This month we have had another example of compromised passwords, this time it was LinkedIn a widely used business networking site.

Thirty years ago, yes I only need to go back that far, user names and passwords were the norm for access control to some computing resource and PINs were all the rage for accessing one's bank account. But in the intervening years the world has changed so much in terms of networking and the attached cybercrime that user names and passwords no longer offer the right protection. The world at large doesn't seem to have realised this, perhaps it will take a breach in PayPal's security or Amazon but you can be assured it will happen, it's just a matter of time!

The logic of the problem is no different to that which made public key cryptography the base of eCommerce back in the 80's and is still the core security mechanism used today. The fundamental problem with symmetric cryptography is that the participants in a transaction both need to share the same secret key. In terms of confidentiality this in general can be made to work because the core business need is to share secret information whether it is information or keys. However when you are talking about authentication and integrity this is no longer true, the participants in a transaction may well have different and even conflicting business needs.

Continued on page 4….
When you are thinking of smart phones you can’t help but look at the overall market which is in the news every week. I gather Nokia has now ceded its position as the manufacturer of the most phones to Samsung. Less than a year ago people said this couldn’t happen because although Symbian might be a problem Nokia dominated the world of less smart phones. All phones are a bit smart so I couldn’t say non-smart phones.

Nokia of course decided to give up on the Symbian operating system and move instead to Microsoft Windows for Mobile. So far the experts don’t seem to be over excited and the take up has been disappointing. Nokia are having more cost cutting exercises including laying off another 10,000 people. Moody’s has responded by pushing Nokia debt grade to Junk status.

Last year we predicted the problems could only get worse, people are talking about succeed or die but I think the roll of the dice has already been made and there is no future for Nokia as an independent company. What a change, I remember only ten years ago that Nokia would never respond to enquiries, they would actually tell you that they didn’t need you…….

The world of mobile phones is however deceptively complicated, our office in India tells us that their local market is based very much on the more basic phones, they don’t see the same penetration of our smart phones.

Then we have the competing operating systems of which the Apple iPhone and Google’s Android create the most attention where the latter has pretty well twice the figures of the former but the charisma of Steve Jobs and the image he created for the IOS products will take some beating in the short term. It will be short of course because the Android has a much greater following of mobile phone manufacturers. Apple is not going to give up this control and now that Steve is no longer with us it is just a matter of time before they quietly start worrying. It’s Déjà vu for the 90s when Microsoft was rumoured to be keeping Apple afloat and one suspects the same thing is going to happen again with different parties? Today we have Blackberry, Nokia and Apple versus the Android camp, something has to happen.

The iPhone in many ways dominates and I’ve noticed over the last 6 months that the corporate executives have started moving away from the ubiquitous BlackBerry to the iPhone.
I think this is as much as anything because the IT departments are under too much pressure to resist change. If you were the head of IT and you had to give way somewhere then I think you would go for the iPhone and iPad. The open approach of Android is great for developers but it’s also a hackers dream.

Now here is the interesting thing, how will Google react? Will they address security and start to look at how to address the issues of malware or will they just leave the industry to get on with it? Apple took this on board from day 1, not without problems but nothing like the daily tales of malware on the Android phones. A big part of the problem is the interaction of the phone manufacturer and the network operator as to how they should configure the Android OS. Apple doesn’t take prisoners, IOS is what you get with no personalization by anybody else. I know they are behind Android but I still think they have the better product for the ordinary mortal. Pretty fool proof and how often do you see an iPhone crash? Also when I go to the Apple on-line store I feel pretty safe (apart from user name and passwords – see this month’s lead article). I’m sure it’s going to change but there’s more rope to let out yet.

When I talk to my friends the iPhone and the iPad dominate people’s perception, it’s actually an iPhone versus a Samsung or HTC or what have you. There are some interesting thoughts here for the brand makers.

Patsy. Researcher

Contents

Regular Features

Lead Story .......................................................... 1
Events Diary .......................................................... 3
World News In Brief .................................................. 5, 8, 12, 17

Industry Articles

Biometrics for Civil ID. .......................................................... 7
Consigned to History by the Smartphone .................................................. 10
Financial services technology meets the world of apps .......................... 14

Events Diary

June 2012

12-14 – Prepaid 2012- www.voicebiocon.com

20-21 – Contactless Cards and Payments - www.smi-online.co.uk/events/overview.asp?is=8&ref=3720

July 2012

02-04 – 1st Latin American High Security Printing Conference - www.cross-conferences.com/latinamerica

Source: www.smartcard.co.uk/calendar/
If the correspondent partner in a message relationship shares the same secret (key, PIN or password, it doesn’t really matter) then they can do whatever the first person can do. So if we are talking about enciphering confidential data then both parties can equally encrypt or decrypt the data. When you are talking about confidential data that all makes sense. Now let’s take a different scenario,

When you ask your bank to carry out some financial operation on your behalf you are not primarily concerned about confidentiality but the bank needs to authenticate your requirement both in terms of your authorization and the correctness of the data.

Now you can start to see the problem, what happens if the customer denies some aspect of the instruction, what happens if the bank denies some other aspect of the instruction? You can imagine the situation, the customer buys some shares which dump in value, and he may have a memory loss about the amount or even doing the transaction. The trouble is that legally it would be very hard to prove the customer initiated the transaction particularly in today’s open network world because the security controls are shared by both parties.

This is why digital signatures only really work if you use asymmetric cryptography because this is the only case where the sender and receiver don’t share the secret value. In a court of law unless you’ve found some quick way of breaking RSA or Elliptic Curve Cryptography there can be no doubt about the evidential value of the digitally signed message.

So back to the ubiquitous user name and password, values both shared by the sender and receiver and dare I say it probably anybody else that can get in the middle. The use of classical TLS or SSL will protect the channel from eavesdroppers but not those that interpose themselves when the secure session is established. The classical Man in The Middle (MITM) works all too well unless you use a client certificate which is rarely done. Why not? It’s so easy to do and it makes all the difference to the security of the connection.

Let’s pretend a little more, imagine that there is no breakdown of security at the client end, no malware, no PINs written down, no phishing, and a secure session is established without any interlopers. Wishful thinking really but let’s pretend for a little longer. Now when the host end comes to authenticate the user he can check the credentials, user name and password against what is stored in his database.

Now we are getting a little closer to the LinkedIn problem, some hacker got to the database. Well that shouldn’t matter you are probably thinking to yourself, it must be encrypted or something. That something of course is where the devil is in the detail.Stand back for a moment and put yourself in the place of the designer, he can’t store plain text passwords because that would be obviously wrong. So how about a hash function, some one way function so you can easily check a password but given access to the hashed file in the database you can’t go back and recreate the password. You could even make this hash function public information, why not, people would probably work it out anyway? SHA-1 has been around for a long time and although it has a few collision weaknesses it’s not really a problem here.

