaution. These steps include approaching a reputable credit reference agency such as Equifax and registering with CIFAS the UK's fraud prevention service. Potential victims are also invited to visit web sites such as banksafeonline.org.uk for further advice and information. I haven't noticed too much enthusiasm for the Guardian at the moment although in all fairness the problem does seem to be with their service provider Madgex.

So where does the Office of the Information Commissioner sit in all this? Credit to the Guardian they have apparently been notified immediately the attack came to light which is certainly not true of some of the other high focus attacks such as Heartland and Worldpay who saved their losses of 1.5 Million card holder's personal information until just before Xmas last year hoping it would get lost in the rush.

One can't help feel concerned at the apparent lack of teeth the OIC seems to exhibit. In many of these public cases it is clear that there is an absence of the necessary security culture, we do not have a high security reliability organisation and yet by all rights it is a legal requirement. We were told that the powers of the Information Commissioner would be increased with even the possibility of prison sentences for severe breaches of duty by the senior management of the organisation. At the moment you seem to get more severe penalties for speeding.

I remember when I first started in security realising that it's pervasive and it's the security of the whole that counts. I doubt anybody would argue the concept but that's not what we are seeing today. In the case of the financial institutions and their partners the value of the PCI-DSS (Payment Card Industry Data Security Standard) is currently moving into disrespect, I wonder why?

Dr David Everett





World News In Brief

Parabon NanoLabs to develop 'briefcase-size' biometrics device at less than \$50

Parabon NanoLabs (PNL) has announced its award of a Department of Homeland Security (DHS) Small Business Innovation Research (SBIR) grant. The funds will be used to demonstrate the effectiveness of the company's new single nucleotide polymorphism (SNP) "SNP chip" (pronounced "snip chip") to rapidly verify identity and kinship using DNA. The goal is to design a briefcase-size biometrics device that will process a DNA sample and determine identity or kinship with an accuracy of 99.99%, in under 45 minutes, at a cost of less than \$50.

Parabon's immediate goal is to develop an easy-to-use, desktop biometric device that, in the future, can be further miniaturized to produce a handheld, high-speed biometric device. The initial device will be briefcase-sized, capable of being brought into the field as a single unit, but its modular design will allow for multiple DNA analyses to be conducted simultaneously, for situations where a higher throughput is necessary. SNPs are fundamentally conducive to miniaturization because they do not require the electrophoresis readout process that short tandem repeat's require.

PNL's device will have enormous commercial value across the homeland security, law enforcement, and defence industries. "Beyond DHS' needs for kinship analysis, a rapid, low-cost DNA-based biometric will have broad applications in mass-casualty situations, reunification of family members following mass evacuations, identification of missing persons, rapid processing of crime-scene and suspect DNA and various scientific and educational uses." Christopher A. Miles, Biometrics Program Manager, U.S. Department of Homeland Security (DHS) said. "Rapid DNA-based screening will reduce the fraud in asylum, refugee and overseas adoptions cases allowing DHS to focus on processing legitimate applications."

Annually Identity Fraud cost's UK more than £1.2bn

According to a study, about a third of UK employees throw documents in the bin instead of shredding them, thereby leading to ID fraud. The companies in UK have to be more careful in dealing with sensitive information of their customers. Shredding paper instead of throwing them in the bin can help cut ID fraud. The study also found almost

three quarters of workers feel their organisations could do more to protect their customers' personal information.

The data as compiled by the National Identity Fraud Prevention Week states that per year identity fraud costs the UK more than £1.2bn. The UK's Fraud Prevention Service also says that 60,000 people have fallen victim due to mishandling of important data this year. ID fraud involves fraudsters stealing all kinds of personal details and then using them, often to apply for credit or benefits in their victim's name.

The survey of 1,000 employees suggested that 36% did not know or were unsure if they had a comprehensive policy in place on handling potentially sensitive documents. Away from the workplace, 64% of people admitted that they failed to shred sensitive personal documents at home. Moreover, about 12% said they used the internet without having any security software installed. Only 21% people stated that they regularly checked their credit report to ensure no one is making applications to borrow money in their name.

National Identity Fraud Prevention Week spokesman, Tyron Hill said that the threat of identity fraud was "real and current". Simple steps, like thoroughly shredding any documents with your name and address on them will protect you from cyber crime.

First Data and PayPal to offer New Online Payment Services

First Data has announced an agreement with PayPal that allows debit cardholders First Data's STAR(r) Network to quickly link their STAR debit card to a PayPal account online. First Data's STAR Network is the first electronic funds transfer network to offer this innovative service to its member financial institutions.

With the STAR Online Partner service, consumers can enrol for a PayPal account through their financial institution's Internet banking site, and, once registered, immediately use their debit card to fund their PayPal account to make online purchases without having to enter debit card account information or expose their debit card number to merchants for each purchase. Member financial institutions provide authentication for the cardholder, adding an extra layer of security to the account.



Zenius Solutions Introduce Innovative NFC Add-on

Zenius Solutions, a leading NFC software company, announced the integration of its software to an NFC add-on for GSM phones. It will have the ability to easily enable interactive NFC capability on current mobile phones. The solution expands on current NFC offerings in the market by supporting multiple NFC applications, providing control to the user from the handset screen, and supporting remote provisioning of NFC applications.

NFC payment capability is achieved by adding a BLADOX Waver product running ZeniusMobilePay software to supported GSM phones, thereby making possible secure Mastercard PayPass, Visa payWave, American Express ExpressPay and Discover Network Zip EMV and non-EMV contactless transactions.



This Zenius-enabled BLADOX Waver solution fits into the phone's SIM slot along with the original SIM card. The add-on flawlessly and securely integrates with wallet applications on the mobile phone and allows a consumer to control and access multiple applications dynamically, providing the same functionalities available in NFC capable phones.

Amazon Payments successfully launched Mobile-Payment Service

According to news sources, Amazon Payments, an Amazon.com company, has successfully launched the Amazon Mobile Payments Service (Amazon MPS). By availing this service, the developers, merchants and distributors of mobile applications can process payments from mobile devices, expanding Amazon's 1-Click checkout experience to customers and thus enabling them to make mobile payments using the existing payment and shipping information in their Amazon.com accounts.

Amazon customers can now buy items and services on third party websites without the need to use separate payment accounts.

Infineon Ranked as Number One Chip Card Semiconductor Vendor for Twelfth Year in a Row

In its market report entitled "World Smart Card IC Markets," the US market research company Frost & Sullivan confirmed that Infineon Technologies AG was the number one supplier of chip card semiconductors, with sales representing about one fourth of the segment's global revenue.

