September/October 2011

Volume 20 • Number 9/10

Smart Card & Identity News

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

www.smartcard.co.uk

Another one bites the dust (Mifare DESFire)!

I'm not sure it's a big surprise but this month David Oswald and Christof Paar from the Horst Gortz Institute for IT Security in Bochum Germany have given a paper at the CHES (Cryptographic Hardware and Embedded Systems) conference in Japan on how to break the Mifare DESFire MF31CD40 contactless memory chip.

So back to basics, do we need to panic, is it important and will there be further repercussions? Really it's no to all these questions but don't go away yet because that would belittle the quality of their work.

They used Side Channel Analysis (SCA) by using an electromagnetic probe to contactlessly measure the power signal taken by the chip. Using these techniques they were able to recover the 2 DES keys (56 bits each) from the chip under test.

After fairly extensive test set up work over several months they were able to show that they could recover the keys in a matter of a few hours using Correlation Power Attacks (CPA) with equipment costing about $3000.

Continued on page 4….

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

Head Office: Smart Card Group,
12 Meadway, Rustington,
BN16 2DD

Telephone: +44 (0) 1903 734677

Website: www.smartcard.co.uk

Email: info@smartcard.co.uk

Editorial

Technical Researcher –
Dr David Everett

Production Team - John Owen,
Lesley Dann, Adam Noyce

Contributors to this Issue –
Dr David Everett, Mary Carol Harris,
Andy Kemshall, Marie Costers,
Ayman S. Ashour

Photographic Images -
Dreamstime.com

Printers – Hastings Printing Company
Limited, UK

ISSN – 1755-1021

Disclaimer

Our Comments

Patsy Everett

Dear Subscribers,

It's that time of the year again when one's mind starts to think of Paris, the Cartes exhibition and mobile wallets (you'll see later why I've dropped that in). You would also be completely forgiven if your memory banks also contained less fond memories of the RER strikes which seemed to have some unbelievable synchronisation with the timing of the conference.

However all looks well for this year's event and it's a great opportunity to meet up with friends from the past and also to make new acquaintances. It's amazing how things have changed over the years and yes I can still remember many years of the troll to La Defense in the earlier days of the conference. Of course in those days it was much easier to stay in the centre of Paris but I think most people still do the same thing today, hoping that the RER is not going to spoil the fun.

Any industry has its battleground and the world of smart cards is no different. Thinking back over the years one can still remember the early days when every year we forecast that next year it would happen and let's be honest it was GSM that turned the party round. The banks had been talking about smart cards a lot longer but struggled with the business case which was and probably still is founded only on security. In the 80's and early 90's a lot of people weren't convinced you needed anything more than a magnetic stripe card and signature, even the introduction of a PIN at the Point of Sale was hotly disputed. And lest we forget in the USA we are only just starting to see the introduction of EMV or Chip & PIN as we know it. It seems unbelievable but I still remember the technical committee of the European banks recommending the introduction of smart cards at the end of the 80s. It took 10 years to get going in Europe (except France where through Cartes Bancaire the banks became smart card pioneers) and 20 years for the USA.

Of course dear readers it will not have escaped your attention of the gold rush taking place in the USA, just about every company, consultant, what have you, have their bags packed to help the banks and merchants get into the world of EMV.

So here's my first prediction for this year in Paris, expect to find lots of people from the USA and a sudden bias to exhibition stalls promoting expertise in EMV.

It's funny really, all the noise we used to hear about smart cards and why you didn't need them and why the consumer wouldn't want them and yet in Europe at least they dominate and from a consumers point of view much preferred to the magnetic stripe. How many of you have got to your hotel room on the 30th floor to discover the magnetic room card has been corrupted (the magnetic sleeve on the Blackberry is often a cause) and you have to go all the way back to reception and queue again. Well we Brits tend to queue although I've noticed this is not a global attribute.

No such problems with the chip card, their reliability even in the washing machine is really quite outstanding.

Anyway back to the battleground which has now moved into the world of the Mobile wallet. The initial battle was all about NFC. I'll bet you have forgotten that the ISO 14443 standard for contactless cards didn't include Phillips Mifare or the Sony Felica. So Sony and Phillips got together to create a new standard that would include their products and they called it NFC for Near Field Communications which means magnetic coupling according to David E who I'm sure would be happy to give you the much longer version. Anyway the interesting thing is that INSIDE Contactless (as they were then) really got there first with their R2R technology where they had the vision of short range communications between mobile devices and also with contactless cards. Anyway that's all over now and we have NFC and its ISO standard (I never could remember the ISO number).

However the proponents of NFC for years, maybe 10, have pushed mobile payments as the driving factor which as we all now know never proved to be the case. At last it has been accepted that payments are not the driving factor but it may be something you need to support the main application. The general thinking here is that it is likely to be some form of integration between social networking and location.

However the battle doesn't stop here because everybody is after getting payments into the mobile phone ready to support whatever it is that we can't yet predict but is likely to suddenly evolve.

Now we get to the problem, modern payment applications use cryptographic security, passing unprotected credit card numbers and security codes over the internet is not the way to go. So if you have cryptography with secret keys how do you protect it in the phone. Well you put it in a secure element (in the nomenclature of GSMA and the NFC world). Yes, you've got it, where is this secure element? Is it the SIM card, some embedded chip in the phone or a removable device like a MicroSD card?

The battle is in full fling, the mobile network operators want the secure element to be the SIM card, the phone manufacturers want it to be an embedded chip and the payment organisations would like it to be their chip such as a MicroSD card. The noise you will hear is the mobile wallet but what it comes down to is where you put this secure memory and processing environment. Much talk has surrounded the Google wallet but you should be aware this is based on the concept of a Google secure element in the phone and to do that they got Samsung to make the Nexus S, there is no other phone with a Google wallet or secure element depending on your thinking.

So I look forward to meeting you all in Paris and let's continue the discussion.
Patsy.

P.S. Our sincere apologies but we slipped on the September issue of the newsletter due to our office move but we will catch up with some special reports on payments and the issues discussed in my letter to be circulated as part of your subscription.

Contents

Regular Features

Industry Articles

Events Diary

November 2011

01-03 Banking Meets Mobile Convention, Istanbul - www.cardist.com.tr/en
02-03 NFC Payments, Miami, USA - www.nfcinsight.com
02-03 Travel 2020, The Kia Oval, London - www.landor.co.uk/travel2020
02-04 ID World International Congress, Milan, Italy - www.idworldonline.com
10-11 Payment Innovation Summit, China - www.cdmc.org.cn/2011/payment
15-17 CARTES & Identification, France - www.cartes.com

December 2011

7-9 Asia High Security Printing Conference, Delhi, India - www.crossconferences.com/asia/

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

…. Continued from page 1

The main work overhead was collecting the necessary 250,000 traces for analysis.

The details of their analysis is freely available on the net as 'Breaking Mifare DESFire MF31CD40: Power Analysis and Templates in the Real World'.

The authors took a reasonable approach in warning NXP back in April that they were going to release their findings at the CHES conference. Perhaps even more impressive and I have criticised NXP in the past for the way they have handled such problems is the letter they put out to their customers at the time of the CHES conference. It was really quite matter of fact, no cover up and a reasonable statement of what NXP are doing about it and what the practical consequences are likely to be. The short answer is that they will discontinue the MF31CD40 chip at the end of this year migrating customers onto the Mifare DESFire EV1 which they introduced in 2008 as we reported at the time of the initial attacks on the Mifare Classic in volume 17, Number 1, January 2008 of smartcard news.

So now we get down to the discrepancy between the German researchers and NXP. The researchers claim that their attack poses a severe threat to many real world applications that employ the broken chip. NXP by comparison play this down, pointing out that it is unlikely that the technical community is suddenly going to spend their time breaking commercial systems for which the main application is mass transit cards.
But more important as they point out is that in most cases the system providers will have other security features in their system and will not be just dependant on the chip. It doesn't really need to be said but they also assume that the system providers will not be using global keys, i.e. the same key in every card.