The trouble is people tend to use fairly short passwords, 4 characters, six maybe and if forced 8 characters. Well you can see the problem, you may not know the password but given the hash file it’s not going to take you very long to try the total password space to find the matching hashed version, you don’t need to find all of them, just enough for your mischievous purpose.

A number of observers have jumped up and down about the obvious protection of adding uncertainty to the hash values by adding some random salt to make the input to the hash function longer. All very well and good but what makes you think the hacker wouldn’t get this value? You need to apply it every time you check the password.

The amusing thing about the whole event is that people have been downloading the compromised hash file to see if their password is in the file because of course anybody can go this way through the one way function.

The lesson here is that the concept of user name and passwords really isn’t the way to go. There are vulnerabilities all the way down the chain. Do you really think that other well-known sites such as PayPal, eBay, Google and Amazon are immune? Proper authentication is all about challenges and responses and for me that means using asymmetric cryptography.
Prolexic Issues Global Warning about Recent DDoS Blackmail Attempts

Prolexic Technologies has reported a troubling trend in DDoS attacks targeted at online gambling sites, with multiple attacks accompanied by extortion letters.

During the past month, more than two dozen online gambling companies have come under attack and been targeted using similar attack methods. In recent days, multiple businesses in the online gambling sector have received extortion emails, demanding payments of up to US$50,000 to prevent new waves of DDoS attacks. The blackmail attempts have included escalation clauses, warning of increased size or frequency - as well as time-related price increases to stop them.

"The online gambling industry should be on high alert," said Neal Quinn, chief operating officer at Prolexic. "This appears to be a coordinated global threat. This is a focused level of effort accompanied by blackmail tactics, targeting a single industry in a compressed timeframe.

Lenovo and VeriFone Announce Mobile POS Platform with PAYware Mobile Enterprise

Lenovo and VeriFone Systems, Inc. announced the ThinkPad Mobile POS, a complete mobile point of sale (POS) platform for retail outlets built on the Lenovo ThinkPad Tablet and a custom version of VeriFone's PAYware Mobile Enterprise for Tablet payment solution.

With the ThinkPad Mobile POS, retailers can easily configure, customise and manage an end-to-end point of sale platform that delivers a more efficient and flexible alternative than stationary cash registers, helping to create new revenue opportunities for retailers, and improving the shopping experience for customers.

Retailers can remotely manage the ThinkPad Mobile POS with ease, including individual device tracking, managing applications, checking status on individual units and even remotely wiping and resetting devices to minimize on-site support intervention.

Survey Shows 66% of Retailers Interested in Mpos

Motorola Solutions, Inc. releases the findings of a survey that demonstrates increasing interest from retail, hospitality and field service industries for mobile Point of Sale (mPOS) solutions as a core strategy for improving customer service. Retailers are embracing mPOS pilots and trials to eliminate the high cost of traditional cash registers.

Michelle Crissey, Customer Solutions lead, Motorola Solutions, "As retailers battle for shoppers' hearts and wallets, mPOS serves as a valuable tool that can help turn browsing into buying. When the power of mPOS is in the hands of every retail associate, shopping becomes an experience and associates are always in a position to make the sale."

The survey was fielded from December 2011-February 2012, targeted to full-time experienced employees in the retail, hospitality and field service industries in North America, United Kingdom, France and Germany.
The survey was designed to reveal interests and experiences with the use of mPOS solutions. 541 respondents completed the survey without knowledge of Motorola Solutions’ sponsorship. The e-Rewards Opinion Panel, operated by Research Now, is the largest "by-invitation-only" online research panel serving more than 900 research firms with more than 3 million respondent members.

For more visit: www.motorolasolutions.com

Samsung No.1 Smartphone Brand Again in Q1

Data from leading mobile analyst firm Juniper Research shows Samsung and Apple trading places once again in the smartphone market, in what is increasingly becoming a two-horse race. In the first quarter of 2012, the company estimates that nearly 60% of the 139 million smartphones shipped worldwide carried either the Apple (35.1 million) or Samsung (46.9 million) brand - up from 46% in the last three months of 2011. While Apple and Samsung have taken it in turns to lead the smartphone market over the last four quarters, it seems as if Samsung may now have established a firm lead in this space - shipping 11.8 million more units that the Cupertino, California company in Q1.

With the iPhone launch craze now past, the analyst firm believes Samsung may hold onto its lead next quarter, but as Daniel Ashdown, Research Analyst with Juniper Research notes: "Apple's revenues from its 'mobile division' continues to remain significantly higher than Samsung's, even when you take into account the latter's feature-phones". Apple's iPhone revenue was $22.7 billion in Q1 ($29.3 billion including the iPad), compared with Samsung's KRW18.9 trillion (~$17.0 billion) from its entire mobile division. While flagship devices, the Samsung Galaxy SII and Galaxy Note contribute substantial unit volumes, the company's rise to top spot is evidence of the smartphone's entry into mass market price points with products like the Galaxy Y.

RIM Launch SDK for BlackBerry 10 Platform

At BlackBerry World, Research In Motion revealed endorsements from a number of key partners who have already confirmed their excitement for the upcoming launch of the BlackBerry 10 platform. RIM released in beta the developer toolkit for the BlackBerry 10 platform, which will allow developers to build and test their apps in preparation for the BlackBerry 10 launch expected in the latter part of 2012.

The toolkit includes the BlackBerry 10 Native SDK with Cascades, which allows developers to create graphically rich, high performance native apps in C/C++ or the Qt Modelling Language (QML). The toolkit also includes support for HTML5 app developers with the BlackBerry 10 WebWorks SDK, allowing them to create native-like apps using common web programming technologies (HTML5, CSS and JavaScript).

"The level of enthusiasm among developers for BlackBerry 10 is amazing. The platform has been built to give developers the ability to create amazing content and a great user experience. The support and excitement we already see from developers is both rewarding and encouraging," said Martyn Mallick, Vice President, Global Alliances and Business Development at Research In Motion.

Council Fined GBP 70,000 for Losing Highly Sensitive Data

The London Borough of Barnet has been issued with a penalty of GBP 70,000 for losing paper records containing highly sensitive and confidential information, including the names, addresses, dates of birth and details of the sexual activities of 15 vulnerable children or young people.

The loss occurred when a social worker took the paper records home to work on them out of hours. The social worker's home was burgled in April last year, and a laptop bag, containing the records and an encrypted computer, was stolen.