In 2008, Infineon's market share was 25.5 percent of the overall chip card IC (integrated circuit) market, totalling about US \$2.4 billion according to Frost & Sullivan. This is the twelfth consecutive year Frost & Sullivan researchers have named Infineon as the top supplier to this market.

Oberthur Technologies introduced the first Microsoft Windows 7 integrated European Citizen Card

Oberthur Technologies, a global leader in the delivery of high security solutions to the ID market, delivered the first Identification Authentication Signature - European Citizen Card (IAS-ECC) cards compatible with Microsoft Windows 7.

ID-One IAS-ECC, an identity card, offers identification, authentication and electronic signature solution that can be implemented throughout Europe, fulfilling the specifications defined for the European Citizen Card.

Thanks to its flexibility and interoperability, IAS-ECC cards can be easily deployed by all integrators and security application providers. The Microsoft minidriver allows the IAS-ECC card to be plug and play with Windows 7 environment.

This card offers an easily deployable, high-end security smart card solution that offers both physical and logical access control for any governmental or corporate identity application.

ID-One IAS-ECC is about to receive all the homologation and security certifications required by any governments, including Common Criteria EAL4+ PP- Secure Signature Creation Device (SSCD), level which is required for all qualified signature projects.

UK Medical Records for Sale in India

Reports have emerged that under cover investigators have been sold medical records from one of Britain's top private London Hospital. Confidential medical records containing patients medical condition, dates of birth and addresses are sent to India for computerisation, but are now being offered for sale for as little as £4 each.





Identity theft – It's no fraud, we're ALL at risk

By Tom Tainton, Smartcard & Identity News



Tom Tainton

It's that time of the year again - Identity Fraud Prevention week is here. And not a moment too soon, either. The scheme, which marks an attempt to raise public awareness of the threat of identity fraud, is a timely reminder of the seriousness of identity theft, reckoned to be one of the UK's fastest growing financial crimes and costing the UK a record £610m. In the last twelve months identity fraud has rocketed by 36% and 4.5 million Brits were unfortunate victims of the crime. That's the highest number of cases in Europe and the figure is set to grow as rising unemployment and social unrest drives more people towards crime. It makes for painful reading, but why is identity fraud an

increasing threat and what can be done about it?

One of the main factors, particularly for British consumers, is naivety. The average Joe continues to ignore advice that could keep his finances safe, surfing the internet without security software and throwing bank statements and bills in the bin without shredding them first. Fairly trivial, one might think, but it could be argued that bins are as big a risk to customer details as computer systems. Armed with just a name and address fraudsters can inflict untold damage. They can empty bank accounts, run up huge debts, ruin credit ratings and tarnish reputations. To make matters worse, the victim has to prove their own innocence.

You'd be forgiven for assuming that it's just the average consumer that is to blame. Large companies and firms are just as bad. In fact, research by the National Fraud Authority (NFA) revealed that over 30% of small and medium-sized businesses had been impacted by fraud. This highlighted a shocking ineptitude amongst the business community – a total lack of understanding of the risks posed and a distinct absence of resources and information for those that were attempting to be vigilant.

The NFA found only 64% of businesses had a clear policy on how to handle documents containing sensitive information, and even less had any measures in place to respond to data loss. The frustrating thing is businesses could easily protect data by using hardware encryption and authentication – an investment which would significantly reduce the threat of ID fraud.

So why aren't they protecting our personal data?

Well, it seems if the government isn't going to take it seriously, then the business community won't either. It's claimed that the Home Office does not appear to be dealing sufficiently with Data Protection Act (DPA) breaches, with no official confirmation as to whether custodial sentences or tougher measures on businesses will be implemented. Until firms are faced with the threat of jail or astronomical fines for DPA breaches, they're quite happy not paying a small fortune to resolve the problem.

Tales of identity fraud are commonplace in countries all over the World. The FBI arrested 53 American citizens accused of carrying out illegal online activities and stealing nearly \$2m from customers belonging to Wells Fargo and Bank of America. 47 more 'co-conspirators' are also set to be detained in what has been dubbed 'Phish Phry', the largest ever number of defendants charged in a single cyber crime case. In Germany, the number of internet-based crimes rose nearly 10% in 2008, and IT analysts predict another increase this year.

Yet the security industry continues to bury its head in the sand, and seems reluctant to confront a difficult and complex problem. The industry body Financial Fraud Action UK have effectively denied the problem altogether, saying that their findings for results this year showed the amount of fraud being committed on plastic cards had fallen 23%, while phone, internet and mail-order levels also dropped. Experts suggested that criminals had turned to targeting foreign-issued cards and criminal activity in Britain was finally coming under control. The introduction of online payment tools, such as MasterCard Secure Code and Verified by Visa have failed as saviours in the battle against identity theft.

However, IT consultant at Consult Hyperion, Richard Allen, is finding fewer reasons to be positive. "Last year was a painful blip - with card payment fraud up significantly, partly due to some very big cases - and so the comparison is best done against figures for 2007. That still gives a trend downward, but far less dramatic."

He may have a point. There were more than 26,000 phishing incidents in the first half of 2009 – a 26%





increase on the figure in the same period last year. Online banking fraud losses rose to £39m, a 55% hike on the first half of 2008.

Allen said, "Looking at these numbers, the trend-bucking statistic is the reduction in card-not-present (CNP) fraud. I'm sure the likes of SecureCode and Verified-by-Visa has played a part in this, but the industry also has rolled out other countermeasures to stem the dramatic rise in CNP fraud over recent years. As a cardholder, you may have noticed changes like delivery only to cardholder address, address verification and the production of the card for travel. The reduction in CNP fraud is welcome, although the numbers certainly deserve some more investigation."

So what next? It's pretty obvious that businesses and individuals need to be more vigilant to protect themselves. Banks can also play their part, creating a position where online banking is conducted in isolation so fraudsters cannot access lucrative account information. Identity Fraud Prevention Week will stress the harsh consequences of identity theft. Many will choose not to listen. As long as the ignorance exists, instances of fraud will continue to increase, leaving more and more victims. Let's hope the message of Identity Fraud Prevention Week lasts a lot longer than seven days this time.

World News In Brief

Smart Card Alliance tackles U.S. Payments Fraud

U.S. payments fraud is expected to rise unless the industry looks towards new technologies like contactless chip cards, the Smart Card Alliance said in a new white paper released on 21st October. Fraud in the U.S. Payments Industry: Fraud Mitigation and Prevention Measures in Use and Chip Card Technology Impact on Fraud, developed by the Contactless and Mobile Payments Council, is available on the Smart Card Alliance website.