There is also a little note in the NXP letter that they are not aware of banking data being held on the DESFire cards. Perhaps not but I would comment that if these cards are used for stored value then there is possibly a bigger concern.

To support their case Oswald and Paar cite the Czech railway in-karta, the Australian myki card and the Clippercard in San Francisco.

We understand that Victoria's Transport Ticketing Authority (TTA) has started a migration plan to upgrade more than 1.1 million myki transport smartcards for the state's trains, trams and buses which were originally issued in 2009 and worth $8.1 million to Mifare DESFire EV1 version of the technology, which should be resistant to such side channel attacks.

The researchers in their paper also quote that during their research they came across a number of mobile payments based on this Mifare DESFire chip, I think I would be surprised to find a payment system of any significance based on this chip which is after all just a memory chip and that's not the way you do payments.

By Dr David Everett

NFC and the smartphone: a look to the future

By Mary Carol Harris, Head of Mobile at Visa Europe

Carol Harris

Think about the way that consumer computing devices such as smartphones have evolved in the past few years. Now think how much more they are likely to evolve. The acceleration of these technologies, as well as the changes they enable in consumer behaviour and the way we pay, is both exciting and inspiring.

2011 has seen major growth in Near Field Communication (NFC) technology, with particular acceleration in the world of payments.

Contactless payment technology, which offers consumers fast and convenient methods for low cost purchases, has seen several major retailer rollouts throughout the year. By the end of 2011, 20 million Visa contactless cards will in circulation in the UK, a growth of almost 7 million since March this year, with more contactless payment points added to an already extensive list on an almost daily basis.

Our recent 'Contactless Barometer', a quarterly benchmark looking at consumer attitudes to new payment methods, found that contactless payment technology is rapidly gaining momentum with consumers. Of those questioned, 90 per cent thought contactless payments make life simpler and 85 per cent of contactless users would recommend the technology to their friends and family. This self-perpetuating cycle is crucial because an increase in contactless users means more retail outlets adopting the technology, and more retail outlets adopting the technology stimulates further user uptake.

Building on these major strides in contactless use and acceptance, 2012 is set to be the year of mobile payment technology, bringing NFC and the contactless infrastructure together with the new, high-performance smartphones. Momentum is already building, with Visa joining other payment companies to support Google's flagship NFC service, the Google Wallet, now available in the USA. Other members of the mobile payment ecosystem are also making significant progress with their mobile payment strategies. For example, following Samsung's first foray into mobile NFC with the Samsung Tocco, and the joint project between Samsung, Visa, Telefonica and La Caixa in Sitges, next year will see the electronics giant releasing the official Olympics and Paralympics Mobile NFC handset, also in collaboration with Visa.

The evolution of smart devices

As a concept, the smartphone has been with us since the early 1990s. Mainstream acceptance took a firm hold in the late 2000s with the launch of the Apple iPhone and the emergence of true mobile broadband. The response from other players across the mobile ecosystem – perhaps most notably from global players like Google, Microsoft and RIM – has added fuel to the fire, creating a plethora of smartphone choice to match the whirlwind of consumer demand. By the final quarter of 2010, smartphones were selling globally at a rate of more than a million a day, up 94 per cent on the fourth quarter of 2009 and equating to almost a quarter of all mobile handset sales worldwide.

The near-ubiquity of high speed connectivity has been hugely instrumental in determining the way in which these devices can be used, dramatically boosting their popularity. Through a combination of WiFi and 3G mobile broadband, smartphones can be constantly and universally interconnected. Within three to five years, we are set to see the progressive emergence of yet more capable wireless network technologies, combined with a whole new level of inbuilt network intelligence such as location and context capabilities; setting the scene for a whole new range of services that work with smart and connected devices.

Redefining the device: the impact of NFC

At the forefront of all these developments is NFC. Already available in some high-end devices such as the Samsung Galaxy SII and some flagship devices from RIM, NFC is set to be bundled in with future iterations of many of the major operating systems. It will reside alongside many other types of functionality and will offer masses of opportunities for the entire payments ecosystem. But to understand the full potential of these smarter, NFC-enabled devices, we need to look beyond today's vision of the smartphone.

We are already surrounded by sensors, displays and actuators, all seamlessly integrated into our environment and the objects we use on a daily basis and linked together through a digital network. In tomorrow's smart environment, any object with a digital heartbeat could be networked, communicating with other devices and enabling a multitude of functions. Components of this future are smart homes and appliances, integrated with smart power grids; smart transport networks, integrated with intelligent cars and road systems; and, of course, security and access control. This future will provide boundless opportunities for payments, often triggered automatically and underpinned by NFC; for example, paying a motorway toll or entering a central business district (already a reality in some countries), or even paying for your next supermarket delivery from a digital window on the front of your fridge.

The future is now

The new generation of devices is already fuelling big changes in the way people behave. The worlds of payment and mobile are well along the path to convergence.

Demand from consumers is high, and the rate at which devices are being brought into the market suggests that we will not be faced with a long tail of legacy phones with limited capability. Consumer behaviour is beginning to shift: contactless technology, as well as providing the infrastructure for future NFC implementations, can also drive the habit to part from cash payments and move to a new form of spending, readying consumers for NFC-integrated smartphones.

The mobile device, in all of its different guises, seems certain to evolve into a mass market payment and acceptance mechanism. Embedded with secure payment details, NFC-enabled devices will initiate and authenticate over-the-air digital payments, and give a two-way link between consumers and their financial services provider. And consumers will expect to use these new payment channels as fully as they do today either online or in the real world.

The new Point of Sale

Device evolution will also have some interesting implications for the acceptance infrastructure. Smartphones will soon have many of the attributes of an existing acceptance device; maintaining constant, ubiquitous contact with the acquiring host, they can be securely interrogated and validated and as a result, will be able to play the role of an acceptance device.

This kind of model could be ideal for smaller merchants, and particularly mobile merchants. Similarly, they could be appropriate to the type of tradesmen who currently resort to cash and cheques. And, for the payment providers, they become an opportunity to reduce the costs and the burden of device management. In the future, we could we see new and innovative ways to enhance the point of sale (POS) experience for consumers, making payment flow better.

The integration of NFC and the smartphone

Smartphones and NFC may have developed separately but their futures are clearly intertwined. Both the payments and mobile industries are innovating at an impressive rate and most crucially, are visibly delivering on the promise of high contactless availability and smartphone variety.

Today's momentum is sure to herald an exciting start to 2012, and will ultimately lead us to unlock new services that will offer consumers even more innovative, convenient and flexible ways to pay and to manage their money in the way that best suits their lifestyles.

World News In Brief

Mobile Wallet from Google

Google Wallet to all Nexus S 4G customers is an app that enables consumers to transform their phones into their wallets and make purchases with a simple tap. Sprint is the first carrier and Nexus S 4G is the first phone in the United States to deliver this.

Google Wallet has been designed for an open commerce ecosystem. It will eventually hold many if not all of the cards you keep in your leather wallet today. And because Google Wallet is a mobile app, it will be able to do more than a regular wallet ever could, like storing thousands of payment cards and Google Offers but without the bulk. Google Wallet will eventually store your loyalty cards, gift cards, receipts, boarding passes, tickets; even your keys will be synced to your Google Wallet. And every offer and loyalty point will be redeemed automatically with a single tap via NFC.

Google Wallet supports Citi MasterCard credit cards and the Google Prepaid MasterCard, powered by First Data. Google plans to support additional cards. Google Wallet is designed to enable safe, secure payments. It requires users to set up a Google Wallet PIN that must be entered before making a purchase to prevent unauthorised access and payments. The Merchant must support MasterCard PayPass to take Google wallet payments.