Simon Entwisle, the ICO's Director of Operations, said: "The potential for damage and distress in this case is obvious. It is therefore extremely disappointing the council had not put in place sufficient measures in time to avoid this second loss."
Biometrics for Civil ID

By Chris Trytten, Director, Developer Product Marketing at DigitalPersona, Inc.

In emerging countries across the world, Civil ID programs are taking shape. For these countries, growth, prosperity and political stability depend on providing burgeoning populations with access to basic services, such as pensions, entitlements, education, banking, as well as secure voting systems. Unlike developed countries, emerging nations often lack an identity infrastructure, making it imperative that identifying and authenticating an individual be easy and resistant to fraud. Because other forms of identity such as personal identification numbers (PINs) or identity cards can be faked, shared, lost or stolen, they are less desirable, as they are susceptible to rampant fraud.

When looking for Civil ID solutions, governments of emerging countries face two critical questions. First, how do you establish citizen identity for whole populations? Second, once identity is established, how do you ensure citizens requesting services are who they say they are, and are therefore entitled to access a service? Fingerprint biometrics has quickly become a key part of establishing and authenticating identity.

Biometrics and National Elections

For emerging countries, enrolling citizens to enforce a one-person, one-vote system is of supreme importance. Without this basic guarantee of fairness, election results are rejected more often than not, resulting in civil unrest. There are an increasing number of instances where fingerprint biometrics has had a transformational impact on the electoral process.

Fingerprint biometrics has had a positive impact on the Nigerian election process. Though Nigeria became a democracy through a presidential election in 1999, balloting remained challenged by voting irregularities. Voter registration lists, developed over the last decade, were full of names of dead and fictitious people. Precincts that had few voters sometimes were reporting a 100 percent turnout in highly-contested local elections. To avoid a repeat, in the weeks and months leading up to Nigeria’s April 2011 elections, the Independent National Electoral Commission (INEC) conducted a program to register all eligible citizens in Africa’s most populous country.

To do so, INEC put out a bid for 132,000 Direct Data Capture (DDC) machines using fingerprint sensors to support voter registration. With the solutions in place, INEC of Nigeria embarked on an ambitious voter registration program. On January 15, 2011, INEC began registering all of its voters for the April general election, making it the first voter registration initiative of this scale and sophistication. All told, 73 million voters across the 36 states and Abuja were successfully registered in time for the election, and the election was deemed a success by previously critical independent observers. Key to this effort was establishing and verifying identity, quickly and simply, through fingerprint biometrics.

Setting the Stage for the Future of Nations

Biometrics is a portable identity for citizens that can be reused in many other programs in both the public and private sectors. Delivering services such as entitlements, banking and voting brings points-of-service access to rural populations in a cost-effective, reliable and secure way. Many countries are now fingerprinting their entire population in anticipation of using biometric databases for a wide range of civil and commercial programs.

DigitalPersona is exhibiting at Infosecurity Europe 2012, the No. 1 industry event in Europe held on 24th – 26th April 2012 at the prestigious venue of Earl's Court, London. The event provides an unrivalled free education programme, exhibitors showcasing new and emerging technologies and offering practical and professional expertise. For further information please visit www.infosec.co.uk

About DigitalPersona

DigitalPersona, Inc. is a global provider of strong authentication and access management solutions that close the gap between people and security for enterprises, government agencies and commercial embedded-solution developers. DigitalPersona's authentication and access management software is shipped by computer manufacturers on millions of notebooks and desktop computers per year;
its cloud- and Active Directory-managed solutions multi-factor/strong authentication, single sign-on (SSO) password management and emergency access recovery simplify compliance and cut IT costs. The company’s fingerprint biometrics technology helps organisations prevent fraud and increase accountability; it is incorporated into multiple national voting systems, almost all brands of biometrically-enabled point-of-sale (POS) stations, as well as many commercial applications in the retail, healthcare, and financial industries. For more information contact DigitalPersona, Inc. at: +1 650.474.4000, or visit www.digitalpersona.com.

World News In Brief

Gemalto Signs Multi-Year Contract with the UK DVLA

Gemalto announced that it has been selected by the Driver and Vehicle Licensing Agency (DVLA) to supply in the range of 40 to 80 million secure Sealys documents for a variety of official permits. These include in particular digital tachograph cards, the next generation of highly-secure polycarbonate driver’s licenses, and biometric residence permits, in a multi-year contract. The DVLA will begin deploying the products in 2013 using Gemalto’s EU-compliant eco-friendly Sealys polycarbonate portfolio of secure documents, fitted with unique security features such as Sealys Edge Sealer, a feature unique in the market comprising a laser engraving process applied during the production stage to the edge of the polycarbonate document, adding an additional layer of security.

Furthermore laser-engraved images will be digitally enhanced to include an additional visible security pattern, which prevents modification of the photo without leaving visible marks.

The move by the United Kingdom’s Driver and Vehicle Licensing Agency is in keeping with the European Commission initiative to create a standard format driver’s license across the European Union, made of high quality polycarbonate documents with high level security features. The agreement has been entered into with Gemalto UK Ltd., the Fareham based central hub for Gemalto in the UK, which is in charge of managing the entire project. Gemalto will also be working closely with the DVLA to enable the personalisation of the products directly by the DVLA.

More Than 1 In 4 Mobile Users in the US and Western Europe Will Pay In-Store Using NFC By 2017

A new report from Juniper Research has found that more than 1 in 4 US and Western European mobile phone users will use their NFC-enabled mobile phone to pay for goods in-store by 2017, compared with less than 2% in 2012. Worldwide, more and more NFC payment pilots are being launched and transitioning to full commercial service being spearheaded by both mobile network operators and financial institutions.

The report found that, while mobile retail payment services of all types are growing in popularity, the ability to "tap" an NFC phone against a POS terminal to make a purchase has tremendous user appeal. For mobile wallet providers and partners, NFC payments also provide new and personalised retail marketing and sales opportunities above and beyond the capabilities of debit or credit cards. NFC payments can also integrate with other NFC applications, such as metro ticketing.

The report warns, however, that NFC retail payments services must be deployed with a fully integrated and tested customer care channel. NFC payments are a complex fusion of mobile, financial and retail technology; a single point of contact to take responsibility for resolving a problem quickly and efficiently must be established or users will desert the service.

According to report co-author Dr Windsor Holden, "NFC retail payments are still at an early stage, but hold great promise. In 2011 we saw significant strides made within the ecosystem such as the launch of Google Wallet, the announcements of more mobile wallet consortia and the supply of an increasing number of NFC-enabled smartphone models. NFC is now impacting the public consciousness and we expect a rapid market expansion from 2012 onwards."
Fujitsu Develops World's Smallest and Slimmest Palm Vein Biometric Authentication Sensor

Fujitsu Laboratories Limited announces the development of the world's smallest and slimmest palm vein authentication sensor that is capable of being employed in tablet devices. By upgrading the technology's design with new image sensors and other optical components, Fujitsu Laboratories has successfully slimmed down the new sensor to a thickness of 5 mm.

