April 2010

Volume 19 • Number 4

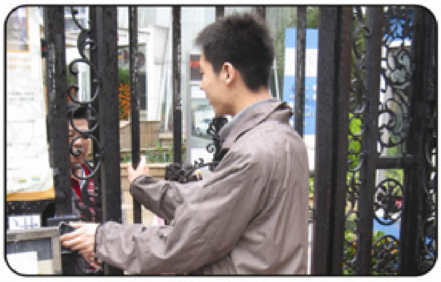
Smart Card & Identity News

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

www.smartcard.co.uk

5 • Trusted Service Managers – Security as a Service

9 • Should our health records be online?



12 • China Mobile halts its 3 Million RF-SIM Cards Production Plan

17 • Trusted eServices in the UK

Apple Set to Dominate Mobile Payments and Ticketing?

Patents are always an interesting way of watching what the big boys are up to. This month a number of patent applications became visible which shows that Apple is clearly doing a lot of research in the mobile payments and ticketing field. For those that have not come across it before there is a whole website devoted to the subject www.patentlyapple.com just for Apple.

Where do we start? Well first of all a lot is happening around NFC for the iPhone. Last month we came across the iCarte 110 NFC Reader for the iPhone.

The advertising spiel tells us that here is the way of making secure contactless payments and downloading coupons, tickets and receipts and just in case we hadn't thought of it for moving data between 2 NFC enabled iPhones. Perhaps we could even make payments between two iPhones?

Now going to the Apple patent web site mentioned previously we immediately walk in to iTravel which is an iPhone application for making travel reservations and downloading the boarding passes etc. This is followed closely by the Concert and Event ticket iPhone application. Just on the same page and not to be ignored are more patents to do with the iTunes on-line virtual store.

Continued on page 4….

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

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

Telephone: +44 (0) 1903 734677

Fax: +44 (0) 1903 734318

Website: www.smartcard.co.uk

Email: info@smartcard.co.uk

Editorial

Managing Director – Patsy Everett

Technical Advisor – Dr David Everett

Production Team - John Owen, Lesley Dann, Suparna Sen

Contributors to this Issue – Chris Shire, Amichai Shulman, Suparna Sen, Tom Tainton, Peter Tomlinson

Photographic Images - Nejron - Dreamstime.com

Printers – Hastings Printing Company Limited, UK

ISSN – 1755-1021

Disclaimer

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

Our Comments

Patsy Everett

Dear Subscribers

Well it's time for another general election in the UK but not perhaps with the same enthusiasm as for a general erection which was overheard at the dinner table with some Japanese colleagues earlier this month. However at such a time ones thoughts are raised into what is happening to all those little projects so close to our heart. The UK national ID card is always top of the agenda and so quite recently, the government still mentions the cards given to foreign migrants but for distribution to the nation as a whole, Mmm… I don't think so.

Just scanning the various election manifestos is always fun, joking really, I don't think I've got the patience but any way those that do such as the London School of Economics (LSE) academics Dr Edgar Whitley and Dr Gus Hosein are happy to tell me that only the Labour Party manifesto has a commitment to deliver ID cards. According to Mark Ballard a fellow journalist The Identity and Passport Service (IPS) is so shady about how they are building the ID cards system that nobody actually knows what's coming or going, if anything that is.

More precisely we are sure that both the conservative party and the Liberal Democrats are on record that they will cancel the national ID card project and a lot that goes with it including the National Identity Register. The LibDems at least have also promised to scrap the next generation of biometric passports that were to include fingerprints. All the current chip passports include a photograph and those of you zooming through Gatwick will have seen the new gates that look at you compared with the picture in the chip. I would have to say that my initial experiences suggest that this works far better than the Iris scan which has been removed and also seems to be more reliable as the old Iris scan gates often seemed to be out of action.

But let's not stop the fun here, how about getting on the buses? Are we going to have anything more than a flash card? A piece of cardboard would be far cheaper here than the latest smart card gizmo. Will ITSO rule the waves and end up as the transport card of choice? Positively running out of breath here but then we have stories that maybe the next government in saving money will have to quash all these travel concessionary cards anyway. That of course would be the end of the buses in anything but the centre of the major cities; rural bus travel would rapidly come to an end because those of you that have tried will know it's made up almost entirely of concessionary fare riders. Somebody once told me that half of them do it just to keep warm and the other half just to have somebody to chat to. On such grounds alone buses provide an essential social service.

You may remember that Michael Leach was appointed interim CEO of ITSO back in February for a couple of months. Can I really believe you would appoint a CEO for a couple of months? I must have got that wrong? Anyway rumour has it that his contract has now been extended for a couple of years so at least there is time to make a mark.

Now what would we like to see him do? I've no doubt if I threw this out for public opinion that the skies would be as misty as ever. However I'll offer a view that may not go down very well but is sadly needed. ITSO is based on backward compatibility; it has been the problem from day one. Whatever you put in place for interoperable fare payments must interoperate with what already exists. If you take this as a starting point it would be OK as long as you had a future migration path into something better, this is what ITSO has never done, concentrating instead on patching the system and floating around to try and optimise integration with the Oyster card scheme in London. In both camps we see a move toward the Mifare DESFire in replacement for the Mifare Classic which has been successfully hacked a few times recently. I've even heard there have been problems with the DESFire cards in that lots of the underground gates can't read the cards correctly. Somebody even told me the other day that the Oyster cards don't even have an expiry date?

So message to ITSO, stop what you are doing and create a realistic 5 year plan for the future and just to give you encouragement remember the banks managed to change from magnetic stripe cards to chip cards not perhaps without problems but as I'm sure everyone will agree to a far better technical solution. Oh and by the way the technologies are not interoperable they do quite different things!

Patsy.

Contents

Regular Features

Industry Articles

Events Diary

May 2010

27-29 Infosecurity Europe 2010, Earls Court, London, UK - http://www.infosec.co.uk/

June 2010

2-4 Debit and Prepaid Conference 2010, Budapest, Hungary

6-8 Mobile Banking and Emerging Applications Summit, Las Vegas, NV, USA - http://www.americanbanker.com/conferences/mobile10/

7-9 Smart Cards + RFID China 2010, Beijing, China - http://www.scsl-china.com/enindex.asp

9-10 European e-Identity Management Conference, Cardinal Place, London - http://www.revolutionevents.plus.com/eema/index.htm

14-16 Prepaid Conference & Expo, London - www.prepaid-conference.com

16-18 Payments Panorama 2010, Vancouver, Canada - http://www.cdnpay.ca/conference/english/homepage.html

