February 2010

Volume 19 • Number 2

Smart Card & Identity News

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

www.smartcard.co.uk

8 • Mobile World Congress showcases latest innovations

9 • PayPal Services blocked in India

11 • Multi-Application Smart Cards – Gaining Momentum

17 • Mobile payments – it takes more than two to tango

Terminal Decline in Cambridge

This month the media has been full of it, The Computer Laboratory from the University of Cambridge has reported[1] (yet again) that Chip & PIN (EMV) is broken although many others seem unconvinced. We are happy to be able to tell you that EMV is probably all right, certainly fit for purpose, but that the real problem is the Point of Sale (POS) terminals. These terminals can (in principle) be interfered with ad infinitum and can cause vast numbers of fraudulent transactions both direct and indirect and it's only going to get worse.

So who is right, has it or hasn't it been broken? To get at the answer we need to understand the principles behind electronic payments and more particularly the credit and debit card transactions we are all so familiar with at the Point of Sale. In particular we will show you why as a result of this attack some of the banks need to tidy up their back end systems, why we all need to worry about the security of the POS terminals and why we probably don't need to lose too much sleep over the EMV protocols.

Let's first look at it from the point of view of the cashier in the retailer; he wants to be paid in exchange for the goods he sells you. If we pay for goods at the POS with cash we are effectively handing over the financial asset from our pocket to that of the cashier's cash box. He gets the funds immediately, nobody else is involved in the transaction and all he needs to know is that the cash is genuine, i.e. not counterfeit. At the end of the day the retailer will deposit the cash collected at his bank.

Continued on page 4….

Smart Card & Identity News
Is published monthly by
Smart Card News Ltd

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

Telephone: +44 (0) 1903 734677

Fax: +44 (0) 1903 734318

Website: www.smartcard.co.uk

Email: info@smartcard.co.uk

Editorial

Managing Director – Patsy Everett

Technical Advisor – Dr David Everett

Production Team - John Owen, Lesley Dann, Suparna Sen

Contributors to this Issue – Tom Tainton, Suparna Sen, Berend van Geffen, Peter Tomlinson, Jan De Meester

Photographic Images - Nejron - Dreamstime.com

Printers – Hastings Printing Company Limited, UK

ISSN – 1755-1021

Disclaimer

Our Comments

Patsy Everett

Dear Subscribers

Well the Global Mobile conference in Barcelona has come and gone again. I don't know whether it's just me but I do still miss the event when it was held in Cannes. There was something about the location and all those intimate parties on the boats. C'est la vie but perhaps even more so is the move from technology to the joys of understanding the consumer proposition. Applications are the name of the game and I must admit that even I am getting a bit excited with all these iPhone gizmos. There is something quite fascinating standing in the supermarket waving your mobile phone over the barcode of products to see how much that item might cost down the road. For those of you interested the application is called RedLaser and costs just $1.99.

To me the theme this year was very much about smart phones and how everybody is expecting this market in particular to really pick up in 2010. And yet there wasn't very much about the security of these smart phones but we know from the PC world that when you have multi application devices connected to the internet that security problems will follow. You may have gathered from our lead article this month that the security of payment systems for example has moved from the smart card to the terminal or in this case the mobile phone.

It was brought home to me this month when I came to upgrade my mobile phone, it's a bit like an electronic handbag as it contains all my personal data and dare I admit it not that well protected. So what would happen if you lose your phone? I think most of us would need to worry. I couldn't resist asking David Everett about this problem and after getting somewhat bored about Cloud Computing and keeping everything in the sky the discussion came to a short end when I reminded him about how often he seems to have a flat battery.

Anyway where does that leave most of us? Where do you store the data on your phone, is it in the SIM card, the mobile phone memory or the SD memory card plugged in the side? It turns out and I don't think I ever really knew that it's in the mobile phone main memory, where the phone goes is where my data goes and I can't just take it out when I come to change phones.

So I've come to the conclusion that the SIM doesn't seem to be doing very much for most people apart from the basic phone operations. And yes you're dying to ask me, how about NFC, surely that means all the applications will be going in the SIM card. Well sorry to disappoint you but as far as I can see NFC is still stuck on the commercial issues about how you might share the SIM card which is the only bit in the phone the Network Operator controls and they don't seem to be rushing to make it available. I saw somewhere that Nokia has cancelled its planned 6216 NFC phone. Lots of talk about how the proposition needs to be improved but I wonder if it has anything to do with the SWP (Single Wire Protocol) which I gather means that the SIM card has to be shared – surely not?

Patsy

Contents

Regular Features

Industry Articles

Events Diary

March 2010

1-5 RSA Conference 2010, San Francisco, USA
- http://www.rsaconference.com/2010/usa/

3-4 Border Security 2010, Crowne Plaza Rome St. Peter's Hotel & Spa, Rome, Italy
- http://www.smi-online.co.uk/events/overview.asp?is=1&ref=3192

15-16 CEE Cards Market 2010, Radisson SAS Béke Hotel, Budapest, Hungary
- http://www.smi-online.co.uk/events/overview.asp?is=3&ref=3196

15-19 Cards Africa, Johannesburg, South Africa
- http://www.terrapinn.com/2010/cardsza/

23-24 Global Commercial Cards and Payments Summit 2010, New York City, USA
- http://www.commercialpaymentsinternational.com/global-summit.htm

April 2010

9-11 Fingerprint Society Annual Conference, University College London, UK
- http://www.fpsociety.org.uk/events/london2010/index.html

20-22 WIMA-NFC Conference, Monaco
- http://www.wima.mc/content/Home-page/home_pageUK.php