Criminals are known to exploit the weakest link in a payments infrastructure. With issuers in the rest of the world moving to EMV, it is likely that criminals are going to move counterfeit card activities to the U.S, attacking both U.S. and international issuers, as said by Randy Vanderhoof, executive director of the Smart Card Alliance. If the United States wants to avoid an incoming tide of higher loss, the industry must be willing and able to make investments in emerging technologies.

Much of the fraud on debit and credit cards in the United States results from activities like counterfeiting and card skimming. Credit and debit card fraud is possible because magnetic stripe cards use static data that can be copied and reproduced on fraudulent cards or used in an Internet purchase transaction. The Alliance does not see protection of data or better fraud detection techniques as the solution to the fraud problem. Rather, the solution is to replace this static data with dynamic data, because it renders stolen account or transaction information useless.

To achieve this goal, the Smart Card Alliance recommends contactless chip cards, already implemented throughout the United States. Current contactless payment devices generate dynamic cryptograms (encrypted codes); similar to those generated by EMV payment cards, so certain data on the card and the terminal change with every transaction. The authentication of the cryptogram assures the issuer that the card presented is authentic. If data is copied or intercepted at the reader, the data is already obsolete for future transaction attempts, and cannot be used successfully to counterfeit cards or replay transactions.

Gemalto launches first-of-its-kind SG FIPS Secure USB Token

Gemalto, the world leader in digital security, announced the FIPS 140-2 level 3 certification for its Smart Guardian (SG) FIPS Smart card-based encrypted USB drive with personal identity verification (PIV) integrated authentication ability. This first of its kind secure storage device is a zero-footprint Smart card protected flash drive that meets U.S. military 810-F environmental standard and is now available to secure the mobile data of U.S. government employees.

The SG FIPS solves the problem of shielding sensitive data in the mobile phones by providing data-at-rest protection for all government data on the device without impacting user productivity, while the PIV integration provides the convenience of only having to remember one PIN. This SG FIPS encrypted USB drive is also extremely easy to use.



Greater Manchester Integrated Transport: Delivering Achievable Transport Plans

By Peter Tomlinson - Smartcard & Identity News



Peter Tomlinson

The vibrant City of Manchester was an appropriate venue for the 23rd September transport conference, billed by organisers Public Service Events as their annual transport event. Greater Manchester Metropolitan County is one of the two City-Region pilots announced in this year's April Budget (the status confers powers closer to those that Greater London has, but not necessarily with a great deal of local accountability), and the city is in turmoil about transport:

- the bungled congestion charge proposal (which Graham Stringer MP, member of the Parliamentary Transport Select Committee, told the conference delegates was a mistaken attempt to introduce a regressive tax) was massively voted down by the electorate,
- many of the central area's streets have been dug up to both extend and refurbish the tram network (and a big gas main replacement job made the city look even more disorganised),
- Piccadilly Station is about as overburdened with people as the pavements of Oxford Street in London, and
- there are major grumbles about the bus fares (and politically about the rapidly rising contract costs for LA supported services) – but there some are free city centre circular buses, although a driver of one of them was telling would-be passengers that it is quicker to walk.

In the face of that, GMPTE and its political umbrella the ITA still hope to invest £1.5 billion in quick fix improvements, with integrated ticketing, delivered via an electronic ticketing system, a key component of the package.

We have been hearing for some time that GMPTE favours a London-style Oyster scheme, but today TfL is saying that a major part of Oyster (the PAYG part) costs too much to administer. Thus TfL wants to move many users to a direct contactless bank card payment method – and GMPTE now expects to follow. What GMPTE's constituency really needs (paraphrasing Graham Stringer again) is a "fair fares" scheme on an integrated network of contract bus services that go everywhere the travellers want to go, yet the PTE is not yet able to bring the passenger offering on their bus network up to the 1990s status of the London network (the original Travelcard era). We heard that 80% of the GMPTE area's public transport journeys are on the buses – but it is trams that of course are being pushed today, yet great big trams don't work very well in narrow streets (compare Brussels with its narrow bodied trams).

Manchester quite rightly points out that investment in its transport system has been well below that in London. From memories of Manchester over 40 years ago, it used to manage very well with a large bus fleet, some trolleybuses and some trains. Today's travel to work areas are much larger than in the 1960s, and the concentration of wealth generation in the major centres, and therefore of jobs, is also much greater (Manchester University's Urban Studies people showed us that), so Manchester really ought to have developed a metro and put it underground in the central area. Liverpool and Newcastle have metros, but Greater Manchester has seen the money spent instead on a motorway ring.

So can GMPTE take the lead in building a passenger-friendly and cost-effective local integrated ticketing scheme, while at the same time meeting the national requirement to 'accept' ITSO format Products?

At the end of September, ITSO's Board, now controlled by DfT, agreed the contents of the next release of their Specification (Version 2.1.4) – and a specification freeze for two years. But V2.1.4 cannot provide everything required to:

- Properly support the required mix of services, customers and ticket types across all of UK surface and sub-surface public transport, and
- Deliver on the government mandate of 'all cards must be useable everywhere'.





Thus, scheme by scheme, there will inevitably be a variety of implementations that privately extend the ITSO Specification, as for example in a metropolitan area for the high volume local users. Such a metropolitan area scheme will also have to accept ITSO Products, starting with acceptance of ENCTS national concessionary travel passes on the buses, but may be unwilling to sell ITSO Products.

Then there is that national integrated ticketing requirement in DfT's Vision for "smart ticketing". That requires some form of through ticketing: multiple journey legs on multiple modes of public transport. That in turn demands provision for linkage between tickets – but the scope of the ITSO specification unfortunately does not include the consequential necessary standardisation of the processes to be run in terminals. And we still have to work out how railway station gates can handle this without a radical simplification of rail ticketing.

World News In Brief

INSIDE Contactless to create a new Mobile Payment Solutions in 2010

INSIDE Contactless announced an initiative to create a new class of mobile payment solutions that banks, brands, transit agencies and others can deploy quickly, easily and in a highly targeted way starting in 2010. INSIDE has already engaged with several innovative technology companies that share its vision to develop a variety of mobile payment solutions based on INSIDE's proven, certified MicroPass(r) platform that will enable existing mobile phones to support mobile payments, as well as transit, ID and access control applications. A number of these solutions are expected to reach the market as early as this fall.

Several new mobile payment solutions are coming to market from partners through INSIDE's initiative will enable mobile phones to integrate with a MicroPass-based secure element outside the phone, enabling solutions to be deployed more rapidly in 2010. Using microSD cards, existing BlueTooth channels, existing data connections, and other methods to communicate with the phone, these peripheral solutions will open the door to more robust, NFC-like payments. Transit and access control applications from among several virtual credit or debit cards stored within the mobile payment peripheral device, see the balance remaining on prepaid debit cards or transit passes, and even collect and redeem coupons and loyalty points.