"Shipping Google Wallet to Sprint is a crucial first step in creating a new way for people to use their phones to make shopping faster and easier," said Osama Bedier, vice president of Payments at Google. "The world is on the brink of the next big shift in payments, and today's announcement demonstrates that we're making real progress in attaining the vision we share with our partners for a new and innovative mobile payments platform. We believe this is just the beginning of a transformation that's soon to come."

Biometric Services for New Zealand Post

The New Zealand Post has begun offering its citizens passport and digital photo's incorporating software from Biometrics developer Daon that will include facial recognition, fingerprint scans and voice samples within the data.

The system, according to a Stuff.co.nz article is being trialled in 14 of the 280 Postshops across the country.

Apparently the real reason behind this trial is to eventually roll out a national ID program which will be an optional way for citizens to authenticate their identity for access to Government services online.

Regulators Uneasy about Virtual Currency?

Microsoft has been watching the electronics payments space for some time, originally micropayments and now virtual currency such as Microsoft points which are used by 30 million online gamers on Xbox LIVE to buy their virtual goodies. You actually buy this virtual currency with real currency using PayPal or a credit card.

In its latest moves Microsoft is lobbying the Reserve Bank of Australia in their review of innovation in the payments system. Microsoft cites virtual currencies such as Facebook Credits and Microsoft Points as strategic tools for value exchange even between the various schemes,

Virtual currencies are however causing the regulators problems, mPesa may be more money transmission than a virtual currency but although very successful in Kenya the regulators in other countries such as India have banned it outright.

The Chinese authorities, for instance, have moved to ban the use of virtual currency in the trade of real goods and services in a bid to limit its possible impact on the financial system while the French courts are being asked to define the status of the virtual currency Bitcoin, after local banks switched off accounts for exchanges handling the currency on the presumption that Bitcoin should conform to electronic money regulations.

The dummies answer to authentication – an anecdote to phone hacking

By Andy Kemshall - SecurEnvoy.

Andy Kemshall

Which is more secure - hardware or software authentication and which should you choose to prevent becoming the next victim of a breach?

The recent events involving the mobile phone hacking actions of News of the World journalists - and quite possibly many others - have highlighted the fact that there are insecurities in the world of mobile telephony.

And with approaching five billion mobiles in circulation - almost at the level of one handset for every person over the age of 10, it is perhaps inevitable that some elements of the services available may be found wanting when it comes to certain aspects of security.

Against this backdrop, much has been made of the fact that cellular phones operate across open radio channels that - with the right equipment in place - they can be subverted.

But this isn't actually true. Most of the hacks of mobiles in recent years - have involved the subversion of the cellular base station, rather than the handset.

As Karsten Nohl and his colleagues demonstrated at the December 2010 Chaos Computer Club meeting in Germany (http://bit.ly/f4TNVH), it is now perfectly possible to subvert the 2G GSM cellular network - using a massive hash of the A5/1 crytpo tables - to eavesdrop on calls.

But it is also important to note that the A5/1 encryption system dates back to the 1980s when GSM was being developed. Since then the GSM standard has been developed extensively and, over the last eight years, we have seen the rise of the smartphone and the 3G standard.

3G, as any radio communications engineer will attest, does not use discrete radio channels with packet-driven data, but uses a radio scattering system known as spread spectrum.

Spread spectrum involves the use of radio signals spread across multiple frequencies which utilise almost all of the available bandwidth in a given waveband.

It's also interesting to note that the technology was originally developed to prevent eavesdropping. As a result, 3G voice and data calls (it's actually all data) are almost impossible to monitor using today's computing architecture.

On top of this, 3G data streams are encrypted using the A5/3 encryption system, which is several steps ahead of the A5/1 system that Nohl and his research team have cracked. As an encryption system, A5/3 is based on a stronger algorithm with larger keys that to date have never been hacked.
It's also worth noting that as soon as the A5/1 flaw was discovered, a security patch fix came out almost immediately.

So where does this leave the security of text messaging?

At the RSA Europe conference in October last year, a US researcher called Zane Lackey - showed how, by subverting the data headers of SMS and MMS transmissions on cellular networks, all manner of social engineering-driven hacks are possible.

According to Lackey, because an MMS is actually a mobile Internet `call' routine built into an SMS data string, it is possible to fool a user's phone into polling a third-party (hacker's) server for the MMS payload content, rather than the mobile phone company's systems.

What Lackey's demonstration at RSA Europe 2010 - later repeated at the Black Hat Abu Dhabi event in November (http://bit.ly/bvekPW) - showed was how it is possible to generate a WBXMA-based message that

appears on a user's mobile and persuades them to access a rogue mobile Internet web site.

It did not, however, demonstrate how fake text messages could be inserted into a live GSM control channel, nor how an SMS data stream could be eavesdropped upon as, whilst this would be technically feasible, it would involve the use of complex electronics and - given the nature of cellular networks - would only operate across a short range.

SMS tokens versus hardware tokens

Thus leads us neatly to the topic of whether an SMS-based token - often described as a tokenless two-factor-authentication (2FA) system - is as `strong' as a hardware-based token such as the RSA SecurID system.

Before we examine this issue, let's look at the security of a 2FA hardware token.

Whilst the hardware itself is tamperproof, given the fact that RSA's servers were publicly hacked earlier this year (http://bit.ly/i3NEKa) the integrity of the system is far from being unhackable.

Furthermore, if the token is `borrowed' by a third party, and the electronics dissected - a process which has been carried out by countless researchers since the arrival of the 2FA hardware token (aka one-time password tokens) in the late 1980s - then it is possible to create a duplicate hardware token using the same algorithm.

Of course, this incredibly complex subversion process - which requires the physical possession of the hardware token for a lengthy period of time and the use of highly complex electronics and counterfeiting technology - can be neatly side-stepped if you simply hack the servers of the company owning the keys.

When this happened with the widely-publicised RSA systems hack in March of this year, the hackers effectively gained access to the seed record database that forms the foundation of the RSA 2FA system.

And it's against this background that the integrity of all 2FA tokens - whether hardware or software - needs to be viewed.

All 2FA systems can be subverted, given enough time and resources, but a hardware-based system, just like a software-based system such as that seen using cellular text messages, takes a lot of time and effort that few people outside of US and other major government law enforcement staff have access to.

A text message might even be eavesdropped upon with malicious software on the phone, but the chances of this happening in the real world - outside the pages of a James Bond movie script - are minimal, just as they would be where the subversion of a hardware-based token is involved.

In addition, given the wide diversity of phone models and operating systems, any text message subversion technique would have to be adapted many dozens of times over to cover all eventualities.

And if the smartphone vendor issues a firmware update - or Google's Android software development team updates the smartphone operating system (as frequently happens) - the cybercriminal would be back to square one.

Phones such as iPhone and Blackberry rely on the App Store that only publishes trusted software that has been checked to be virus free and ensures that the originators identity must be confirmed making it impossible for a hacker to install malicious software anonymously.

It should also be noted that those that have tried to hack personal phone data have ended up in prison, caused the down fall of the News of the World and lost billions (Rupert Murdoch).

The great bonus about putting authentication onto a mobile phone is users realise very quickly when they have lost their mobile phone and therefore report it far quicker than they would with a token. If for any reason someone does manage to retrieve a passcode from a user's phone they will still need to know the User ID and PIN or Windows Password to log on.

The hacker will only get one attempt at getting this correct at which point even if they are denied the system will generate a new passcode that is sent to the user's phone alerting the real user to an illegal log on attempt. A hardware token user would never know if someone had tried to hack them.

Many users leave their tokens in their laptop bag which is very much like gluing your car keys to your car, as opposed to a mobile phone which is almost certainly kept close to the user and separate to their laptop."

If you still don't trust SMS please bear in mind you can still opt to use alternatives like SecurEnvoy Time Sync Soft Token on iPhone, Blackberry, Android and soon laptops which have no reliance on SMS as they are isolated software versions of time sync tokens with the added security benefit that seed records are created at enrolment within your own server and can automatically resynchronise to any time zone in the world.