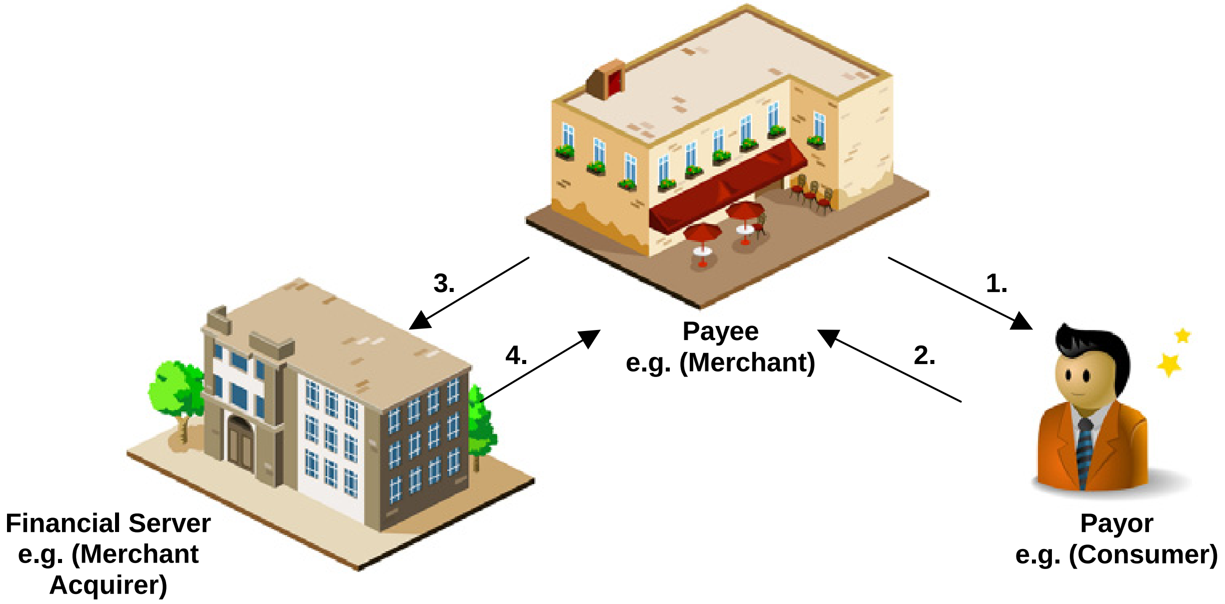
21-22 Contactless Cards & Payments, Marriott Hotel Regents Park, London - http://www.smi-online.co.uk/events/overview.asp?is=8&ref=3407

22-23 Cardware 2010, Ontario, Canada - http://www.actcda.com/calendar.html

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

Apple Set to Dominate Mobile Payments and Ticketing?…. Continued from page 1

Now that's all very well you may say but what's new here? Well we need to add a little more, this month a few more Apple patent applications came to the public's attention. The most interesting one to me was the 'System and Method for Processing Peer-To-Peer Financial Transactions' (US 2010/0078471) part of a set filed by Apple citing Gloria Lin and her co-inventors. Some of the obvious intentions are the handling of conventional credit and debit cards where quite ingeniously the iPhone camera can be used to read the data (using image processing) printed on the surface of the card. However the real interest is in trying to decipher what Apple might really be up to. What is meant by P2P financial transactions because this is the difficult bit with conventional electronic payment schemes? We should also note immediately that it is envisaged that these peer to peer transactions will be based on NFC. So how might this work?



According to the Apple patent it is assumed (as a possible option) that the Payor (i.e. the consumer) has an NFC enabled mobile phone and that the merchant's terminal is also NFC enabled. For a payment transaction the following steps are anticipated,

1. The Merchant sends the payment request message to the consumer's phone using NFC
2. The iPhone sends details of the payment card information to the terminal by NFC
3. The merchant sends the transaction details to his acquirer using the existing protected network connection, who will in turn communicate with the card issuer to get authorization for the transaction
4. The acquirer returns the authorization response to the merchant.
5. The Financial payment operator arranges for the appropriate accounts to be credited and debited as part of the settlement and clearing process

This is effectively the subject of the primary claim in the Apple patent which has an initial filing date of September 30th 2008. I think it is highly unlikely that any patent examiner is going to allow this claim as it is pretty well the basis of the conventional credit and debit card payment protocol.

However claim 2 is more interesting, because the card information sent to the merchant in step 2 above is extracted from an image of the payment instrument (i.e. the card) taken on the phone's camera.

Now I don't think anybody has done this before (Sept 2008) but nor is it likely to revolutionize the electronic payments world. Even in America there are moves towards contactless smart cards so why do you need the additional mobile phone step and if you've got an NFC phone wouldn't you store the card information in the phone? I can't see any security advantage in taking a picture of somebody's credit card, in fact you might be even more worried if the cashier disappeared around the back with your payment card.

So back to the title, why is Apple going to dominate the mobile payments world? It's simple, they're adequately resourced with funds and skills and they are clearly working very hard in this area, what other patents are wandering around that we haven't yet seen? And please ignore the publication date of 1st April, pure coincidence!

And here's the punch line, if anybody can get the user interface right for making a mobile phone payment it's going to be Apple and right now I don't think anybody has got this right. So stand by, mobile phone payment on the iPhone using NFC is probably not far away!

Dr David Everett.

Trusted Service Managers – Security as a Service

By Chris Shire, Infineon Technologies

Chris Shire

Mobile Network Operators (MNO) have for some time considered the ubiquitous "SIM" to be not only the prime configuration management function of a 2G GSM compatible phone, but their exclusive property and a way of controlling user access to communication services. Recently with the growth in advanced communication devices e.g. smart phones, mobile app stores, laptops and netbooks with GPRS or WLAN connectivity etc, the SIM or the 3G USIM has become sidelined and the role of the MNO seen as a "bitpipe" supplier. This balance is about to change again. With the introduction of a smartcard web server (SCWS) function into the USIM and the forthcoming rollout of NFC enabled phones; the USIM will become the heart of a personal communications and transaction ecosystem. This will then position the USIM as a "Security as a Service" portal for whatever or whoever controls the terminal's access to the internet.

However the USIM is not the only prospective core of a personal communications system. NFC and other non-GSM communications processes can be secured using Secure Elements either embedded in the terminal or in a removable memory card. If applications can only be procured from one supplier, e.g. a phone manufacturer's online store, the application and the associated transfer rights for other terminals must come from the same supplier. In this case the online store is acting as a service manager for what is essentially a "walled garden". These applications are written and deployed for one specific scheme and although they can be personalized by the user, they are essentially uncontrolled software with little or no integrated digital rights management.

If a user wants to use multiple third party secure applications, e.g. payment, transport, identity etc. there are issues over control of the encryption keys and certificates. For example it is unlikely that a bank would allow a credit card application to be transferred from one device to another by either walking into to a retail outlet, or online. Devices which hold payment certificates and all the associated management processes must be certified as secure by the payment scheme operator at both the hardware and software level. This does not rule out the use of a Secure Element but various measures are required. Secure Elements could be certified and their pre-personalization controlled, as with normal banking cards, but the logistics and activation processes are still under development. It is likely that some terminal manufacturers may take on this challenge, but there are some commercial issues.

One key issue is a positive return on investment which exposes some questions: does a terminal manufacturer have the right resources? Do they have enough customers wanting the same application from the same bank, transit authorities etc? Does the issuer have the commercial structure to manage groups of disparate 3rd parties? One solution is for a local intermediary to be set up to manage the local 3rd parties. They would ensure the security of the data at issuance, during use and revocation for all the processes and stakeholders across a number of 3rd parties. This is a key process for a Trusted Service Manager (TSM). It assumes the TSM would be given control over the Secure Element by the terminal manufacturer. The TSM would then act as broker for the terminal manufacturer, selling space on the Secure Element to the 3rd party application providers in a specific local region or country. The TSM could provide added services such as customizing the terminal's support of language, currency, and geography with the application security environment to suit the stakeholders.

Such a business model has issues: terminal designs and their software operating systems change frequently. The wide variety software stacks that control the growing range of phones and Secure Elements will take time to be certified by the payment scheme operators. The range of terminals that even one bank might expect its customers to use makes the problem still quite complex even if limited by region. The lack of standardization of the software API in mobile terminals currently makes the security management task one of Herculean proportions. This may change with time, as happened with early computers with emergence of a common operating system, but commercial pressures today are very different. One solution is to use the Secure Element for stand alone applications which need a root of trust for their security processes but are essentially of the "write once, run anywhere" type. Examples include the control of personal or sensitive data e.g. account numbers, passwords, biographical or biometric information. Applications requiring control of 3rd

party provisioned secure data elements such as keys, certificates etc need a defined and certified environment, which is common across many hardware platforms.