New ACOS Smart Card - ACOS3X eXpress Microprocessor in market

Advanced Card Systems Ltd launched its new ACOS smart card - the ACOS3X eXpress Microprocessor Card (ACOS3X). This new card is the fruit of ACS's continual efforts in developing its COS (Card Operating System) technologies and was achieved by enhancing the security level and increasing the reading/writing speed of the cards.

The ACOS3X contains a powerful microprocessor and is fully compatible with the other members of the ACOS3 product line. The ACOS3X card supports a wide range of applications such as loyalty programs, parking registration, network access control and electronic purse. ACOS3X is built with a hardware crypto-engine, which substantially shortens the processing time of crypto commands like Secure Messaging, and its processing time is less than 1/3 of that of standard microprocessor cards, improving the security of various smart card applications.

Gemalto launches easy and convenient Protiva(tm) Smart Guardian

Gemalto announced the launch of Protiva(tm) Smart Guardian, a smart card enabled personal security USB device that offers digital data integrity and data loss prevention for enterprises. Smart Guardian provides nomad workforces with a trusted platform to securely access corporate resources.

Smart Guardian combines endpoint control and secure data storage for protecting sensitive information. It guarantees an unsurpassed level of security, since the encrypted data never leaves the Smart Guardian. Attempts to tamper with the device are detectable and intrusion attempts will cause the token to zero-out its contents.

In addition to providing the highest levels of security, Smart Guardian is remarkably easy and convenient to use. Users simply insert their authorised portable token and enter a pass phrase to unlock the device so that any data transferred to it is encrypted automatically.

Smart Guardian provides two-factor authentication based on something the user has - the USB token - and something the user knows - the pass phrase. This ensures that only authorised users have access to encrypted data, even if the device is lost or stolen. Smart Guardian tokens are easy for IT administrators to deploy and manage, and require no





user training.

"One of the biggest information security challenges today is protecting the large amount of confidential data used by business organisations and government agencies," commented Cédric Collomb, Senior Vice-President, Identity and Access Management at Gemalto. "The combination of endpoint control and secure data storage makes Smart Guardian tokens the ideal platform for protecting sensitive information and controlling how these are transferred throughout the virtual workplace."

T-Systems accredited as independent Testing Lab for rigorous DPA testing of Smart Cards

Cryptography Research, Inc. (CRI) announced the accreditation of T-Systems as an independent testing lab to conduct evaluations for the DPA Countermeasure Validation Program. The program, designed to help chip purchasers and smart card customers identify devices with effective security, involves rigorous independent testing of products to evaluate their resistance to Differential Power Analysis (DPA) attacks.

Robert Hammelrath, head of security analysis & testing at T-Systems has expressed his happiness in working with leading security experts, such as CRI, in the important field of smart card protection.

Big Differences in Big Banks' Security

Some of Britain's biggest banks appear to be leaving their customers' online accounts vulnerable to fraud because of poor security, says Which? Computing.

Online accounts at Abbey and Halifax have weaker visible security measures in place than some of their rivals, while Barclays' security is excellent, say Which? Computing experts.

Halifax has one of the least secure log-in procedures. It asks for three pieces of information to confirm a customer's identity. As each entry is typed in full, this makes the information vulnerable to a simple keylogger, a virus that sits on a computer and tracks every keystroke with the aim of collecting passwords.

Keylogging software is blamed for online banking fraud more than doubling in 2008. It soared to £52.5m last year, up from £22.6m in 2007.

In contrast, Barclays and Lloyds TSB ask customers to use drop-down menus. Simply using menus rather than the keyboard stops keyloggers from quickly capturing passwords. Barclays customers who forget their PINsentry device must enter a five-digit passcode and two characters from a memorable

word.

Browsing to another site can be unsafe with some accounts. Customers of Abbey, Alliance & Leicester, HSBC and Halifax are not immediately logged out if they browse, which means someone else could take over the session, leaving accounts vulnerable if accessed on a shared computer.

Which? Computing also found significant differences in how well money transfers appear to be protected. Abbey, First Direct, Halifax and HSBC have no visible security controls for money transfers, so if a banking session is hijacked, a criminal can enter the amount they want to.

Giesecke & Devrient holds 79 Percent of the Shares in secunet Security Networks AG

The public offer phase for secunet AG's shareholders is over. Giesecke & Devrient (G&D) now holds 79 percent of the shares in the Essen-based company. G&D had announced the voluntary public offer to purchase the shares back in July when it acquired the share package from RWTÜV AG, the major shareholder.

secunet AG is a specialist in high-security IT solutions, with international enterprises and public authorities among its customers. IT security technology is a strategic business field for G&D. Acquiring these shares will allow the Munich-based company to strengthen its foothold and continue expanding its excellent market position in this segment.

G&D had acquired the majority stake of 50 percent plus one share from RWTÜV AG and T-Systems in February 2004. In July 2009, G&D increased its stake by purchasing the RWTÜV AG shares.

GlobalPlatform Launches Transportation Task Force

International smart card infrastructure body, GlobalPlatform, has launched a Transportation Task Force to actively contribute to the evolution of smart ticketing solutions and to promote the benefits that GlobalPlatform's established technology can bring to the sector.

The Transportation Task Force will aim to create a forum with other transportation organisations to promote the value that interoperable technology can add to smart ticketing implementations. The group will also work with the organisation's Card, Device and Systems Committees to modify and advance GlobalPlatform's existing specifications to address specific requirements as highlighted by the industry.





Convergence on the Horizon

By: Watchdata Systems 



After years of being mired in their stakeholders' political bickering, contactless smartcards marrying transport and payment functions finally look like they are taking off.

Public transport commuters are set to enjoy far greater convenience now that smartcard industry players have made headway in resolving differences and coming up with a charging model that is acceptable to all parties.

Contact-less transportation cards are currently wide spread around the world. For example: Oyster Card, as used in London, Shanghai Public Transportation Card (SPTC), Hong Kong's Octopus card and so on.

Watchdata systems, a Chinese pioneer in smart card and contactless technology solutions, have made several successful deployments of their transport cards earlier this year after making headway in resolving differences and coming up with a charging model that is acceptable to all parties. Watchdata cards with micro and macro payment capabilities have now reached the big league.