The new sensor preserves the same authentication performance as existing technology while halving thickness of current models. This also enables easy deployment to mobile devices, such as tablets and slate PCs, which are becoming increasingly slimmer, and helps to expand the range of applications for palm vein authentication. More customers will now be able to perform secure authentication using simple operations.

Fujitsu Laboratories has developed a biometric authentication technology based on the vein patterns in a user's palm. This approach has a number of advantages that are unique even among biometric authentication technologies, including high authentication accuracy and the measurement of data from inside of the body, which makes it difficult to falsify.

G&D Announces MobiCore Integrated Security Platform to Support Samsung GALAXY S III in Europe

Giesecke & Devrient (G&D) has announced that its MobiCore security platform will be integrated in Samsung GALAXY S III smartphones distributed in Europe.

Thanks to MobiCore, the NFC-capable smartphone from Samsung will be the first mobile device to boast a protected area on its application processor in which security-sensitive applications can be securely run and downloaded dynamically.

The MobiCore platform will provide a secure execution environment for mobile payments authentication, emails or corporate VPN access. The first application installed in the Mobicore-protected area on the Samsung GALAXY S III is a digital rights management (DRM) application which provides digital content with effective protection against misuse.

In addition, G&D's Trusted Service Management (TSM) solution will enable organisations such as network operators and banks to install and customise additional security-critical apps in the protected area of the smartphone. Samsung GALAXY S III, with integrated MobiCore security platform, will be made commercially available first in Europe and will then be rolled out globally.

Arcontia Wins Tender for Online Smartcard Reload Terminals

Arcontia Technology AB has won an e-ticketing tender for pick-up devices to be used by Norwegian public transport authority Ruter AS in their e-ticketing system.

The contract includes compact ARC3300T5 smart card terminals for reloading Mifare DESFire travel cards via the new online national order database. To expand current distribution channels and increasing Internet sales, Ruter will be launching a complete online sales solution.

ARC3300T5 terminals will be connected online with the national order database, securing fast and dependable order retrieval directly from the database to the card.

For increased flexibility and accessibility, the terminals will be placed throughout the city of Oslo and Akershus County, encouraging the use of smart cards in public transport and improving the customer experience by making travelling more convenient.

Hackers Steal $90,000 in Bitcoins

Bitcoinica this month suspended operations after a security breach compromised its servers enabling hackers to steal 18,547 Bitcoins valued at approx. $90,000.

Bitcoin is a digital currency that enables instant payments to anyone, anywhere in the world. Bitcoin uses peer-to-peer technology to operate with no central authority. Managing transactions and issuing money are carried out collectively by the network.

This follows the previous hack in March when hackers made off with $71,000 in Bitcoins after compromising web host Linode.

Bitcoinica confirmed that the stolen Bitcoins belonged to the exchange and not the users, saying it will honour any withdrawal request. At this time it is not clear when the website will resume operations.
Consigned to History by the Smartphone

Steve Watts, Co-founder of SecurEnvoy

It might seem hard to believe but the mobile phone was first introduced to the UK in 1985. Just twenty seven years later and the device that we now love is hardly recognisable to those first Motorola handsets. And it’s not just the size and battery life that’s changed. Let’s face it, if you were to upgrade your handset tomorrow, would you just be looking for one that can make calls!

Steve Watts

Considered the top executive toy, the mobile phone became the status symbol of the Yuppie - short for "young urban professional" or "young upwardly mobile professional". Today, with more handsets than people on the planet, it’s changing more than the way we communicate, but consigning some parts of every day life to the history books.

Making calls: It’s almost easy to forget, especially with increasing functionality, but the primary reason for having a mobile phone is for making and receiving phone calls. Spare a thought then for the humble phone box. Last year, BT announced that almost a quarter of phone boxes in Wales were making less than one call a month! Apparently, at that time, only 3% of adults across the UK used a payphone.

Sending letters: Many contracts and PAYG packages include a text bundle. You only have to travel on a train or bus and you’ll witness people busily tapping away on their phones. It is this phenomenon that the Hooper Report gives as a primary argument for the privatisation of Royal Mail.

Fax machine: With many completely ignorant to its predecessor – the telex, the fax machine is also close to becoming obsolete. While it’s true that email is the greater villain, the fact that many phones offer the ability to scan (via their cameras) and send as an email attachment means, in my book, that they’re hardly blame free!

Cameras: Speaking of cameras, how many megapixels is your handset capable of? While digital cameras obliterated film cameras, they are now facing their own nemesis. With the iPhone reportedly more sophisticated than traditional compact cameras, and it’s not the only device to boast superior resolution, it’s hardly surprising that both these and video cameras are on their way into the nearest museum.

Music: Hands up if you remember the walkman! For those of you too young to know, these were portable cassette players. Of course, there was also the boom box blasting out in the park way back when on a warm summer’s day. With even the most basic smartphone capable of storing the entire Elvis back catalogue without even flinching, and playback that most dream of, you too can have music wherever you go.

TV: As screens become bigger, with better resolution, it is now possible to watch your favourite programmes when out and about. That said, I don’t think the HD TV has too much to fear just yet – but perhaps the set top box suppliers may need to watch their backs.

Games Console: Video games consoles have been in decline for a few months with many experts blaming the trend on the increased popularity of casual mobile gaming. While IDC is hopeful the end is not yet sealed, the fact that a major high street gaming retailer only just managed a stay of execution suggests its days could be numbered.

Signature: Mobile phones are becoming so integral to everyday life, they’re capable of confirming our identities. This could mean, one day, we’ll no longer need to sign for things. For example, two factor authentication (2FA) combines something you know, with something you have – an existing example of 2FA in action is ‘chip and pin’ for authorising credit and debit card payments. When accessing corporate networks, completing financial transactions, etc. mobiles offer the perfect tokenless 2FA solution. A passcode is received as an SMS, which you then key in to confirm your identity.
**Tracking device:** Of course, with GPS functionality, it’s hardly surprising mobiles are replacing maps, satellite navigation specific devices and telephone books. You can use them to pinpoint your position if you’re not entirely sure where you are, while services offer to send you numbers based on your location, for example taxi firms or curry houses. But, perhaps rather controversially, you can now download an app for an iPhone, iPad or iPod touch that allows you to track your friends. While handy for checking your child is at school, partner at the office, or how far away your mate is when you’re waiting for them, I’m not sure how comfortable I would be that someone could locate me at their will and not mine.