References

The GSM Specifications - http://bit.ly/f6UE72
May 2002 - IBM research develops technology to protect GSM cell phones' ID cards from hacker attacks - http://bit.ly/eSFzW2
Dec 2009 - GSM 64-bit encryption standard cracked and posted to web - http://bit.ly/g3XLf1
Jul 2010 - Hacker shows how he intercepts GSM cell phone calls - http://bit.ly/9Oa1ya
Dec 2010 - 27C3: GSM cell phones even easier to tap - http://bit.ly/f4TNVH
Mar 2011 - RSA's SecurID customers worried that breach affected seed record database - http://bit.ly/o55YNS

World News In Brief

Samsung Biting into Nokia's Lead

According to The Times of India, Samsung the Korean mobile handset manufacturer is catching up with its Finnish competitor Nokia as growth of Smartphones in India take off.

Nokia is still the market leader in India with 39% of the market share but Samsung has increased its market share 28% in the first seven months of this year.

Nokia has recently adopted Microsoft's Windows as its primary platform for Smartphones. Nokia is also adopting dual SIM in its Xi-01 and C2-00 phones launched in June this year.

According to The Times Nokia will shortly be introducing cheaper Qwerty and touch and type phones. Mobile phone subscriptions in India will soon reach 900M.

RIM Unveils Blackberry Tag

During his keynote presentation at the GITEX conference in Dubai, Research In Motion Co-CEO Jim Balsillie unveiled a new way for BlackBerry smartphone users to connect with one another and share multimedia content.

BlackBerry Tag, which will be incorporated in the next BlackBerry 7 OS update, will allow users to share contact information, documents, URLs, photos and other multimedia content by simply tapping their BlackBerry smartphones together.

BlackBerry Tag will also enable friends to instantly add one another as contacts on BBM (BlackBerry Messenger).

BlackBerry Tag takes advantage of Near Field Communications (NFC) technology included in the recently launched BlackBerry Bold 9900/9930 and BlackBerry Curve 9350/9360/9370 smartphones, and these are the first BlackBerry smartphones that will support BlackBerry Tag.

RIM also announced plans to expose BlackBerry Tag through APIs on the BlackBerry platform, allowing software developers to take advantage of "tap to share" functionality from within their own applications.

Largest ID Theft in US History

111 people have been indicted by the New York authorities accused of participating in an identity theft scam that netted more than $13 million from the use of counterfeit credit cards.

The organised crime rings were based in Queens County, New York. They collected credit card data with card skimming devices.

"This is by far the largest – and certainly among the most sophisticated – identity theft/credit card fraud cases that law enforcement has come across," said District Attorney Brown.

Man In The Middle Attacks (MITM)

By Dr David Everett, Smartcard & Identity News

David Everett

The concept of Man In The Middle (MITM) attacks for electronic payments has been rife the last few months so let's start off by looking at the EMV PIN attacks published by Cambridge University. We will look at other forms of MITM attacks in subsequent newsletters.

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,

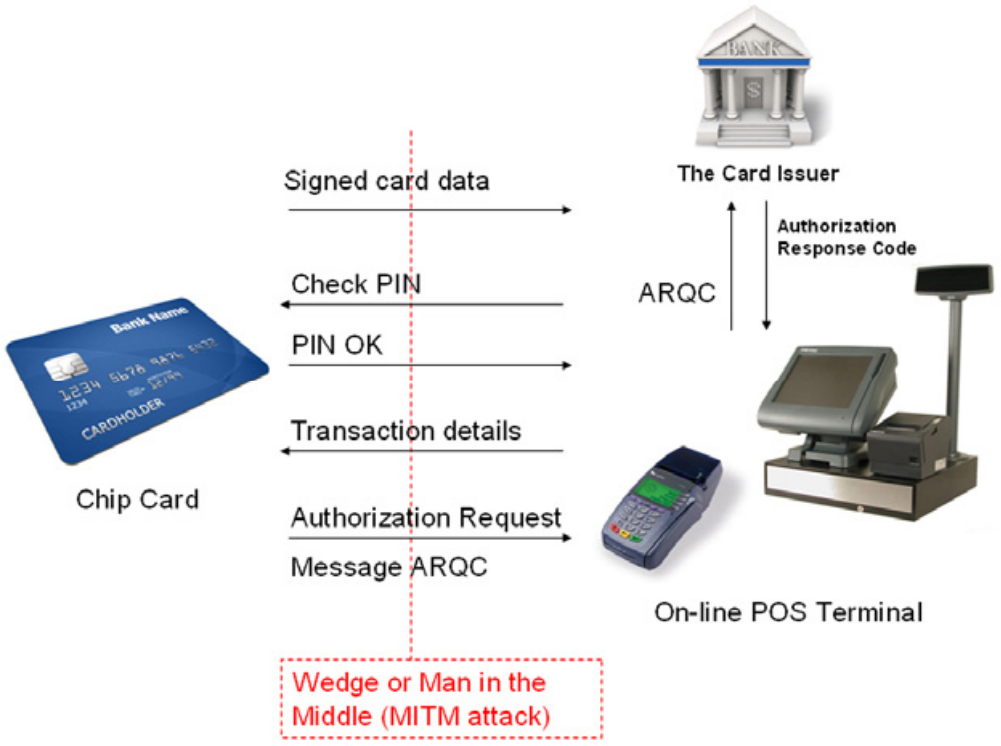
- The chip does not mandate a PIN check
- The chip may not implement public key cryptography
- The terminal does not hold Issuer secret keys
- The terminal may operate off-line

There are two scenarios to consider,

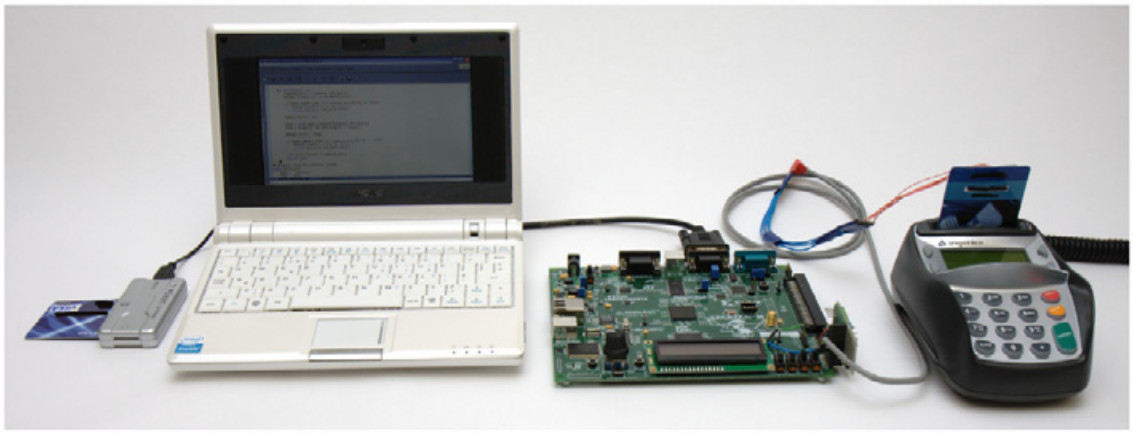
An off-line transaction where the chip doesn't implement public key cryptography, in this case the terminal is incapable of checking any data created by the card because it would require a secret key in the terminal.

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 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 authorization 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 from 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 Authorization 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 uncontrolled downloaded applications – Oh no, not yet!

World News In Brief

Blackout for Blackberry

Blackberry users suffered blackout only hours after RIM claimed the data crash on the 11th Oct had been sorted. Users were unable to access the internet and send SMS messages.

Malik Saadi, Principal Analyst at Informa Telecoms & Media has commented on the recent BlackBerry outages:

"The current situation with the BlackBerry outages couldn't come at a worse time for RIM, following some harsh criticism in recent months. Some businesses may see this as a good reason to re-evaluate their reliance on centralised servers and instead look to investing in more corporately controlled servers.