One of the first large scale transport card deployments emerged in Hong Kong in 1997, as it was weaved into a compact transport card to facilitate fare collection for the mass transit system. Singapore had its own magnetic stripe card servicing transport commuters when the Mass Rapid Transit (MRT) was started way back in 1988. Subsequently, Singapore's card payment system for public transport evolved to a contactless smart card called the ez-link card. And it was not long that ez-link made its way into almost every Singaporean's – children, adult, senior citizens and national servicemen's wallet.

The 'tap and go' experience provided by the ez-link card meant that commuters would no longer need to remove the card from their wallets or handbags. Thus it became such an integral daily item that other functions of the card such as smart access was adopted by private organizations, building owners and government bodies such as the Land Transport Authority (LTA) and Ministry of Education (MOE). This ez-link card was also used to incorporate loyalty rewards scoring and tracking for the tertiary student community.

The high growth and proliferation of this ubiquitous item next caught the eyes of the financial sector, as they had for decades been pushing and issuing credit/debit cards for macro payments. With the integration of micro and macro payment functions on transport cards, travellers can now take buses, trains and taxis, pay for a wide range of bills and carry out credit/debit card transactions worth thousands of dollars with a single card.

It was only earlier this month that Watchdata created yet another milestone in the path of such co-brand cards' development, with the launch of Singapore's first 3-in-1 multi-application single-chip smart card. The company did this in collaboration with DBS and Visa. This highly customized and flexible single-chip smart card offers customers multiple capabilities for cashless payment and uses Watchdata's technology approved by Visa for Visa Smart Debit Credit (VSDC) and payWave.

The card also supports the Singapore Standard for Contactless ePurse Application (CEPAS) that provides better convenience and flexibility for consumers in making cashless payments in and around the island city-state. This single-chip card deploys the most advanced smart card security standards available in the market, thus ensuring reliability and accuracy in each payment transaction.

There is more good news waiting for consumers in the coming years, as the concept of convergence takes root in the telecom and government sectors as well. Telephone companies or Telcos across the world have realized that the ubiquitous SIM card-enabled mobile phone has the potential to become a powerful identification and authentication tool, and hence has started to engage government agencies to see how it could be used to access public services.

According to a Frost and Sullivan report on the Asia Pacific Contactless Smart Card Market, the market earned revenues of US\$770 million in 2008 and will grow to US\$1.35 billion by 2014. However, Gartner's 2009 analysis of the market predicts that by 2011, 20% of smart card authentication projects will be dumped and 30% scaled back in favour of lower-cost, lower-assurance authentication methods.

Across the Pacific Ocean to the shores of Europe, phone trials in the realm of NFC (Near Field



Communication) Technology have seen that adoption is slow (exception: Nokia's "6216 Classic" NFC-equipped handset), as phone manufacturers have yet to fully embed NFC into the phones.

Bridging this obstacle is Watchdata's SIMpass™ technology that will play the role as an interoperable platform. According to company news sources, SIMpass™ is an effective, near-term alternative and implementation of some international mobile payment standards (such as NFC) that paves the way for a broader adoption of such standards down the road.

And, while many governments remain cautious due to the lack of public sector deployment examples, it is obvious that the potential for convergence is tremendous. To industry experts, it will not be long before consumers can look forward to transport, payment, communication and public services from just one card.

With the prediction made by UK-based Juniper Research that 700 million mobile users will be equipped with NFC contactless technology by the year 2013, it's only a matter of time before consumers will have the world at their fingertips.

World News In Brief

Zurich UK Discloses Loss of Data Tape with Customer Information

The UK branch of Zurich Insurance plc ("Zurich UK") announced that it has written to some 51,000 general insurance customers and other parties in the UK to inform them of the loss of a back-up data tape in South Africa and the remedial actions being taken. The customer letters also set out the precautionary measures that Zurich UK recommends that customers can take as well as the steps that Zurich UK has in place to support them.

The back-up tape was lost during a routine transfer within South Africa to a data storage centre in August 2008. The back-up tape also held details of customers and other parties in South Africa and Botswana. Zurich UK's investigation into the loss of the back-up tape has revealed deficiencies in the management of data tape security procedures in South Africa.

To date, Zurich UK has seen no evidence to suggest that this data has been misused or compromised.

Zurich UK has appointed KPMG to conduct a thorough investigation of this matter. KPMG will also be supporting Zurich UK to strengthen its data security procedures. At the same time, Zurich UK has taken steps to improve the security around the transportation of its data tapes.

NXP Wins Supply Contract for Chinese ePassport chips

NXP has announced that its SmartMX security chip has been chosen by the Chinese government to power the country's first ePassport scheme. Utilizing the latest developments in cryptography and security to protect the chip at hardware and software level,

NXP's portfolio of SmartMX products enables data to be securely stored on the passport, creating an even stronger link between the document and its owner. The Chinese government will start issuance of ePassports in 2010, and is planning to replace all paper-based passports. At present over 30 million passports are in circulation within China, therefore substantial rollout volumes of ePassports are expected in the coming years.

Prior to selecting NXP as its main supplier of ePassport chips, the corresponding ministry of the Chinese government undertook a thorough evaluation of Smartcard security chips. The selection has been confirmed by a government official in charge of the ePassport scheme in the following statement: "Following this independent review, we were able to determine that NXP's SmartMX technology offered the highest levels of interoperability, reading distances and read times, therefore meeting our exact requirements. Working in collaboration with NXP's distribution partner in China and the official development team of the ePassport scheme, we've developed an operating system to power the Chinese ePassport scheme based on the SmartMX platform."

"We are extremely proud of being selected by the Chinese Government to supply our leading SmartMX products for the upcoming rollout of electronic passports," said Guenter Schlatter, vice president and general manager, eGovernment, NXP Semiconductors. "Since the introduction of ePassports, NXP has been at the forefront of developing solutions to enhance border security, safeguard privacy and improve interoperability".





The Broken Promise of Anytime, Anywhere Card Payments

A new report from Aite Group, LLC assesses the true costs assumed by the card industry, when U.S. cardholders experience difficulties making card payments abroad. The report is based on a September 2009 Aite Group online survey of 1,019 U.S. resident cardholders that travelled to countries outside Canada - the Caribbean and Mexico between 2006 and 2009. It provides insight into the frequency of failed card payments abroad, the emotional response and lingering effect caused by failed card payments, and how the U.S. card industry can address this problem.

The full report can be found at:
<http://www.aitegroup.com/reports/200910261.php>

Gemalto's Large Memory PIV Card finally gets GSA Approval

Gemalto, the world leader in digital security, announced that its large memory Personal Identity Verification (PIV) card is now listed on the General Services Administration (GSA) Approved Product List (APL). The company has previously begun volume deliveries of the card for the U.S. federal government's PIV program, and the card has already received FIPS 201 and FIPS 140-2 certifications.