An alternative approach is for the MNO to takeover the control of communications and let TSM's manage the services. Using a USIM certified secure by payment scheme operators and compliant with the ETSI specifications. Such a USIM must process the 3rd party applications, including NFC communications, and simultaneously control the mobile phone communications. This can be done with a high end NFC USIM.

With the advent of 32bit core processors, USIMs are capable of running more than one application in real time. An example is the Infineon SLE88CNFX600PM device which is the basis of several NFC USIMs now being deployed. The device can host a SCWS which in conjunction with the large non-volatile memory of over 500K bytes allows for a number of applications to be either instantiated at personalization, or delivered via an Over-The-Air download. Additionally a Single Wire Protocol (SWP) interface now provides a link from the NFC compliant Host Controller Interface software to the outside world. Such a NFC SIM can provide both ISO4443 APDU command interface and Mifare™compatible emulations with multiple UID's. This allows the terminal to interact with payment, transport and other physical systems such as buildings, cars and logical access to computers, games consoles etc.

The TSM can now prove to any 3rd party application provider that their application is held quite securely as the USIM hardware is certified to common criteria EAL5+ High. The software API is ETSI compliant, so the application can run without need to know the terminal model, operating system release etc. The MNO can provide access to a wide range of tested tools and a large population of users. There are still some commercial issues to be overcome. In the case of small providers the TSM may provide a SDK environment for the application developer to use, or may even provide a menu of pre-defined applications which require simple adjustment of data elements e.g. logo, URL etc of the provider. Larger application providers may require a commercial relationship with the MNO to align issues of branding, exclusivity, marketing etc and the consumer relationship management, but the application can be managed by the security of the service offered by the TSM.

So who will provide the role of the TSM? A quick search of the internet provides the names of dozens of companies offering services. But the keys to the access of the NFC USIM are in the hands of the MNO. It is unlikely that a MNO will contract its services with more than a few TSMs in any one country. It has been proposed that a group of TSMs could be installed on to one NFC USIM, but commercial pressures may forestall this, let alone the complex security management problems. The organization providing the initial personalization of the NFC SIM will be quite influential as TSM. In the short term this is likely to be the NFC USIM card manufacturers who have certified secure programming facilities for both mobile and payment industries. The TSM activity offers further opportunities for the card supplier to provide added value services to the MNO and 3rd party application providers. It is conceivable that "gold card" and "platinum account" TSM based services may emerge. These might offer concierge and secure transaction services that configure the applications to match the local environment without the user having to raise a finger, with back up's stored online in case of loss or theft.

It should be clear this TSM based ecosystem is still in its infancy, the first implementations will be seen in 2010, but within a few years no phone will be complete without its NFC SIM storing the user's profile, access rights to systems and products, social network links, banking and transport preferences and 101 other physical devices. A TSM will provide security for these services almost invisibly. Users may no longer have to manage a variety of passwords, multiple cards, rings of keys or pockets full of tickets, tokens and loose change, secure in the knowledge that their phone has everything, safely in one place.

World News In Brief

Inside Contactless Plans to Acquire Atmel Smart Card Chip Unit

France-based Inside Contactless has planned to acquire the smart card chip business of Atmel Corp., enabling the struggling contactless and NFC chip supplier to enter new markets, including chips for EMV banking cards, even SIMs, NFC Times has learned.

The deal, for an undisclosed price, is still not being finalised but is expected to be announced as early as next week, said sources. It would nearly double Inside's headcount to a total of nearly 300, sources told NFC Times. The acquisition would include about 120 research and development, marketing and other personnel located in Rousset, France, and East Kilbride, Scotland, along with intellectual property and other assets of the chip unit. But it would not include any chip manufacturing plants, which Atmel has already sold, meaning Inside will remain a fabless chip supplier.

Olive launches the First Ever Triple SIM Cell Phone!

Olive Telecom (leading designer and supplier of wireless devices; 2G/3G handsets and smartphones) has introduced first ever triple SIM phones - V-Wiz GC800. The Olive Wiz triple SIM cell phone is a (2GSM+CDMA) QWERTY handset, with 2 MP camera and 4GB microSD slot.

This handset offers up-to-date features such as access to Twitter and Facebook in just a click, web-browsing via Opera Mini browser, easy email and QWERTY keypad. The triple SIM cell phone has 2.2 inch colour screen, WAP, GPRS, MMS, stereo handset, speaker phone and FM radio. Available with 3 back panels - yellow, black and silver, it also includes a 100 day replacement warranty as part of the warranty period.

Gemalto acquires Internet Banking Security Specialist Todos

Gemalto, the world leader in digital security, announced that it has completed the acquisition of Todos AB from investors led by 6AP, a fund belonging to the Swedish National Pension system. However, terms of the transaction were not disclosed.

Headquartered in Gothenburg, Sweden, Todos AB is a leading provider of strong authentication solutions for internet banking.

Over the coming months, Todos will be integrated with Gemalto's Identification and Access Management business line. Through this association, Gemalto believes to expand their e-banking business, bringing a complementary customer base and extending the solution offering.

Indian School uses RFID Necklaces for Students

In the Indian state of Karnataka, all students at a Belgaum school are required to wear a radio frequency identification (RFID) card on chains like a necklace. An installed RFID reader on campus then records a student's arrival and passes on the data to a central computer from where messages are automatically generated. This allows parents and school staff to monitor the students throughout the school day. A local RFID expert calls this application a pioneering practice as in the past more animals than people have been tracked using RFID until now. Keeping track of a student's movement will increase the safety and security given the long distances students travel to school.

U.S. and Germany team up for Secure Travelling Program

Department of Homeland Security Deputy Secretary Jane Holl Lute and German Interior Ministry State Secretary Klaus-Dieter Fritsche announced the signing of a document that states each country's intent to integrate biometric trusted traveller programs to ease movement between the two countries.

The eventual integration is expected to utilise both the United States' Global Entry program and Germany's Automated and Biometrics-Supported Border Controls program. Both programs are designed to allow approved travellers access to special security lines that authenticate the user to their passport biometrically leading to a large reduction in wait time in line.

New Line of Contactless Terminals to be launched soon

New Zealand's SmartPay announced it will begin delivery of its software for the PAX range of Electronic Funds Transfer at Point of Sale (EFTPOS) terminals. China-based PAX is the fifth largest EFTPOS terminal supplier in the Asia Pacific markets, producing more than 300,000 units per year.

Through the PAX agreement, SmartPay will offer customers a wider range of EFTPOS hardware, including S80 counter tops, SP30 pin pads, S90 mobile, S90 Wi-Fi - and software at the forefront of compliance and security standards.

Symantec buys PGP for $300M

Symantec will acquire encryption specialist PGP and endpoint security vendor GuardianEdge Technologies for US$300 million and $70 million, respectively, the company said. Both are privately held companies, and the deals are subject to regulatory approval but are expected to close by June.

According to Symantec, the companies' combined specialties in standards-based encryption for e-mail, file systems, removable media and smartphones will complement its security offerings, such as its gateway, endpoint security and data-loss prevention software.

Smartcard Operator identified 'Dishonest'

A Smart travel card will be delivered to Sydney 15 years after it was promised, at four times costlier, by a company that tried to abort the original Tcard contract. A judge described the whole incident as “reprehensible conduct.”