20-21 SIMposium 2010, Rome, Italy
- http://www.simposiumglobal.com/

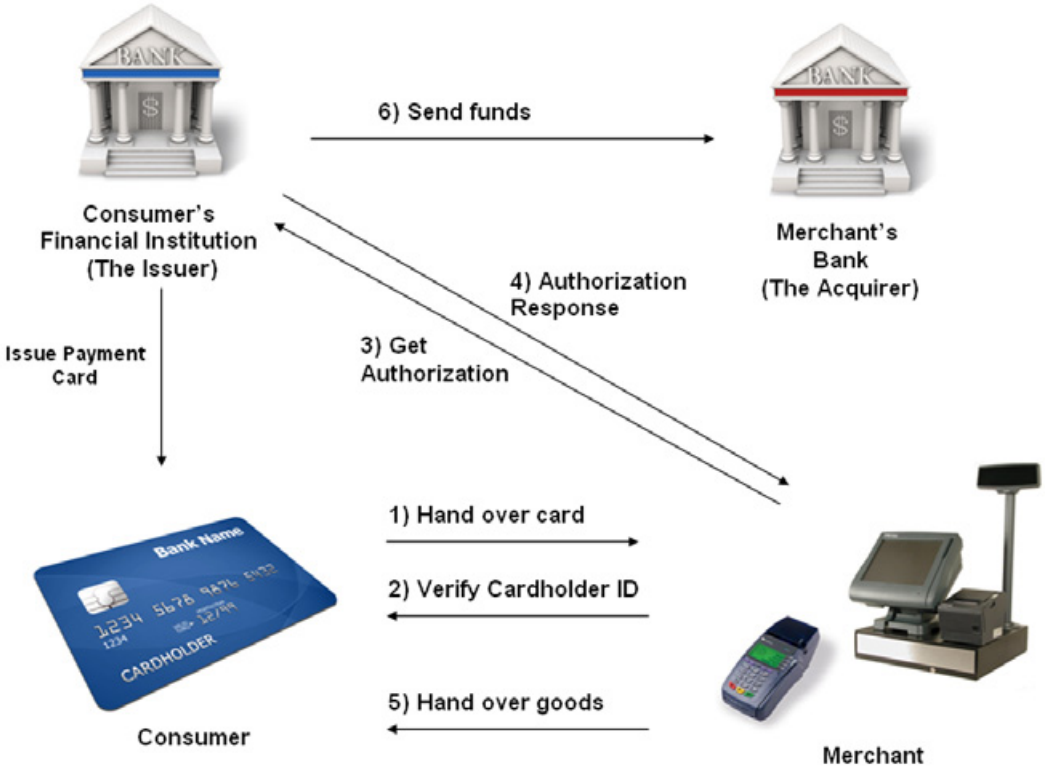
21-24 Prepaid Cards Asia 2010, SUNTEC Singapore Int'l Convention & Exhibition Centre
- http://www.terrapinn.com/2010/prepaidcards/

26-28 Cards/2010, Frei Caneca Convention Center, Sao Paulo, Brazil
- http://www.cards2010.com.br/ing/index.htm

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

Terminal Decline in Cambridge …. Continued from page 1

Now let's look at a consumer with a bank account at some Financial Institution (FI) and a debit card that allows the user to make payments against that current account held by the FI. Who are the participants in this transaction?



Suddenly life gets far more complicated and we enter the world of the 4-Party model. The reason for this complication is that the consumer no longer holds the cash or funds in his pocket, they are actually held by his bank which in the 4-P model is called the Issuer (of the card representing the account held by the bank). When the consumer purchases goods at the merchant he is not handing over cash or funds but instead an instruction to his bank (the Issuer) to make payment to the merchant's bank (called the Acquirer because in practice all the merchant terminal transactions pass through the Acquirer in order to get to the Issuer). Doesn't this sound like an electronic version of a cheque?

Yes, it's exactly that and do you remember what used to happen (a long long time ago)? The consumer would write the details of the transaction and sign the cheque, the merchant would then hand in the cheque at his bank that would go and get the funds from the consumer's bank by passing over the cheque. The consumer's bank would look at the cheque and check the signature, then check the account has funds and if all is well make a funds transfer to the benefit of the merchant's account at its bank.

It seems remarkable but not that many years ago you could pay for goods with a cheque and take the goods away there and then. But things have changed and clearly we have all become more dishonest so the merchant would like to be assured that he is going to get paid before he hands over the goods. So what is required?

- The merchant wants authorisation (that says he will be paid) from the Issuer before handing over the goods
- The issuer needs proof of the consumer identity and the transaction details that need to be authorised (as an agent of the account holder) for payment

So for identity authentication you will remember the three Factors,

- Something you know
- Something you own
- Something you are

[1] Chip and PIN is Broken; Steven J Murdoch, Saar Drimer, Ross Anderson, Mike Bond; University of Cambridge, Computer Laboratory; To appear at the 2010 IEEE symposium on Security and Privacy

Well the card acts as something you own but on its own this would just be single factor authentication (1-F) so it's nice to have at least 2-F authentication. Well in the original world we used a signature (something you are, a sort of biometric) on the cheque so we could just use a signature at the merchant's POS. It provides forensic evidence in the event of a dispute and the cashier can compare signatures, it could even be done electronically. Of course we know this is not very good and the cashier could easily be fooled or even bullied. So enter the Personal Identification Number or PIN.

The PIN is clearly something you know and in conjunction with a card would provide the 2-F authentication. Now how can you actually authenticate the cardholder using the PIN without revealing its secret to all and sundry? Well you can't just give it to the cashier so either the terminal has to check the PIN or you have to send the PIN to the Issuer for checking. You can imagine the security problems of making the terminal adequately secure for PIN checking, the big problem is that you are in danger of creating a systemic attack on all PINs created by that Issuer and of course each Issuer is going to have his own method of protecting PINs. Let's quickly pass on and decide that the PIN needs to be sent to the Issuer. Without entering a long discussion it is readily apparent that the PIN will need to be securely encrypted at the POS terminal and that the Issuer will need to send an encrypted response to the merchant's terminal. If you didn't some hacker might decide to interfere with the communications channel between the merchant and Issuer and yes, don't ask, it's been done in the past.

Fast forward to Chip & PIN which is a colloquialism for the EMV (Europay, Mastercard and Visa) standards first publicly released in 1995. The chip was seen as the way of mitigating the forecasts for increased fraud in the electronic payments world. Not needing to go into too much detail here but the chip card allows 3 security functions to be achieved,

1. Cardholder authentication (by checking the PIN in the chip)
2. Card authentication (proof that the chip knows a secret)
3. Card data authentication (by application of a trusted digital signature)

Now we are starting to get to the problems so in reverse order, it is easy for the Issuer to digitally sign the data held on the card and to ensure that the POS terminal has the appropriate public key (let's avoid the detail of the Public Key Infrastructure or PKI for this discussion) to check the signature and therefore to be assured of the authenticity of the data. Problem is anybody can read this data and signature (after all the specifications are in the public domain) and could easily create a counterfeit chip holding this same data.

Card authentication, this is really the Achilles heal of the payment card's world. The concept is straight forward, the card needs to show it knows (contains) a secret without revealing the secret.

And last but not least we need to get the PIN to check the card and to know the PIN has been checked.

Here we come to the nasty problems that happen in the real world, perhaps the bank's customer can't manage a PIN, for example they may have some memory disorder. Then there are those occasions where it might be impractical to have a PIN pad like at vending machines. And all the time we must remember that the Issuer is holding the account on behalf of the cardholder, the bank must be assured of the identity of the cardholder and the genuineness of the transaction details. To make it worse there are good business reasons that not all transactions are handled by an on-line connection to the Issuer they may be handled by the terminal off-line. So in these cases the Issuer has to trust the POS terminal and the processes applied by the cashier. So what do we get,

- The chip does not mandate a PIN check
- The chip may not implement public key cryptography
- The terminal does not hold Issuer secret keys
- The terminal may operate off-line