Not only would this enable IT departments to minimise the risk of unforeseen collapses but it could also give employees more flexibility to use their own devices.

However, it will take more than just a couple of collapses to persuade loyal consumers of BlackBerry services to look for alternatives. Having said that if RIM does not resolve the problem once and for all, the results could be disastrous for the company in a time where it has already disappointed the financial community."

Android Retains Top Spot as Favourite Smartphone in Britain

Intelligent Environments, a digital banking provider and part of the Parseq Group, reveals that Android phones remain the most popular smartphones for British consumers, with 30 per cent of smartphone users surveyed opting for this platform, up from 28 per cent in March. This increase widens Google's smartphone lead over Apple in Great Britain.

According to the YouGov survey conducted online, 27 per cent of smartphone users surveyed now own an iPhone compared to 26 per cent in the first quarter of the year.

RIM's BlackBerry remains third in line when it comes to smartphone ownership although it has seen resurgence in the last few months with 19 per cent of smartphone users now owning a Blackberry versus 14 per cent in March.

The growing uptake of smartphone adoption looks set to continue with a separate study finding that a third (34%) of standard phone owners want to get a smartphone next time they upgrade or purchase a mobile handset.

James Richards, Director of Mobile at Intelligent Environments, said: "From retail to financial services, businesses in all sectors are taking full advantage of the rise in consumer smartphone adoption.

While the iPhone is the bastion of apps, this research shows that businesses cannot be complacent and must cater to Android and BlackBerry users too. More importantly, businesses should focus on mobile applications and services that bring convenience and simplicity to consumers' lives."

Contactless Card Ensures Aid gets to the right People

Paystream, in partnership with sQuid, have provided a solution, whereby the people of Northern Kenya, affected by severe drought and famine, are issued with a contactless card. These cards can only be used at charity approved stores and outlets for the purchase of food supplies, as intended by Aid agencies and their donors, and will help to ensure that aid gets to the right people and is spent on what it is intended for.

The traditional method used to distribute food aid is cash based, which brings with it a multitude of complications,

often resulting in the misappropriation of funds. Logistical problems and the high cost of transporting supplies to remote villages demand more efficient solutions.

SOS Children's Villages and Paystream have been working together with the local community and shop owners to devise a card that is loaded with value and can be used at specified POS terminals supplied to the stores. It allows villagers to purchase supplies directly from the shops in their areas. Communities are educated as to how the system works the money that each holds and the kind of food stuff that they are allowed to purchase from the shops. Payments are secure, fast and efficient, significantly reducing the administration previously required by SOS to ensure the funds go where they are most needed.

All card based transactions will originate from approved card holders to POS devices deployed by Paystream to appointed stores.

SOS Children's Villages' portal sets descriptions and payment details for the shopkeepers. Simple and intuitive, data can be easily exported into SOS packages for quick and easy accounts reconciliation and visibility of payees.

Gemalto TSM Selected for Singapore's Nation-wide NFC Roll-out

Gemalto announces its selection by IDA to develop and operate its Trusted Services Manager (TSM) solution to securely deploy and manage mobile NFC services such as payment, ticketing, loyalty and other wireless services like the smart poster which allows consumers to interact with advertisements.

This open yet secure platform will also encourage widespread participation by businesses and service providers from wide-ranging industries to join the ecosystem to offer more consumer services, including mobile coupons, mobile tickets and product information.

The complete TSM operation will take place in a secure environment in Singapore, whereby end users' data is provisioned confidentially over the air to their devices. The project is expected to launch commercially to consumers from middle of 2012.

New Solutions for a Paperless Lifestyle

Fujitsu announced new capabilities for sending scanned paperwork to the Apple iPad and iPhone, in addition to new functionality allowing users to upload scanned documents to a wide range of cloud-based services using its ScanSnap S1500, S1500M, S1300 and S1100.

With the launch of its first official app for both the iPad and iPhone "ScanSnap Connect", consumers have a convenient way to send and store their scans to their mobile device, and organisations have a flexible solution to assist with collaboration between colleagues and business partners.

Furthermore, ScanSnap now enables users to scan documents directly to Salesforce Chatter and SugarSync, in addition to the scanners cloud services support for Evernote and Google Docs, giving users even more flexibility to store, share and access their paperwork. Whether it is scanning contracts, receipts, bills, invoices, or business cards on the road or using a PC in one place and a Mac in another, consumers have the necessary tools to be even more productive and paperless virtually anywhere.

"Today, everything is mobile, connected, interactive and immediate, which is helping shape consumer behaviour and drive cloud computing," said Michael Sidejas, product marketing manager, Fujitsu Computer Products of America, Inc. "We've taken pride in our ability to quickly evolve ScanSnap's capabilities and add new features that no other document management company offers today to provide consumers and business professionals the most productive, versatile scanning experience."

Nokia Unveils new Smartphones at Nokia World

At Nokia World, the company's annual event for customers, partners and developers, Nokia demonstrated clear progress on its strategy by unveiling a bold portfolio of innovative phones, services and accessories, including the first smartphones in its Windows Phone-based Nokia Lumia range.

Nokia also launched four new mobile phones the Asha 300, 303, 200 and 201, which blur the line between smartphones and feature phones, offering QWERTY and touch screen experiences, combined with fast and easy access to the Internet, integrated social networking, messaging and world-class applications from the Nokia Store.

"Eight months ago, we shared our new strategy and today we are demonstrating clear progress of this strategy in action. We're driving innovation throughout our entire portfolio, from new smartphone experiences to ever smarter mobile phones," said Stephen Elop,

Nokia President and CEO. "From the Nokia Lumia 800 to the Nokia Asha 201, we are bringing compelling new products to the market faster than ever before. I'm incredibly proud of these new devices - and the people of Nokia who have made this happen."

19% Growth in Smart Card Market

2010 proved to be an extremely successful recovery year for the smart card industry with unit shipments growing 19% compared to 2009. For the smart card IC market, volume growth was even higher at over 20% as card suppliers' inventories were re-stocked. This was one of the top line conclusions from IMS Research's just published report "Smart Cards and Smart Card ICs - World - 2011"This growth rate compares very favourably to the estimated 5% growth seen in 2009 during the recession. 5% was the slowest unit shipments had increased year on year since 2002 and the second worst growth rate on record.

"This 19% growth rate compares very favourably with the long term trends for the market." stated Alex Green, one of the report authors. "Over the last 10 years the average annual growth rate for this market has been around the 20% level, within only 2002 and 2009 dipping significantly below this level," continued Green.

Unfortunately this high level of growth is not forecast to be maintained. "Although the market is not forecast to drop back down to the lows seen in 2009 and 2002, and is still forecast to have double digit annual growth, it will struggle to stay at the 20% level," continues Green. This is largely attributed to that fact that the cellular handset installed base is projected to grow at lower rates than those seen during the last decade and hence the SIM card market will grow at lower levels. "The SIM card market is responsible for the majority of smart cards shipped and so the wider market is very much influenced by trends in SIM card shipments," stressed Green.

That being said, other applications are forecast to "take up the slack" to some extent. Growth for payment and banking cards is projected to remain at the same historically high levels and M2M is forecast to inject additional growth.

BPC Banking Technologies Provide EFT Payment Processing Solution For National Reserve Bank

BPC Banking Technologies, the leading provider of Open System e-payment solutions for the global financial industry, announced that it had been selected by National Reserve Bank to provide an end-to-end in-house EFT payment processing solution.