The NSW (New South Wales) Transport Minister, David Campbell, announced that Cubic Transportation Systems had won a $1.2 billion contract for TCard as part of the Pearl Consortium group. But it was revealed that Cubic sued the government 10 years ago in an action that helped prevent delivery of the TCard by its rival ERG.

ERG had promised to deliver the smartcard for $367 million before the government cancelled its contract in 2008. According to latest news, Cubic will start working to release the second version of TCard. Mr. Campbell believes the smartcards would be introduced in 2012, allowing commuters to tap on and off from different modes of transport - trains, government and private buses and government ferries.

Acer to Launch Full Line of Mobile Internet Devices

Acer has announced that it will be launching a full line of mobile internet devices or MIDs, by the end of May 2010 to hopefully boost profitability. Acer will also launch version 4.0 of its Shell user interface on these new MIDs. Each MID will be able to use a 3G wireless service to access data and can share data and interact with each other. However, Acer offered no details on what exactly these devices will look like or what features will they have.

InCard Technologies unveils $2.95 Security Card Token

InCard Technologies, Inc., developers of the market-proven InCard DisplayCard security device for online banking, online trading, and data access, is introducing a new family of card token products, priced below $3.00 in million-unit quantities. The InCard ICard uses a plastic, credit card form factor in conjunction with a web interface to provide one-time passcode (OTP) security in payment or ID card format. InCard Technologies has already begun marketing the ICard directly to the top financial institutions in North America.

Vasco rolls out the Digipass Pack for Remote Authentication

Authentication and e-signature services provider, Vasco Data Security, has rolled out its Digipass Pack for Remote Authentication, a solution addressing the security needs of SMEs (Small and Medium Enterprises). The Digipass Pack includes Digipass for Mobile licenses, enabling the use of a mobile phone as authentication device. Digipass for Mobile can be used for two factor authentication and digital signature for m-banking, e-banking and e-commerce.

57% Organisations are prone to Data Breaches and Exploitation

Verizon Physical Security Services combine a physical security assessment and penetration test, security awareness training, a social engineering experiment, and an evaluation of relevant logical security technologies such as smart cards and biometric scanners to evaluate and strengthen an organisation's overall security posture.

Data from the 2009 Verizon Business Data Breach Investigations Report demonstrate the importance of physical security for data protection. For example, the report showed that only 43 percent of organisations had properly restricted physical access to confidential cardholder data according to PCI-DSS (Payment Card Industry Data Security Standard) requirements. In other words, 57 percent of organisations had left cardholder data open and exploitable via a physical breach.

Biometric Logins not viable for Mobile Devices

Biometric logins that use fingerprints, voice recognition or identify people by the way they type are not yet a feasible option for portable devices like netbooks, palmtop computers and smart phones.

Smart phones and other portable devices do not currently have the sophistication to be adapted easily for biometric technology.

According to James Pope of the College of Business Administration, University of Toledo, Ohio and Dieter Bartmann of the University of Regensburg, Germany, simply logging in with a password looks set to become technically passé. Security loopholes in login systems and web browsers are posing a threat to online world. The findings were published in the International Journal of Electronic Marketing and Retailing.

Should our health records be online?

By Amichai Shulman, CTO, Imperva

Amichai Shulman

Online medical databases seem like a natural choice in an age where technology is anywhere. They allow emergency teams to have access to critical medical information at time of need, or just making patients life easier when hopping between different healthcare providers. Despite these advantages, voices against it are being heard from a wide spectrum of stakeholders, usually by means of FUD. Doctors, hospitals and various associations are among the objectors to medical computerization programs.

The most recent affair to trigger this debate is the NHS's intention to create a national online repository of personal healthcare information. As an almost instinctive response to this move, the Patients Association announced its discomfort regarding health records going online. According to them, the obvious solution is to have every person hold a smart card with their medical history. In case of emergency, the rescue teams can have the required information from the card. Objectors of this approach claim that the card is not reliable and besides, people cannot be trusted to hold the card with them at all times. In addition to these valid arguments, the discussion always brings up the claims which state that (distributed) paper files are safer than a central electronic database. Indeed, in order to breach paper files, one should have physical access to the storage location. The major implication of this is that the set of individuals that may directly compromise the information is limited. However, besides this alleged restriction, there is no advantage for papers. For instance, there is no effective way to keep an audit trail of who accessed which data or to enforce granular access control policies on it. In addition, in case information should be available from multiple locations, a physical copy needs to be made and shipped, further increasing the chances of it getting lost. In fact, incidents in which sensitive medical records were stolen, lost, or just carelessly dumped to a publically accessible dumpster are not uncommon.

An incident which plays well into the hands of the opposition to online health records was recently reported in Ireland, where catering staff in one hospital have been (carelessly) granted access (through the HSE medical records system) to sensitive personal records. Indeed it seems like a classic example of the risks posed by medical records going online. However, analyzing the facts draws a different picture. Apparently, the system has been designed with security capabilities, taking into account that it will be used in hospitals nationwide. As it turns out, capabilities are not enough. The real problem was not related to the system itself, but to how this particular hospital used it. Lack of deployment guidelines and education made the hospital using it as-is, granting access to sensitive information in a promiscuous way. The lesson which should be learned from this episode is exactly opposed to what the program opposition wants us to learn. Instead of spending void efforts on trying to prevent such programs, they should be recognized and well planned. By taking this approach, clear deployment guidelines and regulations can be in place, minimizing the risk of uncontrolled deployments.

A somewhat similar debate occurs worldwide with respect to databases containing biometric information, which include DNA samples, fingerprints and pictures. The primary motivation behind collecting this information is to have a tool which assists police investigations to resolve crimes and countries to deter terror. Here as well, development and deployment processes are far from being smooth. For example, in Israel there is a heated public debate around a national biometric database, intended to include information such as fingerprints. Arguments against this particular database show up in all flavours, including loss of privacy and honest concerns that it will fall into the wrong hands. An exceptional example of the FUD campaign around this database is the claim that fingerprints may be planted in crime scenes in order to frame innocent people. However, an issue which is never mentioned is that in this particular country, the discussion is void as a biometric database already exists. In Israel, when a soldier is recruited, all his biometric attributes are scanned and kept for good. Combined with the fact that military service is mandatory, we get that this database includes information of most adult citizens. Since the information is kept by the army, there is no public knowledge regarding which security and privacy controls are taken in order to protect it. Furthermore, nothing is practically stopping other government institutions (e.g. police) from accessing this database in case of need.

Another example of fingerprint database of larger scale which already exists is related to United States Department of Homeland Security. Today, every visitor of the U.S. is required to leave fingerprints and digital facial image when entering the country. While this specific issue does not concern U.S. residents, there are

discussions about a national DNA database. Again, information is already kept, currently only for criminals indicted in certain crimes, where the number of qualified crimes is ever increasing. The proposal under discussion offers to keep information on every person arrested, no matter if eventually he is found guilty or not. Whatever approach of the two will eventually be chosen, both are problematic. Statistically, certain populations are more likely to get arrested and convicted, resulting in a racial bias within the database, which in turn leads to more false arrests for this particular population. Another approach which is fairer is to include everyone in the DNA database. By this approach, the database is likely to be far more effective in crime resolution, and the racial bias will be eliminated. In addition, a database which concerns the general public is more likely to have strict controls around it.

One may argue that all above examples are related to cases where people do not have a real choice when it comes to surrendering their biometric or medical information. Even in the health records case, were allegedly patients are given a choice, staying behind with paper files where the entire system goes online will eventually decline basic services. The point is that people do give their information without debating too much, even for the sake of their own convenience. This is well demonstrated in a recent case where a defunct airport fast pass company tried to sell information, which included fingerprints and other personal information.