There are two scenarios to consider,

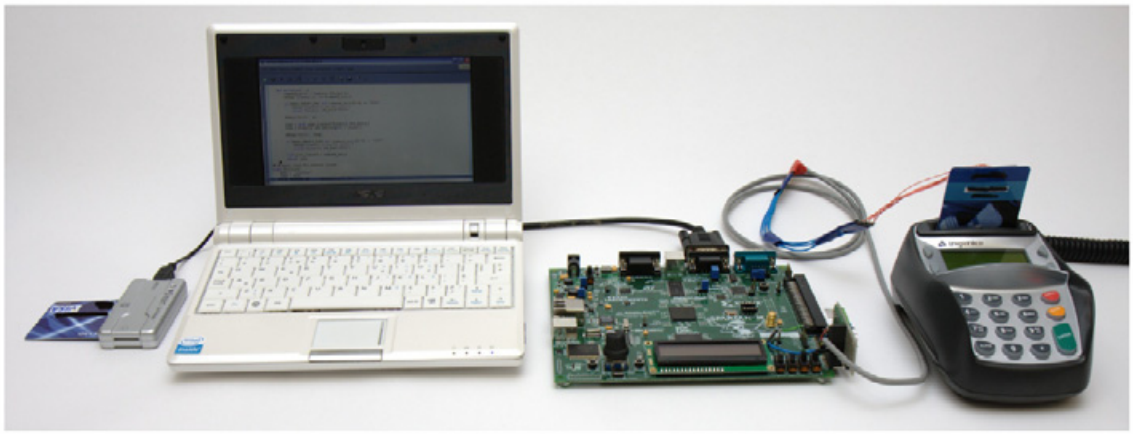
An off-line transaction where the chip doesn't implement public key cryptography, in this case the terminal is incapable of checking any data created by the card because it would require a secret key in the terminal.

So in this case the terminal sends the PIN to the chip card for checking and the chip replies effectively with an OK message. This message is unprotected because the terminal doesn't have any secret keys that would be necessary for an encrypted message. The Transaction Certificate (TC) is also a problem because the terminal doesn't have the necessary secret key to check it, it could be total garbage and it wouldn't know. The signed card data is initially sent by the card to the terminal and this can be checked by the terminal with the public keys previously provided.

Now we can quickly see that it would be easy to make a counterfeit card that will provide a copy of some genuine signed card data, which could say OK to any PIN check and could also create a fraudulent Transaction Certificate that the terminal can't check. The issuer would spot the problem when it gets sent the TC but that would be too late, the goods have gone. If the terminal is operating on-line the fraudulent card (which has to in this case generate an encrypted authorisation request message) would be spotted immediately and the transaction would be declined.

So in the second scenario let's look at an attack on an on-line POS terminal,

For simplicity we have left out some of the messages but this is enough to show the problems and the basis of the latest attacks form the Cambridge Computer Laboratory. Here it is assumed that an attacker intercepts the communication path between the POS terminal and the chip card. This could be done in the terminal or by inserting a skeleton card with wires to the interception system in a genuine terminal as shown below from the Cambridge University paper. In this scenario it is assumed that the card is genuine, it was stolen or found by the attacker, but the attacker doesn't know the PIN.



We can already see where this attack is going, the chip card knows that a PIN check is optional and so will be very happy not to get a check PIN message. The attacker who is intercepting the messages between the card and terminal just removes the PIN check message and sends the necessary (unprotected) OK message to the terminal. The terminal is now satisfied that a PIN check was successfully completed and carries on with the rest of the transaction. The flaw detected by the Cambridge researchers is that the Issuer is not checking the Authorisation Request Message (ARQC) which is encrypted (to create an authentication code) to determine if the card has checked the PIN. This information is in practice included in the ARQC but arguably what the Issuer does about it is outside the EMV specifications. So what they have shown is that you can make a transaction (against some Issuers) at an online POS terminal with a lost or stolen Card without any knowledge of the PIN.

One would want to argue that this is not a break in Chip & PIN but more a lax attitude by some of the Issuer banks who are perfectly capable of checking this information. One of the nasty problems here is that the consumer could be accused of using a PIN (and therefore liable for the transaction) when he didn't. I believe the banks really need to put this right.

But where does all this lead us? It's really an understanding that the POS terminal environment is truly hostile, on-line or off-line and that no matter how secure the individual components any interception between the constituent parts can lead to fraud. We have also discussed previously the TJ-Maxx attack in the USA where the attackers intercepted the terminal Wi-Fi connections to get the details of over 40 million credit cards that could then be used to make fraudulent transactions.

What must be clear here is that if an attacker can interfere with the POS terminal environment then only the imagination can limit the levels of possible fraud. For instance the consumer doesn't actually know what the terminal is doing. It could easily use a genuine card to make transactions of a totally different value to what they expect and of course the terminal could be modified to make a transaction to the benefit of a totally different merchant (depending on the terminal acquisition architecture), the point here is that no matter how good the security of the chip card a fraudulent terminal can be the source of rampant fraud which has already been shown to be the case.

How can the user of a POS terminal (or a PC or a mobile phone) be assured of the authenticity and integrity of that device? Don't laugh we looked at this problem over 25 years ago, I still remember the conversations with David Chaum who I think was the first person to address this problem with the concept of a trusted device that you carry in your pocket. It connects the card to the terminal and has its own keyboard and screen so you can see what is going on. You might be thinking that the mobile phone is the modern equivalent? It could be if it did nothing else, but an internet connected device with downloaded applications – Oh no, not yet, and not in the foreseeable future!

Dr David Everett.

Mobile World Congress showcases Latest Innovations

By Tom Tainton, Smartcard & Identity News

Tom Tainton

The 2010 Mobile World Congress took place in Barcelona this month, showcasing the latest products and cutting edge technology that will define the future of the mobile environment. The event was attended by over 50,000 mobile professionals who gathered to experience some of the industry's most innovative mobile solutions.

Chief Marketing Officer at the GSMA, Michael O'Hara says the Mobile World Congress is a must-attend event: "Through its expansive exhibition and focused specialist events, we address every aspect of the broad mobile communications eco-system; attendees will experience the latest developments in sectors such as healthcare and finance. The GSMA Mobile Innovation Grand Prix celebrates the products that have changed the face of mobile technology".

One of the finalists for the accolade is Dublin-based mobile security firm Sentry. The company have developed the world's first firewall for SIM cards, Sentry Wireless – a security solution that protects children, stops SMS spam and monitors corporate expenditure, controlling the types of contact-less payments that can be made. Sentry Wireless has already won the 'True Mobile Start-up' award last year. The technology has multiple purposes such as Kidsafe, an application that enables parents to approve numbers that can contact their children. SpamGuard allows subscribers to block SMS spam. The reported spam is then blacklisted to protect all subscribers on the network. CallGuard assigns call allowances to individual phones, restricting access to premium and international services.

While Sentry Wireless saves the user from spam and potential fraud, another Mobile Innovation Grand Prix nomination, WellDoc's 'Diabetes Manager', could save lives. WellDoc is a healthcare company that develops mobile solutions to help patients manage chronic disease conditions. The Diabetes Manager solution turns a patient's cell phone into a virtual diabetes doctor that provides personalised feedback to the patient. The mobile platform has demonstrated to significantly reduce the risk of complications of diabetes. WellDoc is also developing solutions for conditions such as asthma, obesity and heart failure.