**Banking:** Today, you can practically carry your high street branch on your handset. Natwest and Barclays are just two that offer mobile banking apps that allow you to make payments, transfer money between accounts, check your balance and view recent transactions.

**Money:** And its not just banking you can do with your phone – you can also carry cash. While not quite consigned to history, could the smartphone be eyeing up the credit card or even physical change as its next casualty? For some time now people have been able to pay for things, such as make charity donations or pay for parking in car parks, but that’s almost immature when compared to Barclays Pingit. It’s the first mobile app to launch in the UK that allows payments of between £1 and £300 to be made. While the jury is still out as to whether it’s secure enough, or will even prove popular, I’m sure Dr Martin Cooper never imagined it would be possible when he invented the first practical mobile phone.

I’m sure you’ll agree, your smartphone is so much more than just a way to talk to people – you’re practically carrying your life on it. If you lose it, how devastated would you be? For organisations the risk is too awful to contemplate and for that reason many are adding encryption to prevent any information on the device being stolen. Perhaps its time we all follow their lead and take pre-emptive action to protect these modern miracles. SecurEnvoy offer SMS passcodes, the equivalent to a chubb lock, so only you can access all your important information, so it remains secure from prying eyes.

Love it or loath it the smartphone has completely revolutionised our lives. And our living rooms, bedrooms, offices, cars ... The question on my mind is, in the next twenty five years, will there by anything smarter than the smartphone or will it have taken over the world - cue villainous laughter and white cat stroking.

---

**World News In Brief**

**E-commerce will Help Sustain Healthy Growth of Merchant Acquiring in Europe**

26.1 billion card payments worth 1.5 trillion-Euros were acquired in Europe’s six largest cards markets in 2010. The UK and France are the largest such markets by a wide margin. Together, they account for more 65% of the volume, and 72% of the value, of card payments acquired in the six countries. These are among the findings of Merchant Acquiring in Europe 2012, recently published by RBR (http://www.rbrlondon.com).

The study, which covers Germany, Italy, Spain and Turkey as well as France and the UK, shows that the merchant acquiring market is often highly concentrated. In five of the six countries covered, the top four acquirers account for over 50% of the acquired value of card payments, and there are signs the market will concentrate yet further.

Moreover, there is a trend towards greater outsourcing of non-core activities so acquirers are likely to become more specialised in the future.

**New Protocol Enables Wireless and Secure Biometric Acquisition with Web Services**

Researchers at the National Institute of Standards and Technology (NIST) have developed and published a new protocol for communicating with biometric sensors over wired and wireless networks-using some of the same technologies that underpin the web.

The new protocol, called WS-Biometric Devices (WS-BD), allows desktops, laptops, tablets and smartphones to access sensors that capture biometric data such as fingerprints, iris images and face images using web services. Web services themselves are not new; for example, video-on-demand services use web services to stream videos to mobile devices and televisions.
The WS-Biometric Devices protocol will greatly simplify setting up and maintaining secure biometric systems for verifying identity because such biometric systems will be easier to assemble with interoperable components compared to current biometrics systems that generally have proprietary device-specific drivers and cables.

WS-BD enables interoperability by adding a device-independent web-services layer in the communication protocol between biometric devices and systems.

**New SIM Card Format for Slimmer, Smaller Phones**

At its 55th meeting held on 31 May and 1 June 2012 in Osaka, Japan, ETSI's Smart Card Platform Technical Committee agreed a new form factor for the UICC, popularly known as the SIM card.

Today's SIM card designs take up a significant amount of space inside a mobile device. This space is more and more valuable in today's handsets which deliver an ever increasing number of features.

The fourth form factor (4FF) card will be 40% smaller than the current smallest SIM card design, at 12.3mm wide by 8.8mm high, and 0.67mm thick. It can be packaged and distributed in a way that is backwards compatible with existing SIM card designs. The new design will offer the same functionality as all current SIM cards.

The SIM is the most successful smart card application ever. A SIM card is used to securely associate a mobile device with a customer account, preventing fraud and ensuring that calls are correctly routed to customers. It is an essential security feature of mobile networks, and is integrated into every GSM, UMTS and LTE device.

Over 25 billion SIM card and derivatives have been produced so far, and the industry continues to issue over 4.5 billion SIM cards each year. The new form factor was adopted by industry with the involvement of major mobile network operators, smart card suppliers and mobile device manufacturers. The new design will be published in due course in ETSI's TS 102 221 specification, freely available like all ETSI standards from the ETSI website.

**Develop Applications for the Next Generation of Business Mobility**

The BYOD (bring your own device) phenomenon has added to the confusion, complexity and cost of developing multiple versions of the same application for different operating systems. The new award-winning RhoMobile Suite from Motorola Solutions, Inc. is a true HTML5 cross-platform development framework that allows developers to write an application once and have it look and act the same on different mobile devices regardless of the current operating system (OS). This new technology will reduce operating expenses by virtually future-proofing applications that will continue to run and perform on current and next generation enterprise and consumer devices.

**Post Office Becomes the Biggest Acceptor of Contactless Payment in Europe**

Post Office Limited is leading the way in payment technology with the announcement that it is to roll out contactless payment terminals across 30,000 counter positions in its unrivalled network of over 11,500 branches. The move makes the Post Office the biggest user of contactless acceptance technology in Europe allowing customers to pay for transactions using contactless cards and NFC equipped mobile phones.

The roll out starts on the 6th June in almost two hundred branches around the various Olympic sites and is expected to be completed by the end of October 2012. It is the largest deployment of contactless technology in Europe and is expected to increase consumer awareness and usage and, through the Post Office network, put this technology within three miles of 99% of the UK population.

Lesley Sewell, Chief Information Officer, Post Office Limited, said: "We are delighted to be delivering cutting edge technology through the Post Office network. Contactless will bring huge benefits to our customers by increasing choice and reducing transaction times. Over the next few years, many Post Office branches will be transformed, becoming more customer focused, opening for longer and providing services in a convenient and efficient manner."

**Biometric Security for SAP**

SecuGen is pleased to announce the availability of biometric identity management and fraud prevention for SAP (Systems Applications and Products) system users with the combination of SecuGen Hamster Plus and Hamster IV fingerprint readers and bioLock software from realtime North America Inc.
SecuGen fingerprint scanners are fully compatible with bioLock software, which gives SAP users biometric control of sensitive system activities at granular levels. Biometric credentials can be re-authenticated when users request restricted information or perform mission-critical activities, using a SecuGen Hamster series reader combined with bioLock software. Passwords become irrelevant and are replaced with robust biometric control. This enhances governance, regulatory compliance and strictly enforces Segregation of Duties (SoD) procedures.