The Gemalto PIV Card is built on dual contact/contactless technology, on the JavaCard platform. This PIV card doubles the storage capacity and allows the identities of government employees and contractors to be verified electronically quickly, while resisting any fraud, tampering or counterfeiting. The card also supports adding new applications, such as biometric match-on-card, if desired.

Infineon Lost a Key Contract with Apple?

Shares in Infineon pared losses after comments from the company cooled market speculation that the German chipmaker lost a key contract with Apple. An Infineon spokesman told Reuters that the company had 'not lost any contracts'.

At 1024 GMT, Infineon shares were 3.6 percent lower at 3.25 euros, rebounding from losses as sharp as 10 percent early on Tuesday (27th October) morning. A Frankfurt-based trader said that the heart of the speculation was a legal debate over 'pass through rights' which allow a handset maker to automatically acquire all intellectual property rights when they purchase chip technology.

Although, Infineon has never officially said it has supplied Apple with the semi-conductor chips used to make its best-selling iPhone, but several

teardowns of the phone have claimed that Infineon makes at least two Apple branded parts in the phone.

3 UK Customers Gain Unprecedented Access to Mobile Money Services

Monitise, the UK's leading mobile money provider, has made it possible for the customers of 3 UK to be the first in the country to directly access a wide selection of its world-leading mobile banking software on their mobile phones.

3 UK is the first UK mobile operator to enable its customers both to receive bank balance alerts by text message and also to download a mobile money application that allows users to manage their bank accounts in real time.

Oberthur selects Award Winning Collis EMV PVT

Oberthur Technologies has accredited Collis with the prestigious role of being the preferred solution provider for EMV card personalisation validation software. The aim is to standardise common EMV card personalisation validation software across Oberthur's personalisation network.

The award winning Collis EMV PVT can test all interfaces of a card-under-test (Magnetic stripe, Embossing, printing, contact chip, contactless chip, NFC). These tools also offer full support for VISA, MasterCard, JCB, American Express, as well as support for domestic brands such as GIE CB (which includes test results in French).

Motorists to 'Wave and Pay' for Parking

Motorists in Central London will be the first in the world to park their cars by waving a credit or debit card at a meter. The initiative, by Westminster Council, comes as the Government moves to encourage the use of cashless payment for transport across the country.

Thanks to the "wave and pay" technology, motorists will neither have to carry cash nor remember their pin number when they park. Instead, they will use contactless credit cards, which they will swipe across a magnetic reader fitted on 20 machines in the West End early next year.

If successful, the readers will be fitted to other meters throughout Westminster. Southampton is also planning to introduce the same technology in spring, and other councils are also expected to follow.

The Department for Transport welcomed the Westminster initiative. "This parking trial is a positive step in the direction of seamless travel", a spokesman said.



Macro move towards Micro-payments

By Suparna Sen, Smartcard & Identity News



Suparna Sen

The usual methods of payment made using Mastercard and Visa carry a charge. A transaction fee often around 0.25 cents made by the merchant makes very small payments unprofitable. Because of this, many companies have tried to capitalise on by making alternative payments systems (micropayments). BitPass, FirstVirtual, Cybercoin, Millicent, DigiCash, Pay2See, and such other online payment systems and providers tried to offer paid digital content and services to customers. However, they ultimately failed to bring any success due to elaborate and meddling sign-up forms, flaky business models, and mandatory plug-ins.

Background;

Bitpass was a California based online payment system for digital content and services, founded in December, 2002. It officially closed down its operations on January 26, 2007, without providing any immediate reason for the shut down. FirstVirtual, the first commercial offer to secure payment for digital information and services over the internet, operated between 1994 and 1998. CyberCash (formed in August 1994), introduced the electronic coin service that enabled cash transactions, typically from \$0.25 to \$10, for buying digital goods and services like software, articles, research, games and music.

DigiCash, a pioneer in the micropayment field, filed for bankruptcy in November 1998 after several years of trying to convert businesses to the idea of charging in tiny increments. MilliCent used an online system of electronic currency called scrip to purchase electronic information and other forms of electronic content from vendors, at a price, from a minimum of one cent (\$.01) or less to a maximum of approximately \$5.00. Pay2See was formed in April 1997 in Oxford, England to provide consulting and information to companies like Chase Manhattan Bank and Bertelsmann on high technology content delivery systems, watermarking, payment system monitoring, and so on.

However to many, these online payment systems failed not because of poor implementation, but because online users often can find free alternative digital content. The controversy over paid content versus free content has gained momentum recently, with Google, the world's largest search engine provider, announcing its plan to introduce a micro payment system aimed at helping online publishers earn additional revenue.

On the request of The Newspaper Association of America, Google submitted its proposal of the micropayment system, which will be an extension of Google Checkout - a payment system that Google rolled out in 2006 and made itself a competitor to eBay's PayPal service, the leading system for online payments. The Newspaper Association of America has requested 10 top technology companies of the world, such as Microsoft, IBM and Oracle to submit paid-content proposals, of which it choose the one submitted by Google.

Now the question is how do you get people to pay for something they're used to getting for free?

The question not only revolves around online publication agencies, but bedevils the music and film industries as well. It's no less of a challenge for anyone trying to monetize an app for Facebook, MySpace or Bebo. But a new approach is emerging, according to the micropayment believers, making it cheap, really cheap. Charge just 10 or 20p for a bingo card, an accessory for a virtual pet or a weapon for a game character. Get enough people signed up and, once you've added up all those pennies, you've made a tidy bunch.

However, like all ideas that sound too good to be true, you probably will be thinking in the same way. But it's not just a theory.

"The nanopayment Report" by Tom May says that in Asia social networking sites have been making big money for years. In 2007, China's Tencent raised \$523million (£318.494million) in revenue— that's four times as much as Facebook, in a country where the average monthly wage is less than \$20 (£12.18)— with operating profits of \$224million (£136.410million).

Moreover, it is found that in general, young people tend to spend more on high-tech gadgets and games. Asian fads Karaoke and Pokémon have made it big in the market and the same thing can happen in the West as well.

The success of Apple's App Store has proved beyond reasonable doubt that people are willing to pay small amounts for virtual goods, whether useful or trivial. More than a billion applications created by 50,000 developers have now been downloaded from the Store, typically for between \$0.99 and \$4.99, from fart noisemakers to translators to virtual spirit levels. Yet if such success is to be repeated on social networks, there's one thing everyone agrees on - the need for stable, reliable, easy to use payment platform.