Secure Phone is mobile device solution that manages security and cost for companies, lowering smart phone costs whilst maintaining reliability. Developed by Inquso, the Secure Phone is a management system tool that has the capability to administrate and secure the usage of mobile technology. The device is divided into three main areas of functionality: device, asset and security management, allowing the cost-conscious organisation to benefit from increased mobility without compromising on security.

STMicroelectronics unveiled their robust low-power processor chip, ST32-MIC, an application dedicated to managing SIM data for machine-to-machine (M2M) cellular communications, a market that is predicted to account for over 200 million mobile connections within three years. The technology enables machines to connect to networks, authenticating themselves and communicating automatically. The ST32-MIC can be used in the European eCall road-accident alert system. Planned for launch later this year, the application allows vehicles to inform rescue services of location and details of an accident. It can also be used and utilised in retail systems such as replenishment monitoring for vending machines, asset-management systems and utility-meter reading.

Fiserv, a global provider of financial services technology solutions, launched 'Corillian', a personalised user interface which combines common banking functionalities onto a single, easily viewable screen. Users of the personal finance management tool will see a graphical display of account balances, transfers, e-payments and recent spending behaviour. The application makes management of day-to-day financial tasks easier and simpler for consumers.

PayPal Services blocked in India

By Suparna Sen, Smartcard & Identity News

Suparna Sen

Thousands of medium and small companies have faced a major cash crunch after India's top bank regulator - the Reserve Bank of India(RBI), suspended PayPal services in the country. Indian users were left frustrated by this sudden decision from the Central Bank.

Many Indian information technology companies and freelance computer professionals were in a state of shock to find out PayPal, (the US-based online payments and money transfer company), suspending all transactions within India. Many Indian merchants have adopted Paypal payments, because it has proved to be a more reliable and quick method of receiving payments from overseas clients.

The problem started over the Payment and Settlement Systems Act, which came into effect in India in August 2008. According to RBI, under this act, any money transfer scheme has to be authorised by the Indian authorities, which PayPal is not.

A spokeswoman from the RBI, Alpana Killawalla has said, they had no other option but to stop PayPal services within the country because "PayPal does not have our authorisation."

On the 6th of February, a PayPal official from the communications team; Anju Nayar wrote a blog post (https://www.thepaypalblog.com/) stating that "personal" payments, or those made from one individual to another, had been blocked to and from India. Transfers to banks in India are also being suspended.

However, Nayar made it clear that people and Indian merchants can still receive "commercial" payments for goods and services, although the real problem lies when merchants are unable to move money from PayPal into their Indian bank account.

Anju Nayar said that it might take several months to resolve issues over personal payments, as Paypal are playing it safe to respond to all enquiries from the Indian regulator before returning the Paypal services.

However, it is expected that Indian Paypal merchants will be able to withdraw their funds to Indian banks within days. (Probably by 3rd of March as "anticipated" by Paypal's Asia-Pacific boss Farhad Irani). Paypal also assured of restoring the money into the accounts of those Indian merchants who have had funds blocked in order to let them know that money is safe in their accounts. Withdrawal fees will also be refunded. As Mr. Nayar has said, the company is working closely to solve this transfer problem at the earliest, and he even apologised to clients for the sudden inconvenience that they are facing.

News sources mention that The Reserve Bank of India asked that Paypal on 27th January to immediately suspend its fund transfers to and from India as well as transfers to local banks in India. PayPal said it complied with the request and suspended its operations from 28th January. Executives from both Indian and American information technology companies say they were literally 'shocked' by the announcement.

Mr. Alok Maheshwari, founder and chief executive of Harmony Infotech, a nine-employee free-lancing web development company in the state of Andhra Pradesh said: "We used to get a check in our company name mailed to us instead, but we stopped because PayPal is very easy to use." Harmony Infotech has been relying on PayPal since 2005, and now averages about $1,500 a month in PayPal transaction payments.

The Reserve Bank has sent PayPal a list of questions, focusing on whether or not personal payments to people in India qualify as remittances, or wire transfers of cash, PayPal said. The regulators told PayPal that they had revised remittance licensing rules.

However, PayPal does not consider itself to be in the remittance business in India because accounts are online only. According to them, recipients must transfer the money to a bank account to withdraw it.

As part of the new regulations (which is to be effective from March 3rd), when requesting a withdrawal, users will need to fill out a new field entitled 'Export Code', with all the information to be given as per the current laws of India, in order to identify the nature of cross-border merchant transactions. However, this is applicable only for settlements involving exports of goods and services, as personal payments remain suspended. PayPal still needs specific government approval to allow personal-inward remittances to India.

PayPal is a popular name in many countries and their cross-border payments account for about 25 percent of the company's total $71 billion payment volume last year. PayPal does not have a domestic business in India, and all payments are made from other countries. It seems that this money-transfer company was not really aware of the latest changes in the licensing rules as stated by the RBI, and hence was unlucky enough to get stuck at the middle. Let's hope that PayPal clears all problems with the Central Bank of India and people start enjoying the benefits of online payments very soon.

World News In Brief

First UK Bank to offer New Enhancement to its Mobile Phone Banking Service

Barclays has made further enhancement to its mobile phone banking service, which will allow customers to make payments to third parties quite easily.

Barclays' latest addition to the service means that customers can now pay funds to existing or new beneficiaries that have been set up through online banking. An interface has been developed specifically for viewing over a mobile phone, making it simpler, faster and easier for customers to do their banking whilst on the move.

Barclays' customers visiting www.barclays.mobi can also view balances, mini-statements and make transfers between their accounts.

Gemalto to Secure Personal Health Records in Bulgaria

Gemalto announced that Bulgaria has started deploying its smart cards to secure access to personal health records for the country's military personnel and their family.

In Bulgaria, Gemalto delivered double-slot readers and smart cards with the associated middleware to KIM-2000, a local company specialised in eHealth projects. KIM-2000 acts as prime contractor for the electronic health record system commissioned by the Military Medical Academy. This innovative system optimises medical treatments, simplifies and modernises procedures and increases security for accessing health information.

INSIDE Contactless and Neowave to Create First NFC Smart Object

Weneo NFC, the industry's first NFC smart object will be created jointly by INSIDE Contactless and Neowave. Integrating INSIDE's third-generation MicroRead NFC solution, the multi-application Weneo NFC smart object creates a link to the Internet for NFC devices, tags and mobile phones for a variety of secure transactions.

The Neowave Weneo NFC is a standalone NFC device in the form of a USB dongle that acts as both a card reader and card emulator to support a variety of NFC applications, including mass transit and other ticketing applications, payments, loyalty, secure physical and logical access and more. When plugged into a computer's USB port, the Weneo NFC enables service operators to communicate securely over the Internet with the customer's NFC handset, contactless card, ISO memory cards NFC tags, and an internal SIM card making it ideal for online reloading applications.

Pico Computing Announced Record DES Cracking Times

Pico Computing has stated that it has achieved the highest-known benchmark speeds for 56-bit DES decryption, with reported throughput of over 280 billion keys per second achieved using a single, hardware-accelerated server.