The Hamster Plus and Hamster IV feature Auto-On, an Automatic Finger Placement Detection technology that checks for the presence of a finger without prompting, thus improving speed significantly. Recognition of difficult fingerprints, such as dry, wet, scarred or aged skin, has been enhanced with Smart Capture, which adjusts brightness to adjust for such conditions.

London NHS Trust Fined for Serious Data Breach

Central London Community Healthcare (CLCH) NHS Trust has been fined GBP 90,000 following a serious breach of the Data Protection Act (DPA), the Information Commissioner's Office (ICO) announced yesterday.

The breach first occurred in March last year, after patient lists from the Pembridge Palliative Care Unit, intended for St John's Hospice, were faxed to the wrong recipient. The individual informed the Trust in June that they had been receiving the patient lists - around 45 faxes over a three month period - but had shredded them.

The patient lists contained sensitive personal data relating to 59 individuals, including medical diagnoses and information relating to their domestic situations and resuscitation instructions.

Stephen Eckersley, the ICO's Head of Enforcement said: "Patients rely on the NHS to keep their details safe. In this case Central London Community Healthcare NHS Trust failed to keep their patients sensitive information secure. The fact that this information was sent to the wrong recipient for three months without anyone noticing, makes this case all the more worrying."

DigitalPersona Delivers Facial Recognition Technology for User Authentication

DigitalPersona, Inc. announced the latest release of DigitalPersona Pro Enterprise software.

The latest release builds upon its existing support for a wide variety of user authentication methods by including facial recognition technology. DigitalPersona Pro Enterprise also delivers expanded browser support, improved multi-credential support and support for kiosk shared accounts. These enhancements address the need for flexible, scalable and cost-effective user authentication and access control in healthcare, financial services and government installations.

"Businesses are under immense pressure to control and manage user access to critical applications and information. However, many authentication solutions can be difficult to deploy and use, impacting employee productivity and driving up IT costs," said Kavya Muthanna, director of enterprise product management at DigitalPersona.

HID Increase Security at Major Power Plant in China

HID Global announces that the company's network access control solutions and contactless readers have been deployed at the Fuxi power plant in China's Sichuan province. The new system provides increased security that ensures the operational safety of production and facility areas, offers real-time monitoring at the central station and enables security administrators to remotely close facility doors for improved safety management.

HID Global's VertX V2000 network access controllers, iCLASS R10 contactless readers and Genuine HIDO credentials were installed at the 141 acre (57 hectare) Fuxi power plant, enabling administrators to restrict staff access levels and entry times based on job titles and critical entry zones, such as the main production plant, engine room, central station and chemical waste areas. With the new system, access to the chemical waste area is restricted to authorised staff, and administrators can now establish access rights to prevent unauthorised entry and ensure occupational safety. Additionally, iCLASS readers provide data encryption and mutual authentication capabilities, significantly increasing the plant's security.
Financial services technology meets the world of apps

How is new technology disrupting the financial services market? How can providers compete and differentiate in this turbulent environment? Maria Nottingham, Chief Marketing Officer at Compass Plus explains how an application model can translate to financial services and the benefits of adopting this model for a variety of providers.

Market transformation

Today’s mobile, socially-oriented, and loyalty-reluctant customers are demanding new services that need to be available all the time via any channel. If they aren’t served by their current provider then they are voting with their feet.

This shift in consumer expectation in the financial services market has led to a state of upheaval. There are two trends that are intertwined - the rapid introduction of new technology and the entrance of a variety of non-traditional financial service players into an already crowded market.

There has never been such a concerted and proliferated explosion of new technology-led payment solutions. Technology is providing consumers with a range of new and compelling ways to make payments and manage their money; Internet and mobile banking, peer-to-peer (P2P) payments, contactless and near field communications (NFC) payments, to name but a few. New players such as mobile operators, retailers and Internet companies are predominantly leading this technology disruption. These companies are now vying for a slice of the customer wallet by taking advantage of this shift in expectations.

A number of recent announcements regarding the entrance of new players and the launch of new services by both non-traditional and traditional players have brought the above trends into focus, for example:

- **Non-traditional financial institution: Virgin Money** – Virgin Money entered the UK in January 2012. Already established in Australia, South Africa and the USA, Virgin claims to offer innovative products and increase focus on customer centricity in the retail banking scene.

- **Retail-led service: Starbucks Mobile Payments** – In January 2011, Starbucks launched an app to pay for in-store purchases in the US. One year on, it announced that the company has processed 42 million mobile payments since its inception.

- **Traditional banking service: Barclays Ping-It** – Barclays launched the smartphone application, Ping-It, in February 2012 in the UK, enabling users to transfer money by using only a mobile phone number.

The challenges

Consumers want it all. As technology advances and we see the proliferation of smartphones, tablets, social media outlets, the everyday consumer wants to access, manage and transact anywhere, anytime via any channel. To accommodate these trends, innovation in financial services is a must. However, in July 2011, a survey conducted by marketing research firm Brand Keys found that consumers make no differentiation between bank brands.4 According to its research, banks are not engaging their customers and do not offer products and services that really make them stand out from the pack.
Of course a few traditional service providers like Barclays with its Ping-It service are already innovating to differentiate. In a market that lacks differentiation, even a small leap is sure to make a big difference. Contactless cards, virtual currencies, Internet and mobile banking are all examples of recent developments that have been made in line with consumer demands. However, the shelf life of innovation is short lived; as more and more markets adopt said innovations, they quickly become standard and consumers move on to the ‘next best thing’.

It’s not just consumers that are driving this market transformation. Greater legislation and regulation from local and international bodies - SEPA, PCI, and card issuer mandates combine to create an environment of constant change which requires financial institutions to make significant investment just to stay compliant. It may be especially cumbersome to the new market entrants who are effectively deploying ‘Greenfield’ financial systems to make sure that they not only stay one step ahead of the traditional players but ensure their services adhere to strict financial regulations and other areas of compliance and governance. When dealing with people’s money, trust is critical and one mistake in terms of security can destroy not only a service but a brand.

Furthermore, reduced margins, loss of profit and shrinking revenue across retail banking, card issuing and acquiring, and merchant business - are driving the need to rationalise, improve performance and consolidate operations whilst creating new revenue streams and achieving better profitability.

Most traditional financial institutions also face an additional hurdle; they are bound by siloed legacy systems and ‘islands’ of in-house development that do not deliver a technology platform for innovation. This begs the question: How can financial service providers customise their platforms quickly, easily and cost-effectively to unlock the potential opportunities that new market dynamics offer?