Acknowledging that biometric databases already exist in various forms and adopting them is likely to benefit the general public, certainly more than bashing them. Moreover, as the public discussion around these databases increase security and privacy awareness, it is less likely to be used without clear regulations and deployment guidelines. Being stored in a centralized digital media, the information may be protected by various technological means which cannot be implemented with plain paper files:

- Role Based Access Control – ability to restrict access to different data based on individual job function enables scalable access control.
- Segregation of Duties – making sure that organization critical tasks are not performed by a single person is a key element in fraud prevention.
- Granular Audit Trail – As opposed to paper files, where one can read a document and put it back in place without drawing attention, in databases all accesses may be logged to the individual user level.
- Software Patch Management – Keeping track of known vulnerabilities is critical for protection against 0-day exploits.
- Administrative User Activity – Super users has always been the weakest link in IT security. Since physically they are allowed access to entire organization data, they should be watched closely.

World News In Brief

A Letter Halted South Africa's Smartcard Project

An anonymous letter, received by South Africa's State Information Technology Agency (SITA), stopped the department of home affairs' so-called Smart ID Card (SIDC) project in its tracks. The contents of the letter, and the allegations it contains, will not be known before the end of June 2010, when a forensic audit report into the matter gets finalised.

Briefing members of Parliament's home affairs portfolio committee, Sita acting chief executive officer Ramabele Magoma-Nthite said the letter, received on September 9 2008, had made allegations about "serious flaws with regards to the evaluation of the Sita tender" for the card. The halted tender process will start once the Auditor General's report comes on compliance with agreed-upon procedures.

Expert shows Serious Flaws in US E-cards

A new study by Avishai Wool, professor at Tel Aviv University's (TAU) School of Electrical Engineering in Israel, finds serious security drawbacks in computer chips that are being embedded in US credit, debit and "smart" cards. Using simple devices constructed from $20 disposable cameras and copper cooking-gas pipes, Wool and his pupils Yossi Oren and Dvir Schirman have demonstrated how easily the cards' radio frequency (RF) signals can be disrupted.

Wool's latest research centres on the new "e-voting" technology being implemented in Israel.

"We show how the Israeli government's new system based on the RFID chip is a very risky approach for security reasons. It allows hackers who are not much more than amateurs to break the system", Wool explains.

Now, every new US e-passport issued since 2007 has been outfitted with the similar chip used in credit, debit and "smart" cards, embedded on its back cover. There are high chances that these passports will be exposed any day by the hackers. The US State Department has already taken Wool's advice, and they have added conductive fibres to the back of every American passport to make it more secured.

Sagem announced Launching of its New NFC Android Phone

Sagem, the world leader in defence, consumer electronics and communication systems, has announced a 2010 launch for its new NFC-enabled Android phone - the Netribe.

Netribe, developed for Puma (German sports brand), will feature biometric technology, solar cells and atmospheric sensors, among what promises to be a myriad of new functions. Sagem has remained hush-hush on the specs of Netribe, but disclosed that it will be "more than an Android open OS tablet phone".

Netribe is expected to ship in the third quarter of 2010 and will cost $150 in the neighbourhood.

Citibank reveals Instant Issuance Credit Card Service

As per The Paypers report, global financial services provider Citi has launched its Same-day Card Issuance Service in Hong Kong, a service that enables customers to obtain their credit card within an hour.

The instantly-issued card will be released as soon as the Citibank credit card applicants submit the application form together with the relevant documents at one of the Citibank branches. In 2006, the instant issuance service was available at Citibank credit card mobile, circulating in different parts of Hong Kong.

Heartland Payment Systems has launched Acceluraid

The US-based payments processor provider Heartland Payment Systems has launched Acceluraid - an electronic aid distribution platform that utilises a single financial account for integration with a campus card system. It will enable students' access to their financial aid refunds through a financial account that links to both Heartlands' Campus OneCard, a prepaid campus ID card and to a school-branded debit card. Additionally, Acceluraid can be used as a platform which distributes aid to a financial account linked only to a debit card.

M2SYS and Fujitsu to Accelerate Adoption of Palm Vein

M2SYS Technology (leading fingerprint identity management technology provider) announced a strategic alliance with Fujitsu Frontech North America (FFNA) (supplier of retail point of sales terminals, self checkout systems, palm vein biometric authentication technology) to lead the widespread growth and adoption of PC-based palm vein biometric recognition systems. Under the partnership, M2SYS has added support for the Fujitsu PalmSecure biometric authentication system to its Bio-Plugin biometrics platform.

Bio-Plugin enables software companies to rapidly integrate and deploy an enterprise-ready biometric recognition system without the development and ongoing support challenges that are associated with low-level biometric SDKs (software development kits). Software companies that want to adopt the highly secure, reliable, and user-friendly Fujitsu palm vein biometric authentication system can now do so within hours, accelerating time-to-market and reducing software engineering and maintenance costs.

Voice Commerce Opens National Trust Centre in the UK

Voice Commerce announced the opening of its UK 'VoiceTransact Trust Centre', a platform using Nuance Voice Authentication technology, which authenticates and verifies any type of commercial transaction that a UK business requires to complete with its customers. Using voice signatures, which are enabled over mobile phone, the UK Trust Centre marks a significant advance toward easy, cost effective adoption of voice signatures by any size or type of business within the UK.

French Officials Announce Date for Nice Trial

French officials in Nice have announced the date - May 21, for the launch of the much-anticipated NFC demonstration project, designed to showcase the range of mobile services made possible by Near Field Communication.

Christian Estrosi, France's minister of industry and the mayor of Nice, will officially launch the project, which French officials have named as a "first in Europe." They had kept the date quiet until now. With multiple mobile operators and service providers, Nice will serve as a critical test of France's cooperative approach to NFC.

China Mobile halts its 3 Million RF-SIM Cards Production Plan

By Suparna Sen, Smartcard & Identity News

Suparna Sen

China Mobile this year ordered 3 million RF-SIM cards. China Mobile has chosen to discard the world-wide NFC (Near Field Communication) ISO/IEC standard for a proprietary mobile phone payment solution instead.

RF-SIM technology was developed and owned by a Chinese Research & Development company Trunkbow. RF-SIM or Radio Frequency Subscriber Identity Module has a tiny aerial embedded within the SIM card that communicates on a 2.45GHZ frequency.

Mobile phones with a RF-SIM card will compete head on with NFC (13.56 MHz) offering much the same functionality as a NFC phone.

Hong Kong based Directel*, a telecommunications company and ambassador of RF-SIM technology, has demonstrated over a dozen usages of RF-SIM:

- E-ticketing: RF-SIM avoids actual ticket delivery and allows e-ticketing in public transport such as train, buses, subway, taxi, etc

Tickets can either be stored in RF-SIM, so that customers can read it to use it as proof in case dissension arises, or it can be totally intangible, as just using your RF ID. When ticket issuers require to check the ticket, customers can hold their mobile phones close to the POS, and the system can find out the e-ticket bought. In this way, after ticket checking (change the status of e-ticket after use), customers are allowed to enter. The e-ticket, once used, becomes invalid and can be deleted.