The FPGA computing platform assembled by Pico Computing for this demonstration, based on 11 Pico EX-Series cards, reportedly consumes less than 1000 peak watts of power and fits into a single off-the-shelf 4U server.

Fingerprint-based ID Capabilities to New Mobile Devices

Sagem Wireless announced its partnership with UPEK to bring fingerprint identity capabilities to a range of new devices that Sagem Wireless is expected to launch later this year, including new Android-based mobile devices.

Sagem Wireless selected UPEK for its superior fingerprint technology, which offers industry-leading recognition accuracy, ruggedness, power efficiency and enhanced touch-input capabilities as well as its support of a standards-based, open-platform software solution.

Data Commissioner in talks over Irish ID Cards

The Data Protection Commissioner has started talks with the Department of Social and Family Affairs over the introduction of national public services identity cards.

One of the key issues of concern for the Office of the Data Protection Commissioner (ODPC) is the decision to include a photograph, a signature and a number such as the PPSN on the cards to make it considered as a de facto national ID card.

Multi-Application Smart Cards – Gaining Momentum

By Berend van Geffen, Chief Commercial Officer at Collis

Berend van Geffen

Smart Cards: Secure and Reliable

Although not (yet) a household name, the smart card has certainly become more popular in daily life since its invention in the late 60's. They underwent their first mass production in France in the 1980's as pay phone cards and since then have undergone many evolutions at both their hardware and software levels. When Europay, MasterCard and Visa (EMV) adopted the smart card to become their chosen "warrior" against card fraud in the payment world, it marked a milestone in the payment history books. One thing became certain: smart cards were here to stay.

Many years on, fraudsters are (thankfully) unable to find the smart card's "Achilles' Heel". This is due to the implementation of cryptographic algorithms such as DES, Triple-DES, RSA and SHA to provide authentication of the card to the processing terminal and the transaction processing centre. This level of cryptography combined with the use of PIN (as opposed to a plain signature), has resulted in a solid, reliable means for making card-based payments.

Gaining pole position… in your wallet

Now that the battle with fraud is coming to an end (or realistically speaking: migrating to non-EMV countries), a new battle has risen. It is a less visible one but an important battle nevertheless. It is the challenge of getting a specific issuer's card to the top of a consumer's wallet.

Let's face it; when issuers provide a customer with a new payment card, they want one thing in return; for them to use it. This may seem like such a simple and straight forward concept, but if it is undermined, it will certainly lead to problems for the issuer. Concerns such as loss of revenue or weakening of the card's brand value are a reality for issuers of cards that are found at the bottom of a wallet or even worse – in the drawer at home.

Convenience for the Customer

So how do you convince a customer to reach for a specific card and not a competitor's one? What added value can the customer receive by using one card and not the other? The answer lies in the convenience for the consumer and the perceived value a certain card possesses. Fortunately, there are numerous ways of increasing this perceived value of a smart card. One of them is by utilising the full potential of the unique physical capabilities that is already part of the smart card; the Integrated Circuit (IC) chip.

Smart cards are like miniature computers. Like computers, they too have the capability to run not just one application but multiple applications. As a result, many issuers are rethinking their strategies and are collaborating more with third parties in bringing the latest multi-application cards to the market.

Remember the days when it was necessary to carry around a separate mobile phone, digital camera, MP3 player or GPS device? Nowadays, for ultimate convenience, (if you really want to have these in possession at all times), all you have to do is slip a decent 3G mobile phone into your pocket. The same convergence of technologies and applications is occurring with smart cards. It is now possible to combine payment, transit and loyalty applications, to name a few, onto one smart card. Who wants to carry around half a dozen smart cards when one or two will do the job fine? Multi-application smart cards allow commercial synergies between partners. They also give rise to new business opportunities and push smart cards towards new domains.

Strong foundations

Many of the large payment schemes have already taken action and entered the multi-application arena in one way or the other. They are laying down strong foundations so that issuers can easily build upon them with dual or multiple applications. Take the recent launch of MasterCard® M/Chip™ Advance for example. This is a payment platform taking the traditional debit, credit and prepaid chip cards to the next level. It does this by strengthening payment functionality, assisting deployment of contactless applications and integrating information that is needed for business applications such as transit and loyalty. The result according to MasterCard is: "the potential to deliver versatile, multi-functional payment capabilities to consumers on one payment card."

Introducing multi-application smart cards into the market is not without its challenges of course. Managing multiple smart card applications is certainly more complicated than single-application smart cards as there are most likely more third parties involved. Choosing a powerful new payment platform such as MasterCard® M/Chip™ Advance is certainly a step in right direction, however it is only the beginning. Reliable testing is essential during development of these cards.

Collis Innovation

To coincide with the kind of development from MasterCard with the release of MasterCard® M/Chip™ Advance, Collis is also working in the same direction. For example we are currently working on a new product (Collis M/Chip™ 4 Release 2 Test Suite), to test the functionality specified by MasterCard. This is an enhancement of the existing Collis M/Chip™ 4 Test Suite that is been used by test labs, card vendors and card application developers. The new version will include all of the new functionality specified in the M/Chip™ 4 Release 2 Payment Enhancements and Data Storage specifications. Similar to any other Collis test tool, the test suite will be implemented with automated testing in mind; therefore, testing will be as simple as execution and following the on-screen instructions. Likewise with the release from Visa of VCPS specifications 2.1 (which has the similar aims as MasterCard® M/Chip™ Advance), Collis is also working on an updated version of our already existing Collis VCPS Test Suite. These kinds of test suites Collis offers really help issuers to speed up the card functional type approval. Their aim is to shorten the development cycle for the issuer and speed up time to market of multi-application card products.

It is not only with our test suites where Collis is leading the way. Our consultancy services help in defining and designing the business models and value chains associated with multi-application cards. This process is often quite sensitive and requires special attention, especially when it comes to questions like: Who owns the cards? Who "owns" the customer? How should key management be organised? What happens when a card is lost or stolen? What about expired cards and applications? Collis can guide the card issuer and other parties involved when it comes to these vital questions.

Ensuring Trust in new Technology

We at Collis embrace this new approach by issuers and the payment schemes moving towards multi-application cards. We understand their need to explore markets that were previously left alone. Our consultants in the fields are working not only with the banks but also with a lot of major transit authorities. We see firsthand the joining of the industries and the symbiosis relationships evolving. Symbiosis in the sense that they both benefit from each other. Look at Oyster/Barclaycard as an example. This is where the transit application (Oyster) is placed on new contactless financial payment cards issued by Barclays. As Oyster is perceived as a very positive brand and is already found near the top of millions of Londoner's wallets, it gives Barclays a unique opportunity to be that card that Londoners will also use when making a payment. The perceived value among customers and the strong loyalty they feel towards a particular card (in this case their Oyster/Barclaycard) should not be underestimated. On the other side of the coin, the transit companies (in this case Transport for London and TranSys) receive revenue from Barclays. They also reduce their costs associated with card issuing. It's a win-win situation!