Last year the analyst house Tower Group reinforced these challenges: “The [financial services] business model will face disruptive, often unwelcome change in every major market...technology will be essential to the success of industry operators seeking profitability after three years of high credit losses, hyperactive regulators, and general economic stress.”

**Enter the application model**

To drive innovation and meet consumer, business and regulatory demands, the industry needs to change; for the industry to change the systems need to change first. An application model is the answer for both traditional and non-traditional financial service providers looking to deliver innovation in the long term. Successful in both the IT and mobile markets, an application model has the potential to revolutionise the financial services market by accelerating the development of products that will provide on-going customer value.

The business-to-consumer application model in IT and mobile markets works like this: there is a platform, say Windows in IT or iOS in the mobile space. Sitting on this platform are applications such as Adobe Reader on Windows or Evernote on iOS. These applications can be created by the platform designers themselves or by third party developers. The model has three tiers – the platform on which the app is created, the app itself, and finally the device with which it is accessed.

The financial services (business-to-business) application model also has multiple tiers and though it has similar underlying principles to the business-to-consumer model, it also has additional elements to consider. One of these major elements is that within this model, the application delivered by the technology vendor – the Adobe Reader application if we revert to the IT model analogy – is customised, branded and turned into a specific financial product or service by the financial service provider; this product or service is then delivered to the consumer.
To enable an application model in financial services, the service provider would need to approach a technology vendor that provides an open application development platform (OADP). These platforms provide a truly open environment that delivers the tools for the development of a diverse range of applications on a single platform. Effectively they allow financial service providers to choose well designed, pre-tested applications from proven vendors built either by external developers or by the vendor themselves. These applications can then be used to launch financial products and services.

All OADPs are structured to offer application developers a full set of sophisticated development tools: builders, designers, editors, debuggers etc. To ensure services remain secure and comply with the relevant regulations, the platform is designed in such a way that all applications comply with the latest mandates and standards, shifting the responsibility for ongoing updates away from the service provider to the technology vendor, yet ensuring the retention of user modifications in the course of applying vendor-supplied updates to the base application software code.

Depending on the OADP used to build the applications, the application model can be taken to the next level to deliver flexibility to the financial service provider by making the above mentioned tools available to both application developers and their users. This would provide an unmatched foundation for professional collaboration between both parties for further application improvement and development.

**Key advantages of the application approach**

The financial services application model supported by a technology vendor can offer service providers the following advantages:

- **Expertise & experience** – The combined knowledge of a network of app developers and technology partners will help the financial service providers offer cutting-edge services.
- **Choice** – Providers can source a variety of applications from the technology vendor who will develop their own applications as well as work with external developers.
- **Unity** – By working with a technology vendor, financial service providers can unify disparate applications on a single platform.
- **Economies of scale** – In the long term, increased competition between app developers will drive down costs and speed up development.
- **Speed** – Accelerated speed of development and the introduction of new services into the market.

**A new model for a new market**

The application model, enabled by OADPs, has the potential to revolutionise the financial services industry. The model removes the burden of developing and maintaining proprietary IT systems so that the financial service providers can concentrate on business innovation. It allows them to quickly and efficiently launch new services, enabling them to compete with existing and new competitors by addressing the demands of the mobile, socially-oriented, technology-wise and loyalty-reluctant customer of today. The model can also help optimise operations and improve performance, in addition to ensuring compliance with the latest regulatory and security mandates whilst remaining at the frontier of innovation.

The market is fast-paced and becoming increasingly turbulent. The financial services application model, if adopted, could open up a world of applications for the rapid delivery of innovative services that meet the needs of consumers today, and into the future.
MasterCard Simplifies Shopping with Launch of PayPass Wallet Services

MasterCard announce PayPass Wallet Services, a new global offering for banks, merchants and partners that will make it faster and easier for their customers to make purchases in stores or online by allowing them to securely pay with a simple click of the mouse, touch of the tablet screen or tap of the smartphone.

PayPass Wallet Services delivers three distinct components - PayPass Acceptance Network (PayPass Online and PayPass Contactless), PayPass Wallet and PayPass API. These services enable a consistent shopping experience no matter where and how consumers shop, as well as a suite of digital wallet services, and developer tools to make it easier to connect other wallets into the PayPass Online acceptance network.

MasterCard will make PayPass Wallet Services available to partners in the third quarter of 2012, initially in the U.S., Canada, U.K. and Australia and, subsequently, will include other countries. PayPass Wallet Services will be expanded to the point of sale over time to create an end-to-end shopping experience for consumers providing additional value-added services such as: at-a-glance account information before making a purchase; spending controls and alerts received in real time; and delivery of targeted offers, coupons and enhanced loyalty programs.

"Consumers are looking to pay for goods when, how and where they choose. Merchants want flexibility to easily accept digital payments so they can convert more browsers to buyers both online and in store," said Ed McLaughlin, chief emerging payments officer, MasterCard. "We realize that when it comes to payments, no single wallet will rule them all. PayPass Wallet Services simplifies the shopping experience while providing flexibility and choice to merchants, banks and consumers."

Samsung and Visa Showcase mPayments at the London 2012 Olympic and Paralympic games

Samsung Electronics and Visa announced that Samsung GALAXY S III, the latest in smartphone innovation, will be Samsung's Olympic Games Phone during the London 2012 Games.

A limited edition showcase device enabled with Visa's mobile payment application, Visa payWave, will be available for Samsung and Visa sponsored athletes and trialists, making it possible to buy merchandise with a wave of the device at thousands of retail locations throughout London.

"Mobile payment services enabled by NFC technology are gaining momentum around the world. The Samsung GALAXY S III has been created with our human needs and capabilities in mind and is the ideal device to showcase the ease and convenience of Visa's mobile payment application at the London 2012 Olympic Games," said DJ Lee, Executive Vice President and Head of Sales and Marketing team of Samsung's Mobile Communications Business.

By the time of the Olympic Games there will be more than 140,000 contactless terminals around the U.K. From the moment visitors land at Heathrow they will be immersed in a contactless payment experience with everything from taxis, to retail outlets, to the Olympic Park itself.

NXP Powers NFC in the Samsung GALAXY S III

Today, NXP Semiconductors N.V. announced that its PN65 Mobile Transactions solution will power the Samsung GALAXY S III bringing a new concept of human-centric mobile experience.

Powered by Google's Android 4.0 Ice Cream Sandwich operating system, the powerful Samsung GALAXY S III supports secure NFC applications, such as wallets being launched by mobile network operators, card associations and others such as Google's Wallet. Additionally NXP's award winning PN65 delivers best in class performance and seamless interoperability with various mobile use cases such as payment, transportation, access control and NFC tag reading largely based on NXP's contactless reader IC technology.