- Member Card: The unique flexible memory of RF SIM enables users to host a number of VIP cards into only one physical object - RF-SIM card. Each VIP card is mutually isolated and independent, and managed by different keys. The unified settlement platform can connect with different VIP cards through their respective keys so that the right transaction is made and the right points are added to the right VIP account.
- E-coupon: The e-coupons issued by merchants can be stored into the RF-SIM card in advance. All you have to do is hold the phone close to the POS and enjoy the discount. You can also download the latest e-coupons when you pay with your RF-SIM at the POS.
- On-line Shopping: Users can enjoy shopping using RF-SIM to make small purchases on line.
- Door keys: RF-SIM offers safe and secure entry and attendance management system. It uses employees' RF-SIM cards rather than buying new cards and enables double access security guarantee. RF-SIM also includes card number identification, password identification, and two modes availability for attendance management: on-line and off-line and attendance information feedback.
- E-license: Vehicle licenses can be planted in "mute card" in the specific place of a car, with RFPOS placed in specific roads. It provides convenient means for police to check the cars, whether fake or not. Also, information of Insurance number and brand of car are planted in one e-license as a substitute of Insurance certificate.

In addition, RF-SIM can be used as an e-purse and support Active OTA (Over The Air), SMS download, Push and STK menu management.

RF-SIM has a second mode of operation which allows it to receive data at a much longer range of 20 meters. The broadcasting terminal enables vendors to send real-time advertisements to pedestrians passing within 20-30 meters of their shop.

Although RF-SIM appears to be a better and quicker route to add contact-less functionality to a mobile phone, it doesn't come without its drawbacks.

* *http://www.directel.cn/eng/*

The high frequency in which RF-SIM operates makes it incompatible with Mastercard's PayPass & Visa's PayWave systems, and with the existing contactless ticketing systems such as FeliCa and Mifare. Local banks and financial institutions would need to replace the existing POS terminals that support only the NFC standard (13.56MHz) to RF-SIM compatible POS.

Huang Gengsheng, principal scientist for wireless at the China Mobile Research Institute, has accepted of some shortcomings in RF-SIM, such as the cards' failing to work with some popular phone models sold in China, including some of the phones made by Samsung and Dopod (a smartphone maker owned by Taiwan-based HTC). The SIM's also don't work in most phones complying with TD-SCDMA network technology - China's own domestic standard for 3G phones.

Furthermore, on watching the online ticket barrier demonstration, it seems the phone needs to held close to the reader for a longer time than other contact-less ticket solutions. (http://www.directel.cn/eng/rfsim_yn_3.html)

It's with these drawbacks in mind that executive director and vice president Li Yue of China Mobile called for a review of China Mobile's decision to roll-out RF-SIM cards.

He questioned the company's ability to get millions of consumers to change their existing payment habits, and ordered the Company to recover the costs for a massive rollout plan of SIM cards and the many readers at the point of sale and at transit gates.

China Mobile had only sold about 100,000 of the RF-SIMs nationwide, out of an initial order of 1 million cards. It also seems to lag behind in deploying point-of-sale terminals that can read the new SIM. The Company initially ordered 10,000 to 15,000 of POS, but failed to arrange them on time.

So what's next for China Mobile? According to latest news report, China Mobile may finally go for a combined NFC and RF SIM service. In addition to the existing RF-SIM 2.45GHz short range frequency (that require the phone to be swiped across the reader), the Company is going to try and profiteer for RF-SIM's medium to long range mode that could transmit a tiny amount of data in excess of 20 meters. However, in long range mode, the data would only be something like a link to a website and would not be used for making payments.

Other telecom giants seem to follow closely the whereabouts of China Mobile. Of late, China Telecom, one of China's three leading mobile network operators (China Mobile, China Unicom and China Telecom) has shown a great deal of interest in RF-SIM technology. The operator has begun a trial in Shanghai in conjunction with RF SIM supplier, Seimma Tech Co. Two hundred POS will be equipped to accept RF SIM payments and in the process, 1,000 subscribers will participate.

According to Seimma's marketing director Ding Peihua, (reported by Global Times), if the China Telecom trial proves successful, very soon new RF SIM-based projects will be rolled out in supermarkets and restaurants all over the country.

Verifone already invested $5 million, with the integration of some 125,000 mobile payment terminals, and has been named the preferred supplier of payment systems technology to Trunkbow. Global M Pays has also shown interest in RF-SIM.

World News In Brief

GlobalPlatform's NFC Mobile: Managing Multiple Secure Elements

GlobalPlatform has released a technical paper that analyses the implications of managing multiple secure chips in a single mobile handset to deliver near-field-communication (NFC) services. The document, entitled 'GlobalPlatform's Requirements for NFC Mobile: Management of Multiple Secure Elements' is free to download at http://www.globalplatform.org/mediawhitepapers.asp.

GlobalPlatform's Mobile Task Force undertook research to understand the technological possibilities and challenges of using multiple secure elements - tamper resistant devices with embedded microprocessor chips in a mobile device. The white paper is the result of this investigation, which identified two different business models, and details the functional requirements needed to support the acknowledged technical architectures.

Apple wants Siri

What is Siri? And why would Apple buy it? Siri is basically a new kind of search engine for mobile devices. Some have described it as part of the new web - a web that comes after the era of typing searches into Google.
Siri (http://siri.com/) offers an array of services in just a click from booking a table for two at your favourite restaurant next Sunday to wanting a taxi right now or getting information on tomorrow's weather.

Apple want to own this technology to make the iPhone - a wallet for financial transactions and paving the way of making future iPhones e-ticket repositories for cinema, concert or even plane bookings. Perhaps, Apple plans to insert a RFID tag built into the iPhone for easy verification when one reaches the concert hall door or while boarding a flight. Adding Siri's technology on the iPhone as a basic part of iPhone OS or a system app, and then putting those two extra features, will make the iPhone the must have PDA we all dreamed of owning.

NXP introduced its Latest UHF Solutions in Market

NXP Semiconductors, the leader in RFID chips, has introduced its latest UHF solutions for the fashion, retail and electronics markets, reports globalsmart.com. The UCODE G2iL and G2iL+ enable leading-edge read ranges based on a simple, cost-effective single antenna solution. The new chips also offer a variety of industry-first features, including a tag tamper alarm, several privacy mode options, and password-protected data transfer or digital switch.

Citi to make its First Move in Mobile Payment

U.S. based Citigroup plans to issue contactless-payment stickers in the U.S at the end of this month, as its first move beyond pilots for a possible national rollout of mobile payment, NFC Times reported.

Citi is said to order some hundreds of thousands of stickers that customers will use to attach to their phones or other devices to make low-value purchases. The Citi stickers are expected to be issued in several U.S. cities and carry a MasterCard PayPass credit application, which is accepted in about 70,000 merchant locations in the country, along with some taxis and vending machines, as well as locations abroad.

Edible RFID Microchip for Patients

Researchers at the University of Florida have combined two-way radio-frequency communications, microchips and printed nano-particle antennas to make pills that communicate with cell phones or laptops to tell doctors whether patients are taking their medicines or not.

NHS – Worst for Data Breaches

The NHS has reported the highest number of serious data breaches of any UK organisation since the end of 2007, the Information Commissioner's Office says. David Smith, deputy commissioner at the ICO told the Infosec security conference the NHS had highlighted 287 breaches to it, accounting for more than 30% of the total number reported in the period.

The NHS, the UK's largest employer with 1.7m staff, is in the process of rolling out digital patient records. Most of the breaches (113) were the result of stolen data or hardware, followed by 82 cases of lost data or hardware.

Motorola unveils New Biometrics Monitor

Motorola showcased a solution developed by Annapolis, Md.-based Zephyr Technology, in which Motorola made a capital investment last year. The device monitors and wirelessly transmits data via Bluetooth on body functions such as heart rate, breathing rate and skin temperature. As many as 64 personnel can be monitored by a single application.