It took only five months to develop and implement new platform in the Bank's processing centres, manage the migration from the legacy system, pass all certifications with Visa and complete the training of the Bank's operational staff. Following a competitive bid process SmartVista won the deal for most exactly meeting National Reserve Bank's requirements as a highly functional, flexible and scalable solution. The Bank decided to move from an outsourced model to a modern Open System in-house processing solution to manage its ambitious growth plans for its payment's business, to improve its speed to market, lower the TCO and gain direct control over a strategic line of business. The state-of-art solution runs the Bank's processing and personalisation centres in Moscow, covering the Moscow region and Voronezh, covering the rest of Russia. The processing centres will now handle all card management, card personalisation, switching and authorisation and ATM management. In the immediate future the Bank plans to widen its range of payment services to include issuing EMV smartcards, e-commerce, i-banking and MasterCard products.

"We are proud to have been selected to play such an important role in supporting National Reserve Bank's strategic shift in its payments business. With SmartVista to run all payment processing the Bank will enjoy a flexible, scalable and low cost payments infrastructure for many years to come," said Vasily Grigoriev, CEO, BPC Banking Technologies.

"The constraints of our original payments infrastructure would not have managed our aggressive growth plans to increase our card base significantly and to expand the range of payment services to our customers We took the decision to assume direct control over our payments business and have been very pleased with our choice of SmartVista and BPC's ability to implement the new solution quickly and seamlessly," commented Oksana Pogodina, Deputy Chairman of the Board, National Reserve Bank.

Mobile Banking App Usage in the U.S. Increases 45 Percent from Q4 2010

ComScore, Inc., a leader in measuring the digital world, released analysis of mobile financial services usage in the U.S. which showed an increase of 45 percent from Q4 2010.

PayPal Unveils the Future of Shopping

In his blog Scott Thompson, President of PayPal starts to reveal PayPal's new payment technology. "PayPal is re-imagining money and making it work better for merchants and consumers - whatever device you're on, wherever you are in the world, and however you prefer to pay (whether that's cash, credit, or instalments).

And let's be clear about something - we're not just shoving a credit card on a phone", blogged Scott. PayPal will be announcing more over the coming months.

Blackberry Bold 9900 and Curve 9360 are Worlds first SIM-Based Smartphones to receive Mastercard Paypass Handset Certification

Research In Motion announced the BlackBerry Bold 9900 and BlackBerry Curve 9360 smartphones are the first SIM-based NFC smartphones to be certified by MasterCard Worldwide as PayPass-approved devices.

The certification was granted on the basis of the BlackBerry smartphones meeting the functionality, interoperability and security requirements of MasterCard. With this certification, any MasterCard PayPass-issuing bank globally will be able to deploy MasterCard PayPass-enabled accounts to the SIM card of these smartphones.

The ecosystem to allow customers to take advantage of the certified BlackBerry smartphones for NFC payments is already growing. France Telecom - Orange believes that mobile NFC has the potential to enable a new revolution in mobile by further connecting people's mobile digital world with the physical world around them. France Telecom – Orange is the first operator worldwide to have commercial NFC launches in two countries, UK and France, with trials in several European markets.

"We are happy to offer the BlackBerry Bold 9900 and BlackBerry Curve 9360 as part of the Orange range of mobile NFC devices. We are committed to actively marketing NFC devices, and these new smartphones will help accelerate the adoption of mobile NFC services secured by an Orange SIM, Director of Contactless Services at France Telecom – Orange. "We have a strong partnership with RIM,

and look forward to working together on more NFC initiatives in the future."

Patients' Details Binned on Two Occasions

University Hospitals Coventry & Warwickshire NHS Trust breached the Data Protection Act by losing patients' medical information on two separate occasions, the Information Commissioner's Office (ICO) said.

In February, records relating to the treatment of 18 patients were found in a communal waste bin at a residential apartment block. The information had been taken home by a member of staff and accidentally disposed of in a public bin along with other rubbish.

In a second incident - which took place in May - a member of the public discovered details relating to a patient's sensitive medical procedures and test results which were allegedly found in a bin outside Coventry University Hospital.

The ICO's investigation found that the trust's policies and procedures on the use of personal information were not sufficient. During the Commissioner's investigation, concerns were also raised about the delivery and collection point for patient notes at one of the Trust's hospitals.

HID Global and ASSA ABLOY Strengthen Patent Portfolio in NFC Technology

HID Global announced that the company and its parent, ASSA ABLOY, have been notified by the United States Patent Office that their patent, US 2008/0163361, titled "Method and Apparatus for Making a Decision on a Card," has been allowed and will issue shortly.

This invention covers the use of portable credentials in a secure access network, in which the access decision can be made within a portable credential (such as the secure element of a mobile device) using data and algorithms stored within the credential.

Public Transport: Nevermind the gap!

By Marie Costers, Clear2pay

Marie Costers

Mobility is an essential feature of our daily lives. In just a few decades it has become astonishingly easy to travel around the country, within continents and around world.

The history of public transport is a story about innovation, from the world's first ferries, stagecoaches and omnibuses to travelling with cable cars, trains, motor buses and planes. Transport technology has shaped cities and countries and structured our lives. The impact of technology is truly inspiring; the world withholds an impressive amount of travellers and commuters and promotes an increasingly global marketplace with blurring geographical boundaries.

Shaping a new payment sphere

We see a similar change in how we pay for public transport and how we interact with the adjacent applications and services of the journey chain.

Most transport schemes started off, and many still are, as closed-loop (single vendor) transport schemes that used proprietary fare collection systems, with the aim of merely collecting funds. These 1st generation infrastructures are lone islands lacking the slightest bit of compatibility and created legacy systems based on basic contactless memory card technology. Such schemes helped in establishing contactless technology to become widely available and relatively cheap.

Next generation ticketing

With today's adjusted travel expectations it is time to migrate to more powerful, integrated solutions. From a scheme operator perspective not only the support of more advanced travel related services and ticketing types (including stored travel value solutions) but also alleged security breaches are a driver to move to more secure microprocessor-based contactless cards. Moreover, advanced back-office systems allows for more efficient planning. All are significant factors for a smart public transport and a sustainable and superior travel experience.

Today's technology also allows for better knowing, understanding and informing the customer. But there is more... For some time now, international travellers are familiar with using use their debit and credit (smart) cards wherever they go. Why shouldn't this be possible with transport tickets: one ticket accepted internationally, allowing an end-to-end, multi-modal journey?

The new generation of transport systems that are being developed today are bound to be the foundation of Automatic Fare Collection (AFC) systems for years to come, and should take care of the modern traveller's demands.

Open standards for interoperability

One of the recent answers to these needs is the use of EMV-based ticketing, where the existing payment standards are extended to support transit specific needs. One example is South-Africa, where the National Department of Transport is currently implementing a modern, integrated AFC system based on the newest generation of contactless payment cards inhibiting data storage capabilities. This enables electronic tickets or subscriptions to be stored on regular payment cards (issued by banks).

Because of the specific requirements of public transit however, other's are working on dedicated open transport standards. Just to name a few:

The Open Standard for Public Transport (OSPT) Alliance, founded by Giesecke & Devrient, Infineon Technologies, Inside secure and Oberthur Technologies, developed CIPURSE: an open security standard to foster the next generation of more secure, cost-effective, scalable and extensible transit fare collection

systems.

Calypso is another example set of standardising specifications, developed by a group of European partners from Belgium, Portugal, Germany, France and Italy. Calypso is not simply restricted to transport applications but offers the opportunity to enable access to third-party services, using the same device within a multi-applications scheme.

ITSO is a UK government-backed non-profit organisation which sets a common technical standard for transport. It enables transport operators to link up offering a seamless transport experience to UK passengers. The ITSO smart cards can be used for multiple services, other than transport.

Key in open standards is interoperability. Interoperability is the ability of a system or a product to work flawlessly with other systems or products. Interoperability can or should be established at different levels: at technological level, where new technologies like Near Field Communication need to be integrated in legacy contactless environments, as well as at business level , where compatibility of ticketing information and clearing and settlements, should be achieved. Quite a challenging mission. Yet, transport authorities and operators willing to set up truly interoperable transport, need to agree on many rules and regulations.