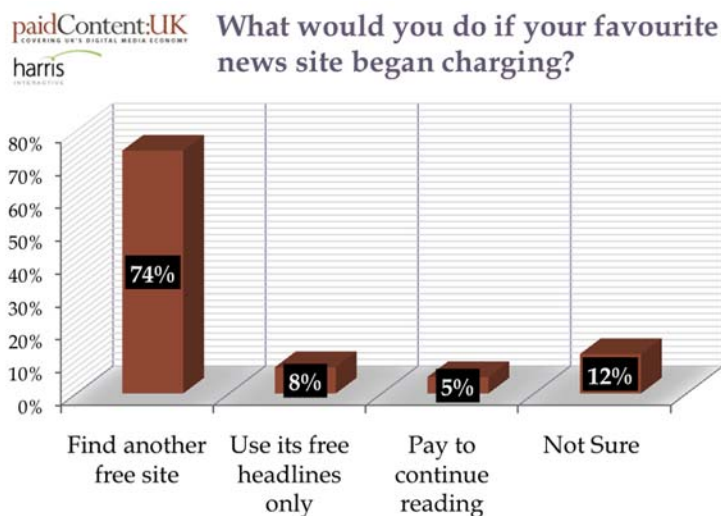


At the end of 2007 it looked as if Facebook was joining in the party. Just before Christmas of that year, the site announced the beta test of Facebook Payments, which would enable firms to accept small payments from users directly inside their Facebook apps. But nothing really happened. However, you can't keep a good idea down for long.

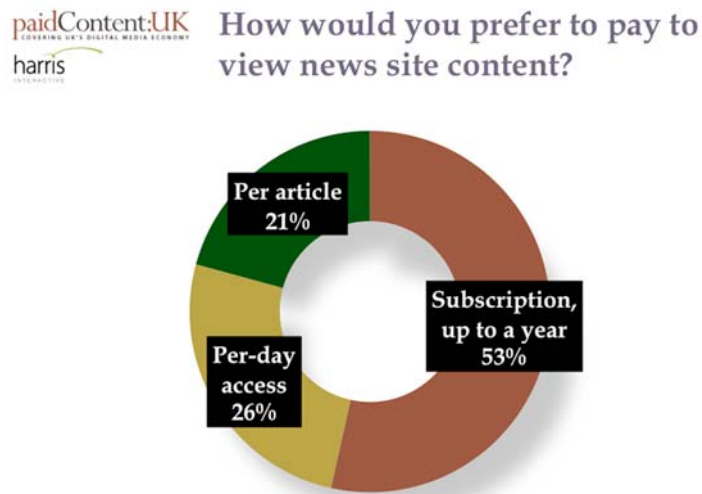
MySpace COO Amit Kapur revealed at last November's Web 2.0 Summit that MySpace is working on its own payment platform. And while developers are waiting for the big boys to come up with their goods, a number of start-ups have already sprung up to fill the gap, such as Spare Change (sparechangeinc.com), Zong (zong.com), OneTouch (onetouchpurchasing.com) and PayByCash (paybycash.com).

In UK, the site called paidContent.UK (www.paidcontent.co.uk) owned by Guardian newspaper, was found to help define sustainable business models and innovation within the digital media sector.

paidContent.UK made 2 online polls to find out how many people would respond to online payment. The first poll revealed that most users 'would run a mile' if they are to pay for news content.



The second poll which was conducted at the end of last month surveyed 1,188 adults (aged 16-64) online within the UK between August 26 and September 2, 2009 only to find out if web users have to pay, would they prefer subscriptions over micro-payments?





American journalist Michael Kingley also thinks in the same way. According to him, newspaper readers have never paid for online content (words and photos) before.

Walter Isaacson, the President and CEO of the Aspen Institute stated that iTunes of Apple Inc. is an easy and quick micropayment method. According to him, something like digital coins or an E-Z Pass digital wallet - a one-click system could easily be developed to make purchase of a newspaper, magazine, article, blog, or application. Although, companies like Flooz, Beenz, CyberCash, BitPass, Peppercoin, and DigiCash have failed miserably in trying to implement micropayment systems, nowadays things have changed. "With newspapers entering bankruptcy even as their audience grows, the threat is not just to the companies that own them, but also to the news itself," as the New York Times columnist David Carr says earlier this year.

However, challenging the views of Walter Isaacson, Clay Shirky, the author of "Here Comes Everybody," tweeted: "MicroPay talk appears whenever a biz is dying". The basic thrust of Isaacson's argument, 'It works for iTunes, so it can work for news' has been widely criticised. When Walter was interviewed on The Daily Show, host Jon Stewart pointed out that while a song lasts a lifetime, news is fleeting, so people are less willing to pay for it. Also, unlike iTunes, news providers have to compete with a myriad of legitimate free sources, not just online, but also on radio and TV.

Clay Shirky continues; "micropayments can only succeed when a provider has a monopoly on a particular type of content and a proprietary system of distribution. For instance, in the case of Cyworld, users who want a certain kind of digital decoration for their online presence can only buy it through Cyworld".

Now achieving the same level of control over other digital goods, especially something as easily duplicable as a photo or news article, is not easy a job.

Tony Cohen, CEO of X Factor producer FremantleMedia, called for a radical rethink of on-demand TV. At the MediaGuardian's Changing Media Summit, he stressed on the need to look on for the potential of micropayments per-view. "Charging just a few pence, say £0.05, to watch catchup could really help stimulate demand", he said.

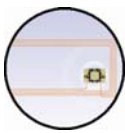
In support of Cohen's view, the San Francisco-based startup, Bitcents is allowing online news publishers to charge for their content. The company claims to provide the first fully-functional micropayment service that enables publishers to charge on a per-story basis and to determine their own prices.

Whether or not micropayments are a financial cure, all remains to be seen, but the fact that new payment methods are opening up to developers can only be a good thing. In this web world, when newer technologies and adaptations are continuously taking place, we can surely say that a high quality and professionally produced content can have a hierarchy of readers and an array of services, from free to highly customized and pricey.

Google has internet dominance to make micropayment a success where others have failed. Google have succeeded in dominating the search engine market and in online maps, blogs, and cloud applications (calendar, mail, etc).

Google believes that its micropayments model will be a simple payment vehicle available to both Google and non-Google properties within 2010. "The idea is to allow viable payments of a penny to several dollars by aggregating purchases across merchants and over time", as said by Google. But have they forgotten the time when Google Video got dumped badly. Google Video was mainly a pay site. It was not long that YouTube took over the online video world, eventually leading to Google shelling out almost \$2 billion.





Contactless Payments – Going Global?