So with our experts out in field among customers in banks and transit companies, we see how the trends are moving. The feedback and ideas we receive is shared internally among competence centres. As a result, the information collected has a positive impact on the products we are developing. Take Collis EMV Personalisation Validation Tool; the market leading test tool for validation of the personalisation of a smart card. Up to now it has been used by banks worldwide in

validating their payment applications on their EMV cards prior to production. Through the years, the tool has been adapted to support many EMV-compliant and proprietary (domestic) cards. Recently, our personalisation validation solution entered the Public Transportation area and is now being used for testing Mifare-based e-tickets. This means added-convenience for the card issuer who is already working with or thinking of implementing a transit application onto their cards.

As mentioned before, rolling out multi-application cards is much more complicated than single-application cards. There are more parties involved and hence new questions to be answered. For example: Who is the card operator? The bank or the transit company? Who is responsible for the applications? Assuming the card operator is the bank, at what stage is the transit application loaded onto the card? Which party is doing this? Is transit functionality handled by the payment application, or by a separate one? Whatever the answers to these questions are - which would normally be answered while developing the business case - we feel the Collis personalisation validation solution is making giant steps in the right direction. It will be one less worry for the card issuer, and one powerful weapon in the battle of getting to that privileged top spot in the end-user's wallet.

World News In Brief

UK Police Engage Print Industry to Stop Fake IDs

The U.K. police are trying to get wider participation from printer manufacturers and makers of specialist equipment in a voluntary program, designed to cut off criminals from the tools they need to make fraudulent passports and ID cards.

The program asks distributors and resellers to profile their customers and tell police if they suspect equipment such as thermal card printers being ordered under suspicious conditions, said Nick Downing, detective chief inspector with the Economic and Specialist Crime Unit of the Metropolitan police.

So far, 90 entities have agreed to abide by the police code of conduct, which includes not selling equipment if there are doubts as to how it will be used. Those 90 make up to 75 percent of the total industry. But the remaining 25 percent consists of up to 10,000 small businesses, distributors and resellers, and the goal is to get those organisations to agree to the code of conduct.

Russia to issue only Biometric Passports from 1st March

Russia will issue only biometric external passports starting from March 1, says a government resolution posted in the newspaper Rossiyskaya Gazeta. It will bring identification documents of Russian citizens in correspondence with international standards, the newspaper said.

Prior to that, Russian citizens had a choice between biometric and regular passports. But now there will be no such choices. New external passports will be issued to average citizens starting this year, while diplomats and other officers will receive new passports starting from October 1st.

NEC Facial Biometrics gets First Place

NEC Corp., a developer of new technologies including biometric and other security technology, has announced they received first place in the Still-Face Dataset of the Multiple Biometric Grand Challenge for their face recognition technology. The challenge was carried out by the National Institute of Standards and Technology, commissioned by the U.S. Department of Homeland Security and included testing of the technology in anticipated real-world scenarios such as compressed images and images taken in poor lighting.

Banks in Italy and Poland plan widespread Contactless Card Deployments in 2010

Poland and Italy have become the latest countries to take a significant drive towards contactless cards and NFC-compatible point-of-sale terminals.

In Poland, PKO Bank Polski, the country's largest debit card issuer is spearheading the move with the announcement that it will begin replacing all its 6.5 million debit cards with contactless Visa PayWave cards from mid-2010.

In Italy, Intesa Sanpaolo, Italy's largest banking group with 11 million customers has become the first bank to commit to a large-scale roll out of contactless technology.

All Change at credEcard Limited

credEcard, the fast growing e-payments and prepaid card company has announced the completion of its £2m financing round and stated its plan to re-name the company as Contis Cards Solutions and Contis Technologies Ltd. This is in consequence of the fulfilment of its desire to make a change from a B2C company to a pure B2B enterprise.

Atmel Announce Sale of Smart Card Business

By Tom Tainton, Smartcard & Identity News

Tom Tainton

California based microcontroller vendor Atmel Corp has revealed that its smart card business located in France and the UK is up for sale, but has confirmed that it intends to discontinue any plans to sell its other branches within its ASIC sector. Atmel's ASIC (application-specific integrated circuit) business provides high performance security solutions to industrial, aerospace and consumer markets operating in three areas: smart cards, customer specific products and commercial aerospace. The announcement marks a turbulent period for the company which has seen disappointing financial results and rumblings of strike action among its French employees.

Atmel insist that it has been pursuing strategic alternatives for the ASIC business as part of its 'transformation plan' which is aimed at focusing attention and resources at the vendor's high-growth and high-margin projects, while washing their hands of the less successful businesses at the same time. Atmel's smart card sector operations include the development of computer chips for items such as cable set-top boxes to control access to TV channels, and a chip wafer fabrication plant. The proposed sale leaves workers at plants in Rousset, France and East Kilbride, Scotland facing an uncertain future.

An official statement from Steven Laub, Atmel president and CEO, suggested that the company were already in the process of discussing the potential sale with interested parties. "We are pleased with the progress we are making with the strategic alternatives process for the ASIC business and related manufacturing assets. We are continuing to discuss the potential sale of the SMS business segment with interested parties. As part of our review, we have also determined that shareholders' interests are best served by Atmel retaining the CSP and aerospace business segments".

In the light of last year's financial results, it seems that sustaining the smart card business was not a viable option for Laub and his senior executives. Atmel reported a fourth-quarter net loss of nearly $77m in 2009, as sales dropped to $1.22bn for the year compared to $1.57bn in 2008. Stephen Cumming, Vice-President of Finance blamed the 'lower utilisation and production levels' at Atmel's Rousset facility. In addition, gross profit failed to meet the group's target range of 32-35% of revenue, representing 31.1%. And with the recession no longer considered a valid excuse, Atmel have taken swift action. Already the company has made arrangements to sell its French water fabrication business to Germany's LFoundry GmbH. Announced in December; Amtel officials say the deal is still on track and pending approval from employee representatives in Rousset.

This may prove to be a stumbling block, however. Angry workers in Rousset are in the midst of an unlimited strike, protesting against Atmel's decision to sell the site without guaranteeing that jobs will be maintained. The company has failed to confirm that a plan signed last spring which ensured worker's protection after the sale would still be implemented. The signed agreement promised that workers would be redeployed, or compensated if a buyer fails.

Secure Elements

By Peter Tomlinson - Smartcard & Identity News

Pe*ter Tomlinson*

Ever heard the term 'secure element' before this year? The focus now is not on smart cards, or smart media, or even on NFC stick-ons, but on the logic mega-cell design that can become a smart card, or a smart keyfob, or be one part of a bigger chip such as the latest mobile phone SIM, even be embedded in a Whizzo dongle... The message that has been hinted at during the last couple of months is that we are nearly there with commercial launches of more feature-rich SIMs, and thus close to the next generation of mobile phones and of exotic dongles. The aim is to ramp up availability of secure mobile transaction technology, using both the network and short distance NFC. Now one company is first out of the stalls – in mid February Gemplus announced the incorporation of a secure element into a SIM: "This innovation will enable commuters to use their NFC (Near Field Communication) mobile phone as an e-ticket, as simply as any other contactless travelcard. A high level of security is ensured, as the tickets are stored in the SIM card and the application meets the stringent security requirements of the DESFire specifications."