Interview with CEO Cyril Lalo and CTO Philippe Guillaud – NagraID

By Tom Tainton, Smartcard & Identity News

Tom Tainton

Who are NagraID Security and what is their background?

NagraID Security SA is a subsidiary of the Kudelski Group and produces multi-component and other complex cards for the security and identification industry. Our office is in Los Angeles where most of our R&D team is based and our corporate headquarters are situated in Switzerland. We are the leader in display card manufacturing with over 1 million display cards deployed in 29 countries last year.

What is the 306 series?

The 306 series card is the latest addition to our family of powered display cards. It is a 6-digit, 12 Button Touch Keypad display card credential packaged in a familiar standard credit card form factor. The integration of a touch keypad now enables us and our partners to develop and implement multi-function applications on a single card such as PIN activation and challenge response. The 306 Series card can function as a One Time Password credential, physical access device, PKI chip card, contactless eWallet and a payment device.

Why is it different to competitor's models?

The 306 Series contains several features that differentiate it from the competition. The most obvious distinguishing feature that the consumer will notice is how sleek the card is when they first hold it in their hands. In fact, the event based version has the same ISO certified dimensions as a classic credit card.
A second distinguishing feature is how fast the display and processor work, every operation is instantaneous. We developed a high contrast, ultra fast and flexible LCD panel specifically for this product. Unlike other card display technologies available from our competitors, the 306 Series display supports the scrolling of large data strings.

Another unique attribute of the 306 Series is that it is the first smart display card to integrate a Touch Keypad. Compared to mechanical buttons typically found in this type of application, the Touch Keypad provides outstanding reliability, key registration accuracy and lower power consumption for increased battery life.
Other less evident features that really set this display card on top of the competition lie inside the card at the chip level. The card is fully programmable and has large data storage capacity that enables the development of innovative applications, all via the integrated contactless interface. Besides the technical advantages, our partners and clients know that they can rely on a solid company with the finest EMV-certified card manufacturing and personalization facility in the world. All the cards are produced under strict security guidelines of NagraID SA that meet or exceed the highest standards which is the foundation of the reputation of Swiss competence.

How will it improve e-security?

Today with the usage of static, easy to guess passwords, it is relatively easy to hack into online accounts, resulting in frauds and identity thefts. The easiest and secure way around this is to use multifactor authentication which includes one time passwords (OTP). With the introduction of the 306 Series, NagraID Security is offering a unique product that is multi-functional and convenient to carry in a wallet. It's more secure as the Touch Keypad can be used to PIN protect the card.

What industries and consumers will 306 series particularly benefit, and how?

The unique ability of the 306 Series to run customized software, integrate a contact chip, magnetic stripe and wireless interface makes it ideally suited for all online based transactions requiring enhanced security.
The banking and financial sectors are already big users for this technology, and this year we see growing interest from healthcare, retail and entertainment industries. OTP tokens were traditionally only available in the Key-fob form factor and single function; for the consumers. The possibilities are endless.

What next for NagraID Security?

We will continue to listen to our customers and partners, understand their needs and back them with exceptional products meeting the highest industry standards. As a market leader, we continue to invest in research and development, focus on innovation and being first to bring new features and capabilities to our products.

World News In Brief

Precise Biometrics introduces Biometric Logon Solution for Windows 7

Swedish fingerprint recognition solutions provider, Precise Biometrics AB, has announced the introduction of Precise BioMatch Logon for Windows 7.

According to the company, the logon application offers a convenient way of personalising the access to a user's computer and files using their fingerprint. It can be used with most swipe sensors in the market such as laptop-integrated sensors. The readers have to be supported in Windows 7's framework for biometric applications, Windows Biometric Framework (WBF).

Precise BioMatch Logon does not require any smart card and will be available for download at Precise Biometrics' website: http://precisebiometrics.com/

Mexico deploying Multi-Modal Biometric ID

Mexico plans to start enrolling its 110 million citizens into the National ID card program this summer. The program will be among the first to capture iris, fingerprint and facial biometrics for identification, says Terry Hartmann, vice president of identity solutions at Unisys.

Unisys' Mexican subsidiary was awarded a contract by the Mexican Ministry of Internal Affairs and National Citizen Registry to create and manage the biometric-based citizen identification solution. The agency will issue another tender for companies to compete for the ID card issuance portion of the project. The country expects to issue cards to citizens within the next three to four years.

INSIDE Contactless, Sagem Orga and TazTag Partner on New NFC Mobile Payment Device

INSIDE Contactless, Sagem Orga and TazTag announced the joint development of a new method of delivering NFC payment functionality. Based on TazTag's innovative TazCard, the new device is currently in pre-alpha testing and shows the feasibility of an option that facilitates NFC contactless payment transactions while providing full NFC functionality for other applications as well. About the size of an ordinary credit card, the TazCard is a special-purpose, Java-based handheld device capable of supporting a variety of NFC applications, including payments. For this new payment device, INSIDE's Java-based test payment application has been installed on a Single Wire Protocol (SWP)-enabled SIM card developed by Sagem Orga, which is connected to the INSIDE MicroRead NFC controller built into the TazCard. The TazCard also utilises INSIDE's Open NFC protocol stack. With its 3.5-inch colour touch screen, the TazCard is able to provide the user with a full NFC experience for payment and other NFC transactions.

VeriFone selects RBS WorldPay for PAYware Mobile

US-based electronic payment processing services provider RBS WorldPay, has been selected by VeriFone to provide merchant accounts for the buyers of the VeriFone PAYware Mobile card payment service available on the iPhone.

The PAYware Mobile application provides small businesses with card processing options via the iPhone. The application incorporates VeriFone's card encryption technology, which encrypts each transaction from the time of card swipe until it reaches RBS WorldPay, and ensures payment processing.

VeriFone's card reader includes a stylus for signature capture and a mini-USB port for charging iPhone while the reader is attached.

ActivIdentity introduces PKI Secure Mobile Solution for Smart Phones

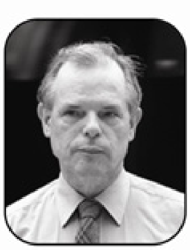
ActivIdentity Corporation a, global leader in strong authentication and credential management, introduced a new solution to provision public key infrastructure (PKI) and Federal Information Processing Standard (FIPS) 201-compliant credentials onto BlackBerry smart phones. Using a secure microSD card, ActivIdentity enables BlackBerry users to sign secure emails digitally or provide two-factor authentication when remotely accessing protected network (Web) portals.

Canadian ePassports – 2012 Affair

Passport Canada plans to launch an ePassport in 2012, while it wants to hear Canadians' thoughts on the issue, including revised fees - a development that requires consultation with Canadians, under the User Fees Act. The new passport will have little change in appearance, but will contain an electronic chip encoded with the bearer's name, gender, date and place of birth, and also a digital portrait of the traveller's face. Canadians are asked to fill out an online questionnaire on Passport Canada's website by May 7. The comments will then be considered in the development of the new passport and its fees.