The dream solution

And then there's the mobile phone… almost everyone's favourite smallest bit of technology. Logically, what would really satisfy the 21st century traveller is a ticketing system that makes smart use of the power of mobile phones. The ubiquitous mobile instrument is more likely to be in the pocket of a consumer than the classic leather wallet which contains lots of different plastic cards and paper tickets. A recent report states that the US consumer now spends more time on mobile applications than on web consumption on a PC (Source: Flurry, June 2011). The mobile phone is a potential e-wallet and, in combination with contactless terminals or smart posters a mobile ticket machine, a time schedule, a route planner, remote traffic info and a paperless receipt. The mobile phone is connecting people and has the ability to simplify connection between places as well.

It seems that Near Field Communication is the technology that will enable the ultimate e-ticketing platform. It's a standards-based short-range wireless connectivity technology that enables simple, powerful and intuitive two-way interactions between electronic devices such as mobile phones and terminals and tags. It allows fast and easy ticketing, speedy access control, download of information and more. Moreover, it can be used with the existing contactless transport infrastructures requiring no additional investment and allowing a greener behaviour ending the issuance of paper and plastic cards and reducing cash handling.

On the proving ground

For open standard transport systems to be a success, compliance to the standard and interoperability needs to be proven. Here, the payment space can serve as an example. EMVCo, the payments standard body, imposed international rules to which card payments components should comply, enabling conformity and global interoperability. To ensure quality and global acceptance, a rigid certification regime for the different components such as cards and devices was put in place. At technology level, in the NFC space, we see a similar tendency with the NFC Forum standards-based specifications and certification program.

Testing eradicates failures, identifies risk areas and pinpoints issues that can lead to costly modifications post-launch. It is an essential step in the process of reaching truly interoperable public transport systems that offer intuitive, value-added experiences to voyagers. Cards, devices, software, back-office system or other components of the chain should be tested meticulously for compliance to ruling standards before being put into operation or rolled into the field. So this implies adding application (read business logic) compliance testing.

To achieve the all important interoperability and watertight integration of all components, the different parts of the puzzle need to undergo an even more specific and complex test process: interoperability testing. This particular type of testing does not only test whether components communicate with each other, as detailed in the specifications, but also tests the "internal" interoperability of the components itself such as e.g. accurate interaction between technology layers and the business logics.

Sure, testing is not the core activity of transport operators. It's companies such as Clear2Pay among others, who

build on years of experience, that can assess the complexity of testing transport transactional systems with certification services and readily available test solutions. These test tools can be instrumental throughout the development phases as well, as an interim benchmark.

In the long run, large-scale certification or acceptance programs will prove essential in putting advanced public transport on the road to success. Certification provides formal recognition of the conformance of a vendor product to the client's functional specifications. Vendors will have to make clear claims of conformance. This will enable authorities and operators to choose, in full confidence, between different products from different vendors offering the exact same functionalities. A more open market as such will encourage competition and improve quality at reduces prices.

Just imagine...

The transport sector is reshaping and evolution will not stop for a while. Since the beginning of time, the way we move around has dramatically changed and is still changing today. Where will we stand in 2030, who will tell...will we be time travelling maybe? At Clear2Pay we are already looking into testing this, one never knows. But seriously, it would be just great to have transport systems synchronizing around the globe and provide travellers a seamless journey without any gaps in their itinerary.

World News In Brief

Smart Cards Could Identify Fake Lawyers

The Bar Council of Tamil Nadu (BCT), one of 28 States in India, which monitors the professional activities of around 70,000 advocates in the State, is to embark on a digitisation project to weed out bogus certificates and misuse of BCT stickers for non-professionals. Documents will be scanned and digitised in a tamper-proof format. The Identity and enrolment details of each advocate will be in a smart card for easy verification of their credentials.

NFC payments in UAE

Etisalat - a major telecom operator in The United Arab Emirates will launch the middle east's first pay by phone system. This will allow a pre paid debit card to be stored on the phone. Based on NFC communications, the system will allow subscribers to pay amounts up to $50. It will initially be available on Blackberry Bold 9900 phones and other phones are planned for the future. The system is still awaiting approval from regulators.

INSIDE Secure Surpasses 10 million NFC Chip Shipments

INSIDE Secure announced that it has shipped more than 10 million MicroRead and SecuRead NFC solutions to date this year to multiple manufacturers of a broad range of mobile NFC devices. This milestone heralds the imminent arrival of mainstream NFC smartphones and devices to global markets as the industry achieves liftoff in 2011, and means that devices with INSIDE NFC solutions will soon be in the hands of millions of people who will use them to enjoy the rich consumer experiences of new mobile services.

Watchdata's NFC Solution Selected as Finalist for SESAMES Award

Watchdata has been selected as a finalist (banking/retail/loyalty category) for the SESAMES Award at the upcoming CARTES event in Paris. The SESAMES Award recognises the best innovative technological application in the field of smart cards, digital security, contactless and secure transactions.

Watchdata's innovation is a SIM-based full-NFC-solution designed to address a void in the NFC payment space where vast majority of the phones cannot be easily transformed to perform functions such as making NFC payments. With Watchdata's SIM-based solution, it is now possible to integrate 3 chips into 1 SIM card, therefore providing emulation, reader and Peer2Peer modes in one card.

Cryptography Research license DPA countermeasures to major Smartphone Manufacturer

Cryptography Research, Inc., a division of Rambus Inc. has signed a license agreement with a major smartphone manufacturer for the use of CRI's Differential Power Analysis (DPA) countermeasures patents.

Under the agreement, ongoing royalties will be paid for the use of CRI's patented innovations. Specific terms of the agreement and disclosure of the smartphone manufacturer are confidential.

"Consumers increasingly rely on their smartphones and tablets to perform financial transactions, store personal data and access premium content," said Paul Kocher, president and chief scientist of Cryptography Research. "Our DPA countermeasures technology is a key part of securing mobile devices to safeguard the data of consumers and content providers worldwide."

Differential Power Analysis (DPA form of attack that involves monitoring variations in electrical power consumption of a target device and then uses advanced statistical methods to derive cryptographic keys or other secrets. Strong countermeasures to DPA are important for securing mobile devices, bank cards, pay television systems, secure identity products, secure storage media, and other electronic systems and components. Many of the world's leading security standards include requirements that devices be protected against DPA and related attacks.

Cryptography Research has developed a portfolio of more than 55 patents covering countermeasures to DPA attacks, with additional patent applications pending worldwide.

UPM and Hansaprint Introduce NFC Mobile App at Nokia World

UPM RFID and Finnish-based printing house Hansaprint are introducing a revolutionary NFC mobile application called TagAge Mobile. The TagAge Mobile tag creator is the first of its kind in the world, allowing users to create NFC tag content and graphics using their own photos stored on smartphone.

Users don't need to have NFC phones for tag encoding; they can simply create the content in the app and order printed and encoded tags for delivery to the desired address.

Content creation supports all NFC NDEF formats. The graphical user interface provides ease-of-use as well as a sticker sample library with ready-made designs.

TagAge Mobile for Nokia Symbian smartphones will be available to the public free of charge via Nokia Store during November 2011.

"With TagAge Mobile we are removing the last barrier to making NFC tags easily available to consumers. We expect that great, undiscovered ideas and concepts will start to flow rapidly now that consumers have all the required tools, NFC tags and smartphones available," says Mikko Nikkanen, Business Development Director, UPM RFID.

Free Apps & support for Blackberry Users

Research In Motion announced that a selection of premium apps worth a total value of more than US $100 will be offered free of charge to subscribers as an expression of appreciation for their patience during the recent service disruptions. The apps will be made available to customers over the coming weeks on BlackBerry App World and will continue to be available until December 31, 2011.