That illustrates that offering the user something seductively simple and easy to use, and also secure, reliable and low cost, is the way to go. Gemplus have taken the secure mega-cell and mated it with DESFire, which is NXP's secure filestore on a chip; they have included the AES crypto function that the current DESFire product family uses. They have shoehorned the extra function set into a SIM alongside all those other functions that, with parallel upgrades to the technology in the body of the mobile device, make it all happen. They benefited from advances in semiconductor technology, particularly in reducing power consumption and getting manufacturing costs down. But it has been a long route to get here, 65 years in fact, with a mix of hard grind and small but significant leaps forward, starting with Alan Turing's concept of the stored program computer – your reporter has participated in some of the steps in that long march, for example in the introduction of the single button reset and boot that is now on all of your PCs but started life as an innovation in late 1960s mainframes. Much later (alongside Dr Everett when the Mondex concept was emerging) he was involved in the definition of the smart card's crypto co-processor. But here there is no claim to absolute originality, because these steps forward tend to emerge simultaneously in several places, and so we know that the two major European secure element core chip suppliers, NXP and Infineon, are marching along in parallel.

Yet it was only 3 years ago that it seemed that innovation in smart cards had reached a plateau above which it might not climb. In November 2007, CardTechnology magazine, based in New York and long a reliable reporter of new developments, closed down. Its last cover page proclaimed The Industry's New Look:

"A new reality has settled over the smart card industry: It's survival of the fittest, and card vendors have stepped up their cost-cutting measures in a drive to return to profitability."

Of course in 2007 the USA had not decided to move to Chip & PIN, and their PIV market (Personal Identity Verification for public sector employees) had not really got moving. Nor had the UK completed Chip & PIN rollout, and in ticketing, the other UK market with potential high volume, only a very few isolated ITSO compliant schemes were under way, primarily using 1st generation Mifare Classic®. Smart ticketing was mainly being used in small scale, closed schemes, such as for football clubs. NFC from Philips/NXP and collaborators seemed like a technology for handshaking with smart posters (for the benefit of the marketeers, of course). But low power secure chips were creeping into passports, and already most of the big chip companies were feeding the far east markets, with the Europeans setting up manufacturing out there. Hackers were beginning to get to grips with Mifare Classic® and even with the dominant symmetric crypto method DES, yet the cost of using better methods in these volume markets were seen to be prohibitive. Despite that, the big industry players carried on with development of better products and processes, right through the credit crunch.

Secure elements are not all of the story, for the rest of the supply chain has been working away on many fronts during the recent recession. Gemplus is first out, showing their mobile market innovation, while others take their own routes to different affordable products. Now the equipment and solution providers are busy, but not always quite as bullish as the chip people and their immediate customers. It is not simply a matter of plucking the low-hanging fruit from the chip makers' trees in order to provide attractive products for the end user markets that need security and low cost – those markets are building access, e-ticketing, and payment, using high volumes of smart media to keep in your pocket or otherwise hanging around your body, and in part wanting to move to mobile network solutions. Be careful – there are hints that sometimes the fruit is not yet

ripe, that sample chips are not yet available.

We know that NXP has also defined Mifare Plus, an even lower cost product than DESFire, and available with AES crypto; we know that a consortium including Infineon and INSIDE has a parallel offering – but there are few terminals to work with AES, ITSO's SAM doesn't implement AES arithmetic in its processor chip hardware, there is much applications software work to do, and there is the worry that many of the new chip products are actually or effectively single source – even where third party manufacturing licenses have already been issued, that doesn't guarantee anything. It could be that we are at least 18 months away from being regular users of the consequential new generation of secure, usable and cost effective services, longer where existing schemes have to be upgraded, but we may very soon be offered more ways of accessing existing services.

[1] *The USA endorsed symmetric crypto that is the next step on from DES*

World News In Brief

Police Investigating on Serious Debit Card Frauds

Windsor Police are investigating a large number of debit card fraud complaints which occurred over the weekend. The WPS Financial Crimes Unit received numerous calls from people who advised that their debit card had been compromised and money had been removed fraudulently from their bank accounts. The investigation has revealed that the actual withdrawals from the complainants' accounts were made from Automatic Teller Machines (ATMs) located in the province of Quebec, Canada.

Information has been received that organised crime cells within Quebec are travelling the highway 401 corridor and tampering with the Point of Sale PIN Pads enabling them to obtain the banking information of unsuspecting customers. Windsor Police have made several arrests within the city during the past year of suspects who have tampered with these PIN pads.

Sagem Orga introduces World's First NFC Java Card Sticker

One of the leading smart card manufacturers, Sagem Orga (Safran group), launched "SIMply Mobile Wallet", the world's first Near Field Communication (NFC) Sticker with phone connectivity and integrating a Java Card secure element chip. Sagem Orga developed the solution in cooperation with Twinlinx, a company focused on the development of innovative technologies designed to accelerate the growth of NFC applications and markets.

Iris Technology to Drive Global Biometric Market in 2010-2012

The Iris recognition technology market is forecasted to grow at a CAGR of around 30% during the 2010-2012 to reach around US$ 900 million by 2012 end, says a new RNCOS, an industry research firm report. With the identity management market growing rapidly, biometric identifiers are recognised and accepted as integral components of identification process in the public and private sectors.

The new research report "Global Biometric Forecast to 2012" has found that the global biometric market will grow at a CAGR of around 18% during 2010-2012 owing to the rising usage of key biometric technologies like hand geometry, iris technology and finger recognition by governments worldwide. RNCOS has further found out that iris recognition will primarily be used in applications that require high levels of security though convenience-driven deployments will continue.

Ex-Army Man Cracks Popular Security Chip

Hardware hacker Christopher Tarnovsky just wanted to break Microsoft's grip on peripherals for its Xbox 360 game console. In the process, he cracked one of the most heavily fortified chips ever put into a consumer device.

The attack by the former US Army computer-security specialist is notable because it goes where no hacker has gone before - into the widely used Infineon SLE 66PE, a microcontroller that carries the TPM, or Trusted Platform Module designation of security. The hack means he can access sensitive data and algorithms locked away in the chip's digital vault and even make counterfeit clones that could fool the many devices that rely on it.

Hybrid Card for Financial Control

Tsys (provider of outsourced payment services, and offering issuer and acquirer-processing technologies) has unveiled a new payment card that allows consumers to choose how they want to pay. The patent-pending Tsys Hybrid card combines credit and checking payment functionality on a single card, creating an easy-to-manage payment solution that gives customers financial control.

Customers can set preferences for posting transactions to their various accounts using their web browser. Transactions will be conducted to allow customers to carry credit balances or 'pay now' from their deposit or other accounts depending on what works best for them.