By Steve Brunswick, Strategy Manager at Thales Information Systems Security



Steve Brunswick

Contactless payments are increasingly becoming a part of our daily lives. In London, for example, residents have long become accustomed to using Oyster cards for travelling around the capital. Contactless is now an established form of payment in some shape or form across many countries around the world, with Japan and South Korea leading the way. In Europe, contactless cards have been issued, and some shops are equipped with terminals to read them. As for the US, it remains the biggest population for contactless cards where merchant infrastructure is already in place and most of the major cities with transit systems are using contactless.

Contactless trends around the globe

Contactless payments are likely to boom across Europe over the next two years, thanks in part to a series of bold initiatives from card companies, mobile phone operators and big retail groups. Two payment card operators in Europe, Visa and MasterCard, are pushing ahead with their contactless plans. Visa estimates that the number of its cards equipped for contactless transactions, the so-called 'Visa payWave', will grow from the current 0.5 million to 7 million by the end of 2009 in Europe. Most cards will be distributed across the UK, but Italy and Turkey are the other two front-runners. Pilot projects have also been launched in France, Germany, Poland, Spain and Switzerland.

Visa's main competitor, MasterCard, is committing similar amount of resources across Europe to furthering the trend. Earlier this year, MasterCard and global retail leader Carrefour announced the launch of the PASS MasterCard® card, the result of a partnership designed to offer French consumers the very latest in 'best-in-class' card payments. The MasterCard® PayPass™ technology is already available on nearly 44 million cards and devices across the world. Barclays have announced that their debit card customers will have contactless cards by 2011, which it predicts will double card transaction volumes for all UK acquirers.

Asian consumers are already well versed with contactless technology for both payment and transport. Japan and Korea lead the way, but Taiwan and Malaysia also have a fast adoption rate and already have contactless infrastructures for payment (Visa Paywave and MasterCard Paypass) and contactless tickets for transportation. Tech savvy city dwellers use their mobile phones to ride the subway, pay for movies and even meals. Given the progressive nature of the region, the move to mobile payments and the uptake of Near Field Communications (NFC) technology is expected to occur at a fast rate. Indeed, Japan and Korea have already been pioneering this technology for some time.

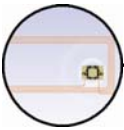
The U.S. has a more diverse card market than many other regions where brands such as American Express® (ExpressPay) and Discover® Network ZipSM are very important. It was back in 2005 that North America first saw the introduction of contactless payment cards for small value payments and the 1990s when contactless transit cards were introduced. The infrastructure support for contactless payment has grown ever since. Various retailers have already seen success with contactless payment cards, and are also expanding the infrastructure throughout the region. Many have been able to measure a 40 per cent growth in sales after the introduction of contactless payment cards due to reduced down time and increased convenience for both the retailer and the end-user.

More further afield, a 'Citi Tap and Pay' scheme has been introduced in the city of Bengaluru, bringing contactless credit card payments based on NFC technology to India, and MTN Uganda is rolling out a nationwide mobile payment programme. In Latin America, Visa has announced a mobile payment programme in collaboration with Visanet Perú and Telefónica.

Card or mobile – which will win?

It's clear that the rollout of contactless is acting as a driver for payments made via mobile phone handsets. Although the majority of contactless rollouts to date have been card-based, the mobile is becoming a strong contender as the de-facto device for contactless payments as the above regional developments indicate. Initially held back by a lack of consensus between the mobile and banking worlds, there have been some recent developments which are taking us a step closer to enabling widespread mobile payments, particularly in Europe.





In 2008, GSMA, the association grouping the main mobile phone companies in the world, struck a deal with the European Payment Council, representing the EU banking sector, to deploy the new technology in the EU. While progress has unequivocally been made in this area, there do remain certain issues to iron out.

Issuers are concerned about the fact that if the contactless application resides on the mobile, they will need to create a different model for the provision of the payment functionality. Currently, when a bank issues a card, it creates the encrypted data and posts the card to the customer. However, when banks are issuing a contactless payment application for a mobile, they will not have the actual device, so they will need to rely on over-the-air provisioning by making use of the services of a Trusted Service Manager (TSM). While these technical challenges between the issuers and the MNOs (Mobile Network Operators) have been largely resolved, question marks still hang over who 'owns' the customer and the relationship.

A business model that works for both MNO and issuer is needed, since the MNO will not gain additional airtime revenue once the application is deployed. The mobile phone acts only as a carrier, with the payment application residing on the SIM, and interacting with the payment system via the NFC service, rather than the mobile network.

A new Nokia phone is due out later this year, which is based on the new SIM standard, and this will hopefully drive mobile payments, in Europe at least, and help to resolve some of the issues discussed above.

Ultimately, bankcard and mobile phone will co-exist for some time in the contactless payments space. In fact there is probably room for other form factors of contactless payment including key fob cards and contactless wristbands, which have been used by MasterCard for festival goers for on-site payments. Ultimately, the consumer, or a particular demographic, will dictate the success of individual contactless devices through their popularity and up-take.

Readying the payment infrastructure

If contactless payments take off as expected and replace even a small percentage of cash payments worldwide, card transaction volumes are likely to increase dramatically. From a payments infrastructure point of view, this increase will need to be planned for appropriately, particularly in the U.S, where all card payments are processed on-line at the time of the transaction. Payment card companies, retailers and payment processing organisations will need to prepare their payment processing systems in line with expected demand, so that a consistent service can still be provided.

In other geographies, contactless transactions are generally processed offline and sent off to the acquirer in a batch at the end of the day during off-peak times. In these countries, the impact on the payment network capacity required will be less dramatic. Wherever contactless payments are deployed, the good news for acquirers and payment processors is that with the right software, the existing payment card security infrastructure can handle contactless payments.

Security implications

Although fraud remains a concern in all payment channels, contactless payments should be viewed as robust from a security point of view. The industry has been careful to add security on both the contactless devices and in the processing network, including a unique built-in secret key on the card, which generates a unique CVV.

In addition, the networks have the ability to detect repeat transaction information, which has been a problem in the past for other types of transactions. A 'repeat attack' is where the fraudster obtains all the information from a real transaction and then conducts the same transaction many times over. The fraudster relies on the system that they're trying to attack not realising that it is receiving the same instances of the real transaction. The added network security for contactless means however that a contactless transaction can only be processed once. Furthermore, the processing of contactless payments does not require the use of the cardholder's name and some cards do not even include the cardholder's account number.

Contactless – what the future holds

It's more than likely that large cities around the world will continue to lead the adoption of contactless where the application can really add value around convenience, speed and security for low value payments. As with all new technologies, uptake is gradual but it seems that contactless payments are now well positioned for mainstream adoption.