Trusted eServices in the UK

By Peter Tomlinson, Smartcard & Identity News



Peter Tomlinson

There is a tide in the affairs of men[1]… Not just of men, of course, but equally of women. On April 13th, nearly 150 people were awaiting a presentation by Jayne Nickalls, CEO of Directgov, who was to tell us about their approach to trust in eServices for the public – services delivered electronically. The background is last December's White Paper 'Putting The Frontline First: smarter government[2]. The determination now seen is (at last) to implement M. Prodi's eEurope concept: a win-win environment of better services for the public and businesses, with lower costs for the public sector – that appears to be the way that the tide is now flowing.
The event was the pre-launch information day for a Technology Strategy Board (TSB) competition, introducing £10.3M of grant funding. The target is a raft of projects in the area of trusted services to the public[3] – but not just services delivered on-line via the now almost classic broadband internet. And not just public sector services, either. A competition for the grants will open on 10th May. Up to 50% of project costs are available for qualifying "business-led collaborative projects to develop trusted services … that will deliver significant improvements over today's service offerings" and "collaborative R&D projects[4]".

Ms Nickalls was prevented by pre-election purdah from fulfilling her commitment to talk, leaving us with many unanswered questions.

Why have this competition now? It must be said that there was considerable scepticism among the audience. We could not obtain anything specific – but there is certainly a growing awareness that there is a need to deploy more, and more secure, eServices in the UK public sector. Directgov, as it morphs into Mygov[5], needs to do that.

Later the same day TSB gave a shortened presentation to the Smart Card Club. There Richard Poynder (Smartex Ltd) asked the obvious questions, about the duality of trust and convenience. First: why do we not have a national eID scheme, so that each person can have a single secure token for signing in to many services? And a further question: about securing the linkage between the eID token and the person who is trying to use that eID. Silence on both counts. Of course we were not talking to the right people – that purdah again – but the people to whom we were talking are confident of the direction of the tide. Notable is that the hmg.gov.uk web site on which the White Paper was published hosts a growing portfolio of cross-departmental material, showing that civil servants are buying in to a collaborative programme – a programme that should fully embrace Information Assurance (IA, meaning Information Security and Service Quality).

A related question had been asked at the TSB event: will the contracts awarding the grants bind the recipients to Infosec assessment and thorough testing if they develop a trusted service, a supporting trust service, or a tool associated with such services? After all, much of this is ICT engineering. The speaker at that point in the proceedings was baffled. So the TSB is not part of a movement to get trusted services right by design. How do we do that? The Information Commissioner way to data protection gives sticks to a regulator, with which to beat the service providers when they get it wrong. Central govt civil servants have recently been given basic training on Data Protection, which is a start. Perhaps we might soon see an upfront quality and Infosec programme, with training for public servants in getting it right (for both in-house projects and contracted out projects)?

So, should we expect the TSB to unilaterally put Information Assurance conditions on projects that they support financially? Only if there is a national programme to do that, right across the public sector.

There is some positive evidence of IA being applied. ITSO Services Ltd (ISL) was set up by the Department for Transport (DfT) to support the issuing of most of the ENCTS[6] cards, plus overseeing and logging some of the activity when they are used. ISL manages the security modules in all the card personalisation equipment connected to it, and holds the database of issued ITSO Shells (application data areas) held in cards issued on behalf of its client Local Authorities. ISL's system was stress tested to ensure that it could support the volume of issuing in the run-up to the scheme going live. DfT is already, alongside its December 2009 Smart and Integrated Ticketing Strategy[7] and associated funding, engaged in moving public transport in 9 metropolitan areas closer to being overall a convenient public service. The Department of Work and Pensions (DWP) is developing a method to share space on a citizen service card, with an eye on sharing ENCTS smart cards[8]. On the negative side, the DEFRA Rural Payments Agency's Single Farm Payment scheme (software and process organisation combined) did not work well and is still problematical, and more recently the Student Loan Company's system has exhibited a similar failure mode.

Maybe the Civil Service will overall pick up the IA baton now – and also take advantage of the experience of other countries, particularly those that have already deployed strong security eID. But here are a couple of notes of caution: a framework and programme for eID has to be opt-in and provide privacy, so it cannot be the current UK ID card scheme – an eID scheme at this level needs to have privacy built-in – and securing the linkage to the real person remains problematical.

In this fragmented and technically challenging environment, it is very difficult for supply-side players to find and engage with relevant government projects and initiatives. A new trade association has this month been launched, with the aim of giving a unified voice to the supply chain that enables the development and delivery of eServices and the use of smart media (smart cards, and tokens embedded in mobile phones and other devices). Its name is Smartcard and Secure eServices Association (SSeSA). Its scope is described on the web site of its hosts, AIDC (UK) Ltd: www.aidc.org.

By bringing clarity and the clout of a single industry voice, SSeSa intends to provide a three way win: for the service user, for the service provider, and for the supply chain. It can also encourage government to do the "right thing" by bringing industry intelligence to bear on the importance of Information Assurance at the design stage of service delivery.

[1] Julius Caesar, Act 4, Scene 3, 218-224, William Shakespeare
[2] Cm 7753, found, along with an update, at http://www.hmg.gov.uk/frontlinefirst.aspx
[3] http://www.innovateuk.org/content/competition/trusted-services-competition.ashx
[4] http://www.innovateuk.org/_assets/pdf/competition-documents/briefs/tsb_trustedservice6pagecompflyer.pdf
[5] E.g. see http://www.guardian.co.uk/technology/2010/mar/22/mygov-personalised-government-web-services
[6] English National Concessionary Travel Scheme http://www.dft.gov.uk/pgr/regional/buses/concessionary/
[7] http://www.dft.gov.uk/pgr/regional/smart-integrated-ticketing/
[8] Building a society for all ages http://www.hmg.gov.uk/buildingasocietyforallages.aspx

Integration and Innovation: The Future for Transport Smartcards

27th May 2010, Bircham Dyson Bell, London

The Smartcard industry continues to develop rapidly with the number of Smartcard schemes across the UK increasing and local authorities and transport providers expanding both the geographical size of schemes and the range of functions they cover. The introduction of the concessionary travel scheme has provided a significant boost to Smartcard use and in London Oyster has been successfully extended to cover London Rail and Thames Clipper Services.

Compliance continues to be a challenge with ITSO now coming under the remit of the Department for Transport and a new business plan expected in May. Meanwhile in Europe the Interoperable Fare Management Project is working towards a 2015 deadline for compatible Smartcard ticketing.

This conference provides the opportunity to hear the latest on Smartcard policy in the UK and on the development of Smartcard schemes across the country. It also presents an opportunity to discuss the latest developments on key issues such as card security and the use of cashless payment.

The conference will cover the following:

- Developing a new business plan for ITSO
- The benefits and costs of a national smart ticketing infrastructure
- The Interoperable Fare Management Project and progress towards the 2015 deadline
- Extending Oyster to cover London Rail and Thames Clipper Services
- The potential of Smartcards for simplifying local authority service delivery
- Expanding the use of Smartcards for cashless payment
- Progress towards achieving EMV and ITSO compliance
- A passenger perspective on Smartcard development
- Increasing card security
- Reducing the cost of ITSO compliance and increasing accessibility

Confirmed Speakers Include:

Michael Leach Chief Executive Officer ITSO
Neil Scales OBE Chief Executive and Director General Merseytravel
Simon Ardron Head of Branch, Strategy Implementation Department for Transport Richard Bradshaw Head of Transport Detica
Jeremy Meal Director Smart Card and Ticketing Strategies MVA Consultancy
Sid Bulloch NEC Programme Manager Dundee City Council
Mick Davies Chairman Local Authority Smartcards Standards e-Organisation (LASSeO)
Speaker from Merseytravel
Nick Maltby Partner Bircham Dyson Bell
Chris Stanford Director CJS Consultancy Ltd
Mike Cowen Vice President, Chip Product Management MasterCard
Sharon Hedges Passenger Link Manager Passenger Focus

For further information and to register please visit https://www.eventsforce.net/smartcards