"We are in the midst of a golden era of mobile and Samsung continues to set the bar with coveted products like the GALAXY S III," said Henri Ardevol, vice president and general manager, secure transactions with NXP Semiconductors. "Samsung's flagship phones require flagship-worthy NFC solutions and NXP is proud to support Samsung on its GALAXY S line. We eagerly look forward to the extraordinary mobile experiences the GALAXY S III will deliver including those enabled by NFC."
Over 4 Million-Pounds of Counterfeit Coins Recovered

A record GBP 4.1 million in counterfeit coins has been recovered by detectives from the Metropolitan Police Service's Projects Team following a proactive operation. The seizure is thought to be the biggest recovery of counterfeit coins within the UK.

The money was seized on Wednesday, 23 May from three properties in Enfield, Herts and Essex; and two vehicles in the Essex area.

An estimated 4 million-Pounds worth of blank coins were discovered within a 40ft freight container; and a further 107,000 Pounds in counterfeit coins were also found.

Three men - aged 52, 43 and 27 - have been arrested in connection with the investigation and are currently being held at a north London police station on suspicion of offences such as production of counterfeit monies, money laundering and fraud.

E-commerce will Help Sustain Healthy Growth of Merchant Acquiring in Europe

26.1 billion card payments worth 1.5 trillion-Euros were acquired in Europe's six largest cards markets in 2010. The UK and France are the largest such markets by a wide margin. Together, they account for more 65% of the volume, and 72% of the value, of card payments acquired in the six countries. These are among the findings of Merchant Acquiring in Europe 2012, recently published by RBR (http://www.rbrlondon.com).

The study, which covers Germany, Italy, Spain and Turkey as well as France and the UK, shows that the merchant acquiring market is often highly concentrated. In five of the six countries covered, the top four acquirers account for over 50% of the acquired value of card payments, and there are signs the market will concentrate yet further. Moreover, there is a trend towards greater outsourcing of non-core activities so acquirers are likely to become more specialised in the future.

Metropolitan Police Roll-out Mobile Fingerprint Scanners

On Wednesday 23rd May Mobile Identification [MobileID] went live across the force as part of the Commissioner's commitment to make better use of technology to fight crime and is part of a nationwide roll out of the device led by the National Policing Improvement Agency [NPIA].

The MobileID is about the size of a mobile phone and allows police to read the fingerprint of an index finger. It checks the fingerprints with the national database but does not retain them afterwards. The device will be used in instances where an individual is suspected of committing an offence, or wanted for a previous offence.

In total, 350 devices will be deployed across the Metropolitan Police Service over the next month. Other units including the Territorial Support Group, Traffic and Safer Transport Command will also have MobileID capability.

Precise Biometrics Kicks Off Global Launch of Tactivo for iPhone and iPad

Precise Biometrics’ product for mobile security for smartphones and tablets, Tactivo, has now been certified by Apple. The first delivery of Tactivo for iPhone has already arrived from the company’s new production partner, Flextronics, in the United States. Precise Biometrics estimates that the first orders for Tactivo will come during the summer 2012.

Tactivo is a smart casing for tablets and smartphones that includes an embedded fingerprint and smart card reader. Together with different types of apps, Tactivo enables government agencies and companies to maintain a high level of security when employees use mobile units to access sensitive information.

The first generation of Tactivo is being launched for iPhone 4S and iPhone 4. Apple has now certified Tactivo in its Made For iPhone (MFi) Program. Precise Biometrics will also be launching Tactivo for iPad after the summer.

PayPal Taps ShopKeep POS for In-Store Payments

With the launch of the PayPal partnership, nearly 2,000 merchants nationwide who use ShopKeep POS can now accept PayPal cardless payments.
The process is simple -- PayPal customers check-in at participating merchants with their PayPal iPhone app. At checkout, the customer’s name and photo will appear on the ShopKeep POS iPad register. The cashier identifies the customer and finalises the transaction. Once the transaction is complete, the customer is automatically checked out of the store and receives an email receipt of the transaction.

Merchants in New York City and Boston have already started accepting PayPal mobile payments as part of the ShopKeep POS / PayPal east coast pilot program.

Everything Everywhere and Stagecoach Partner to Transform Public Transport Ticketing

Transport operator Stagecoach Group and Everything Everywhere announce plans to transform the way consumers use tickets to travel on public transport.

The two companies have unveiled the UK’s first Government-standard commercial deployment of mobile contactless transport ticketing, which could lead to a nationwide roll out across select bus and rail services in 2013.

The trial, already underway on the Stagecoach bus network in Cambridgeshire, enables a small cross section of bus users to receive, store and validate their bus tickets using their mobile phone. Everything Everywhere is providing each customer in the trial with a Quick Tap enabled mobile handset. The trial uses the Department of Transport’s preferred ITSO (Integrated Transport Smartcard Organisation) smart ticketing technology, and will monitor the levels of customer convenience the Quick Tap service provides. The trial also contributes to the Government’s vision to deliver, along with transport operators and public sector bodies, the infrastructure to enable most public transport journeys to be undertaken using smart ticketing by December 2014.

Cortus Launches APS3R 32 bit Microcontroller IP Core for Low Energy Embedded Applications

Cortus, a technology leader in ultra low power, silicon efficient 32-bit processor IP, announces the release of the latest member of their processor family: the energy efficient APS3R. The APS3R is a 32-bit processor designed specifically for low power embedded systems featuring a 32-bit modern RISC architecture with sixteen 32-bit registers and a 5-7 stage pipeline.

The APS3R has been developed for applications requiring good computational performance but very low power. It is well suited to applications such as wireless communication, sensing, smart cards, SIM cards, touchscreen controllers and systems using energy harvesting.

MasterCard Loses Appeal Over Fees

Yesterday the General Court in Luxembourg rejected the legal challenge by MasterCard to overturn the European Commission’s 2007 decision over its Multilateral Interchange Fees (MIF’s).

In its judgment the General Court dismissed the action and confirmed the Commissions’ decision.

Multilateral Interchange Fees are a fee paid between banks for the acceptance of card based transactions. In a credit card or debit card transaction, the card-issuing bank in a payment transaction deducts the interchange fee from the amount it pays the acquiring bank that handles a credit or debit card transaction for a merchant. The acquiring bank then pays the merchant the amount of the transaction minus both the interchange fee and an additional fee for the acquiring bank.

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 +44 (0)1903 734677 or email info@smartcard.co.uk, subscription can also be purchased on Amazon by searching for “Smart Card & Identity News”