Smartphone Compatible Radiation Detector

Universal Detection Technology, a developer of early-warning monitoring technologies to protect against biological, chemical, radiological, and nuclear (CBRN) threats, announced that it has started developing a smart phone compatible radiation detector. The device will be able to read radiation levels and to communicate the results with smart phones such as Apple's iPhone.

The initial development of the device has been focused on making it "blue tooth" compatible with Apple's iPhone although the Company expects to add other smartphone platforms in the future.

Smartcard News Subscription

Smart Card & Identity News is an independent international newsletter.

Our key industry topics are smartcards, biometrics, cryptography, identity management, RFID, Mobile and payments.

Within these industries we cover technological advances, security breaches, new products, personnel changes, contracts and company take-overs. We also include opinion pieces and technical tutorials from the industry's leading experts.

To subscribe please contact us on 01903 734677 or email info@smartcard.co.uk, subscription can also be purchased on Amazon by searching for "Smart Card & Identity News"

How NFC will change our lives...

By Ayman S. Ashour, Identive Group, Inc.

Ayman S. Ashour

The evolution of identities and credentials

From the very beginning of time, we human beings have employed differing forms of identification and privilege management. Early man relied on the simple, direct identification of others to grant a privilege such as sharing a meal or shelter. Sometimes just the voice was enough to grant access to a cave or path, sometimes visual ID was required. Generally, in their small, closed settlements, early humans knew those in their community and had minimal interactions with outsiders. As we moved on, however, to larger tribes and settlements, and the number of these interactions increased, markings, colors, code words or sounds began to become more important in the proper identification and privilege management of these individuals. The challenge continued over the millennia and finding ways to identify people grew more complex: locks and keys were invented for physical access; barter moved on to precious metals and later coins and currency were introduced to allow for commerce. Gradually, wax seals, signatures and the possession of keys or currency played bigger roles in commerce and privilege management. Commerce is, at its core, an exchange of privilege, through possession or consumption. As populations grew and settlements expanded into villages, towns and large cities, the need to deal with total strangers and for methods of granting them specific privileges continued to grow. Increased travel complicated matters a great deal further.

Complexity of managing increased number of credentials

We move on to our twenty-first century with far more advanced societies and unprecedented levels of movement, migration, travel and international commerce. The phrase "global village" may be an annoying oxymoron for some, but it is a living reality for the more than one billion people who travel, building friendships, connections and business with others across the globe. Our need for identification and privileges management has exploded in volume and complexity. We carry drivers' licenses to drive and, in the US, for general ID purposes such as domestic travel or checking into a hotel. We carry passports to travel internationally; we carry health insurance cards for access to medical treatment or to obtain medication; we carry frequent flier cards, bus passes, library cards, bank debit and credit cards, even ski passes and loyalty cards for every tenth coffee. We also carry badges or cards to get into our office building, college dorm, parking structure, company cafeteria or gym. We sometimes use cards or tokens to gain access to a website or to log on to a network; we also use a multitude of passwords that we must try and memorize. Passwords are driving us all crazy as we are forced to include symbols and characters and to change them every ninety days or so. For extra security we are sometimes even forced to use an external password generator, provide a finger print or allow an eye scan, either alone or in a combination with an ID card, fob or PIN.

There is mounting irritation and confusion as we have to deal with so many different ways to prove that we are entitled to whatever it is we are trying to access: our money, healthcare, the workplace, the ski slope, a private airport lounge, a travel website, online banking, a social or company network. We deal with disparate systems, each with its own key, its own lock. So we walk around burdened with numerous keys and cards, trying to remember many different passwords with different rules. All of them dedicated credentials and methods of ID, used on proprietary systems and applications.

Move towards convergence of credentials

In some areas there has been a strong drive towards converging multiple functions onto one card in order to increase security by having a single point where credentials can be issued, managed or revoked. The U.S. Government, for example, has been engaged in a multi-year effort to replace the plethora of cards issued for access to physical buildings and the dedicated smart card for network access used by employees and contractors with one single credential, known as the personal identity verification, or PIV card. Enterprises are also beginning to converge their employees' credentials so that both physical sites and computer networks can be accessed with the same card. On the technology side, miniaturization has made it possible to transfer the security benefits of smart cards to RFID cards, creating what is known as a contactless smart card, so that user convenience is further enhanced with the ability to just touch one's identity card to a door or computer reader to gain entry.

While this convergence of physical and IT access control in the workplace requires significant upgrades to the various systems involved, it also offers the employer the ability to manage different types of privileges on one, single smart credential.

NFC creates one, simple-to-use system for everyone

Near field communication, or NFC technology is a revolutionary development that promises to provide the convenience of a single, contactless credential for each of us – and a lot more – by enabling a highly secure ***personal credential*** to be built into our mobile phones. An NFC-enabled phone such as the Google Nexus S or a Nokia N9 incorporates all the functions of a secure contactless smart card, comparable in its level of security and sophistication to highly secure electronic credentials such as electronic passports, credit cards or expensive electronic tickets. What makes NFC phones really powerful is the convenience of enabling them anywhere, anytime through secure mobile connections, to act as our personal credential for an endless number of possible mobile applications. We can use our NFC-enabled smart phones to help us sign on to different websites, networks or loyalty programs, thus eliminating the need to remember all those multiple passwords. We can download a ski pass to our phone, or tap our phone to workout machines to log our fitness routine or map our run.

We can also use our NFC phones as a ***reader or scanner.*** Just as we use the camera to take photos, we can use the NFC reader features in our phone to download data such as merchant coupons or restaurant reviews from smart tags or smart posters. We can buy and download our Charlie, Oyster, BART, MARTA or other transit pass on our NFC-enabled phone and just hop on the bus or subway using a machine-to-machine transaction between our mobile device and the ticket issuing machine. We can follow organizations or people on Twitter and Facebook or receive RSS feeds by simply using our smart phones as readers. NFC also supports more secure transactions. In many countries, online banking transactions are required by law to use the strong authentication of a one-time password, or OTP, generated from a card or token issued by a bank. NFC-enabled phones, however, can do the trick without the need for carrying an additional battery-powered device dedicated to reading out an OTP.

Choice, convenience, cost, security and above all fun and simplicity will determine what kind of world we will shape with our NFC phones in a new era of electronic consumer empowerment. So in this new brave, connected world, we move towards an integrated multi-application, multi-use credential and a secure multi-use, multi-application reader, both incorporated into our NFC-enabled phones; an inevitable move to a more integrated, more connected world.

Finally, as with the case with any new wireless technology, there may be lingering concerns about the security of vital data and communications. NFC is actually very secure. Because it operates only at very close ranges (1 to 4 cm), it is difficult to hack the data being transferred using NFC signals. The usual precautions of passwords or prompts before launching new applications on a smart phone apply with NFC just as they do elsewhere. And NFC-enabled phones don't require activation of GPS or global positioning, or even a cellular connection; they require a deliberate use by the consumer to read or be read. Therefore privacy concerns are abated as most NFC transactions take place within the mobile phone users' reach. NFC offers user-based control over which application we choose to read from or write to, and where or to whom we wish to make our presence known. The level of security can also be put in the user's hands. Settings can be changed to make a transaction automatic with a touch, require an app to launch first (i.e. must push a button), or even require entry of a pin code. The user can set the level of security based on his or her own personal comfort level with individual applications and use cases.

Most mobile phone manufacturers have announced plans to include NFC functionality in the next generations of their mobile phones. With up to 280 million people carrying NFC-enabled phones by 2013, new applications will develop rapidly. Credentials such as keys, access cards, tickets, business cards, plastic loyalty cards and payment cards could rapidly disappear in favor of a single personal credential on your phone. Consequently, NFC represents a paradigm shift in how we live, making everyday activities easier and more convenient by building on existing systems and human behavior. It will make accessing new media and content services more intuitive; make it easier to pay for things; easier to discover, synchronize and share information; and easier to use transport and other public services. How will NFC ultimately change our lives? In more ways than we can imagine.