Mobile Payments
– *it takes more than two to tango*

By Jan De Meester, Integri

Jan De Meester

With a worldwide market penetration of more than 50% and tens of countries exceeding 100%, the mobile phone is literally everywhere. And as mobile devices are getting smarter and prices of mobile connectivity continue to fall, consumers increasingly rely on mobile phones to surf the internet, keep in touch via social media, share information and stay organized…on-the-go. Moreover, according to a recent study, 59% of consumers are interested in using their phone to pay at the cash registers just as they would do with their debit or credit card. (Source: StrategyOne, 2009). The story has been told maybe too many times: technology is ready to offer consumers a fast and rich payment experience with added value applications such as e-Vouchers, Loyalty, e-Money Transfers, and more. However, despite technology being ready and after several successful pilots around the world, the expected mass roll-out has yet to happen.

Looking at the mobile service markets today, it is a very fragmented market with a multitude of players and not fully compatible technology standards. Whilst it is widely accepted that some form of a collaborative model makes the most sense for the industry, the convergence of the mobile and payment space proves extremely complex, requiring the co-operation of many players, in particular financial institutions such as banks and mobile network operators. It is this complexity that is one of the main hindrances for an extensive roll-out of secure mobile services.

Welcome to the new connected world

New technologies have the potential to create new trends and transform user habits. For example, the spread of affordable mobile phones has connected people via speech and SMS technology, and now the advent of smarter phones and high-speed connectivity leads to richer forms of communication. Similar to the internet that grew from a "static" database to a dynamic application-loaded platform that connects the world, the mobile phone is going through a similar evolution. It is morphing to an essential, personal device for purchasing goods, sharing files, browsing the web, e-mailing, with even the capability of replacing a PC. And with Near Field Communication (NFC), it seems we have the ability to convert the phone into a wave & pay device.

The connection of the mobile ecosystem with the existing micro payment ecosystems like cards, ticketing, loyalty, couponing and the internet (social media) is inevitable. Obviously, the mobile phone has the power to replace our physical wallets and thus enable us to go without cash, visit ATM machines or perform wire transfers: financial and retail transactions at the touch of the fingertip. But then why have mobile payments and commerce failed to materialize?

The fragmented mobile omniverse

Offering mobile services necessitates the cooperation of multiple parties from different market sectors, each with very different motivations and challenges: SIM manufacturers, handset vendors, mobile operators, financial institutions, processors, payment schemes, merchants, transport operators and there's more. The market is fragmented across many stakeholders. Let's break down the mobile end-to-end omniverse into the major parts to fully understand the complexity:

- End-user credentials: phones, cards, paper vouchers, USB tokens
- Channels: payment terminals, cash registers, phones
- Channel and credential management services: control mechanisms for devices, channels and users
- Application services: a wide array of commercial services

- Payment methods: bank accounts, credit cards, phones, e-money, vouchers
- Processor gateways: facilitates the moving of money via banking/payment systems
- Security services: authentication, transaction non-repudiation
- Fraud management: activity monitoring, dispute handling (chargebacks)
- Trusted third parties
- Regulators

Connecting all these components is a complex exercise and one can often not see the wood from the trees. Understandably, many mobile projects only solve part of the equation and confusion between mobile banking and mobile payments is rife.

The successful pilot ambiguity

The complex and diversified market and the wide array of players have contributed to the slow uptake of mobile payment services. Today the industry is using many different technologies for front end systems, communication protocols, payment processing and so on, which has restricted any natural cooperation between the several partners and resulted in an opportunistic approach covering only parts of the end-to-end process.

Today, there are mobile commerce pilot schemes in abundance, of which some have been quite successful. But when exactly is a test project a success? Let's have a closer look. Such pilots are limited in scope and capabilities, and focus primarily on the more visible end-user device as a driver of the service. Given the small scale of these trial schemes, they are limited to small numbers of users with proprietary handsets operating over a single network connecting to a single bank. Evidently, customers will only replace cash with a mobile equivalent if they can use it with any NFC-enabled phone at any mobile payment accepting Point-Of-Sale, regardless the bank or mobile operator. Furthermore, a bank would want to offer its service to all its account holders, independent of their operator and vice versa. As explained above, connecting the different building blocks and players of the payment value chain is a complex yet essential task.

Moreover, most pilots are technology centric with limited use cases. Instead of leveraging on the existing payment infrastructure they customarily make use of proprietary equipment requiring substitution of existing components such as for example payment terminals. Operators and banks are also often in conflict over access to the customer and see each other as a threat to their desire of becoming more entangled with the customer. Both fear that the other might intervene in the relation of "their" customer. And how is the revenue split across all parties? Anyone owning financial liability, assessing the risks, taking care of security aspects or safeguarding privacy? The business case in many instances is simply not there. Last but not least, pilots mainly test payment solutions, while there's so much more to be explored: coupons, smart posters, vouchers, loyalty points, e-money transfers from person to person and more.

Collaboration is the key to success

It is not very likely that a single bank or operator business model is to break out from the pilot phase and propose a viable e-Wallet solution. We are convinced that a business model with the most potential for commercial success involves collaboration between banks, operators and the many different stakeholders. A first step in putting the pieces of the puzzle together is establishing partnership or collaborations with companies that have complementary specialized knowledge so to create a value added solution and linking the necessary bits and pieces.

The vision of the e-Wallet is to combine everything we ever need on a single smart phone, simply because this is a logical evolution. However, it is the customer that will decide if it really takes off one day. Besides that it is way cooler to pay for a newspaper or sandwich with the newest iPhone, there should be more in it for the end-user to make the switch from the comfort of cash and the convenience of cards.
Let us look at the following example. Clear2Pay recently signed a partnership with Alcatel-Lucent to create a mobile micro payment framework that combines the respective companies' long time payment knowledge with mobile network experience. It's exactly this complementariness that allows synchronizing the involved parties with the underlying payment mechanisms. The framework is an open, end-to-end solution that

integrates seamlessly with existing payment infrastructures, e-shops and applications. It features the essential payment gateway enabling to settle and redirect payments.

The framework is in fact a stored value account solution which steps away from the traditional account that simply adds and subtracts numbers but allows creation of value by its ability to store coupons, vouchers and loyalty points. Through this co-operative effort, Clear2Pay and touchatag have created an e-Wallet solution that allows consumers and merchants to enjoy mobile point-of-sale transactions on top of added-value services such as the collection and redemption of loyalty points, issuance of gift cards, delivery of electronic store receipts, interactive advertising and promotions as well as person to person e-money transfers. Users also gain the benefit of checking transactions and balances in real time on their mobile phone and manage many relationships with merchants, banks, and day-to-day applications without adding single use cards to their physical wallet.

In these challenging times, the market is looking for profitable and secure mobile solutions which have true business potential. With the likely commercial deployment of NFC from 2011/2012 onwards, ubiquitous smart phones and a wealth of value-added applications, the front-end application of the mobile ecosystem is ready to go. It's the industry's task to choose the right partnership and succeed in connecting the different components of the value chain to make the e-Wallet the natural next step for a convergence of industries. But anyway, regardless of technology and how all stakeholders work together, the success of the m-commerce will largely be influenced by whether the e-Wallet fits within the consumer's lifestyle.