Smart Card & Identity News

Smart Cards, SIM, Payment, Biometrics, NFC and RFID
www.smartcard.co.uk

Identity Fraud: Why the companies affected are just as criminal

Christmas is approaching fast, but the World's fraudsters don't seem to be in a festive spirit. The payment fraud juggernaut continued to build momentum with a flurry of incidents recorded across Europe and America. There's nothing new or extraordinary in the reported crimes either. Instead, a familiar pattern of ineptitude, carelessness and sheer stupidity on behalf of the authorities and companies remain in question.

We'll start closest to home. The T-Mobile customer records scandal was well publicised in the UK media and drew criticism from the phone operator's customers. Allegedly, a former employee sold the personal details of thousands of customers, including information about when their contracts expired, to a number of 'brokers' who passed the data onto rival networks and other phone retailers.

Our Comments

Dear Subscribers

Once again Cartes has come and gone, no rail strike and perfect weather. In a way it seems to reflect the industry as a whole. The technology is hidden away and now we are only presented with the business propositions, the icing on the cake. Not a complaint just a realisation that the industry is now truly mature. It's funny really but when you are following the technology everybody is busy telling you that it's all going to happen next year and of course it never does. When people stop evangelising then suddenly it's all done and dusted.

So are there any loose ends? Well you wouldn't want to be disappointed would you? Does NFC ring any bells? Now here's the interesting thing the evangelists have gone, no more ramming it down your throat, a sort of acceptance that it will probably happen but no time real soon and that there probably isn't a killer application. It's all a matter of an instrument that gives you a better way of life. In other words the phones will eventually have NFC and people will find things to do with it.

Now it's taken a little time but I've got there, the phone is an instrument of social networking, either to talk, text or email and just about everything else pails into insignificance. Most phones have Bluetooth but it's not really a part of everyday life, I suspect most people never use it. The camera, oh yes that's a biggy because it fits into our social networking by providing a means of sharing experiences. Don't laugh even I take pictures on my mobile phone, in fact I was persuaded by my other half to upgrade my phone just to improve the camera. It takes a little longer but on a good day I can even get the pictures off the phone and onto the PC.

So here's the question does NFC help with my social networking? Payments – no, mass transit – no, security – no, information – no, connecting with my network - ? Now we've got to the Achilles' heal, does NFC help me communicate? By definition NFC, remember Near Field Communications, and according to he who knows about these things that means magnetic fields operating over a few centimetres or to use the buzz words Person to Person (P2P) but almost with physical contact. So what does NFC allow me to do that I can't physically do given that the other person is standing next to me? And before some bright spark emails me it's not about shaking hands with the Queen without touching her.

Let's be more practical, I can pass data stored in my phone to the phone of the other person. But I can do that today with Bluetooth and most people don't bother they usually send a text or an email. Smart phone users send emails and everybody else sends text messages, well that's my observation anyway. Ah ha they tell me but look how much easier it will be to do this with NFC, there's no pairing required which you need to do with Bluetooth when two devices first meet. The trouble is you are still going to have to set up the application that uses NFC so I can imagine people will still use text or email.

But it's free, there are no network costs to communicate by NFC, I don't think anybody cares. Those with smart phones will already have a data contract and those with text messaging just seem to see that as a part of life.

Now let's not give up, the Apple iPhone has a huge cult following of which a big part is the world of iPhone applications. Can you imagine developers producing applications that use NFC? That's assuming Apple decide to include NFC of course but I'm told by insiders they are seriously considering their options. But I'm stuck again, what could you do with NFC that you can't do with Wi-Fi or Bluetooth? In fact those few centimetres seem to be a problem unless I want to make sure nobody can over hear me, now what thought does that put in your mind?

We seem to say it so often but if you don't need security don't use smart cards, that has been our mission statement for years. NFC is based around a secure element, the SIM card or some other chip. Nobody has shown me an application for NFC other than payments that needs security and everybody now tells me that payments are not a major driver – so where do we go next?

Patsy.

Contents

Regular Features

Industry Articles

Events Diary

December 2009

7 – 8 3G Middle East 2009, Dubai, UAE - http://me.comworldseries.com/

8 – 9 RFID 2009, Paris, France - http://www.rfid-show.com/

13 -15 Cardex 2009, Cairo, Egypt - http://www.digital-idassurance.com/

January 2010

19-20 Fraud World 2010, Dexter House, London - http://www.iir-events.com/IIR-conf/AuditRisk/EventView.aspx?EventID=1869

19-21 Omnicard, Berlin - www.omnicard.de

20-21 Nordic Cards, Stockholm - http://www.smi-online.co.uk/venues/default.asp?ref=127

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

3

The Information Commissioner's Office (ICO) announced it was actively investigating the case which involved 'substantial amounts of money changing hands.'

T-mobile claim they are free of any guilt, since they 'approached' the watchdog themselves. A cynic might suggest they were just pre-empting the inevitable onslaught of media criticism when the story emerged. So have T-mobile issued a whole-hearted apology to their customers? Have they promised to assist fully with the investigation or compensate furious clients? Of course not. Instead, a company spokesman expressed 'surprise' that the ICO had gone public with the story. It seems they would have rather swept this unfortunate incident under the carpet and forgot about it.

This isn't the first time a company's staff have sold sensitive data to others in the UK. Fear not though, the Police are investigating all cases. Whether they will solve the mystery in which an unnamed Scotland Yard employee illegally accessed personal details from the Police national computer remains to be seen.

In the USA, they like to go the extra mile and give fraud criminals a helping hand. A Boston-based security consultant found he could purchase second-hand ATM machines containing sensitive transaction data on eBay and Craigslist. For less than $800 (479.003 GBP) Robert Siciliano bought an ATM and extracted a log of hundreds of credit and debit card numbers as well as account details. Siciliano was able to make the purchase anonymously online and even managed to barter down the asking price.

And just in case an inexperienced fraudster gets a little bit confused, there's a manual supplied alongside the machine giving clear instructions on how to access the sensitive data stored inside. Scary, isn't it?
In Spain, German authorities recalled more than 100,000 credit cards, the largest retraction in their history, amid fears that crooks had obtained sensitive data via an unnamed payment processing firm. Holidaymakers who used their Visa or Mastercard in Spain could be at risk of fraud following the security breach. Holders of cards issued by Barclays, DKB-Bank and Karstadt-Quelle were among those at risk.

The Volks and Raiffeisenbank banking group recalled as many as 60,000 potentially compromised credit cards as a precautionary measure. However, in a typical fashion, Visa and Mastercard deny any mishaps on their part, and pointed the blame elsewhere in the payment chain.

In a statement, the German Central Credit Card Commission (ZKA) convinced the public saying that the affected cardholders would be notified by their banks and any card fraud case will be properly addressed. Cardholders were advised to check their statements for suspicious transactions. The German banks and savings banks have already started exchanging potentially compromised cards free of charge.

But all hope is not lost. The eight members of an Eastern European crime ring have been charged for their part in the hacking of RBS WorldPay last year. After stealing more than $9m (5,388,786 GBP) in half a day, the men dispatched cashers in 280 cities worldwide to withdraw the money. The suspects were charged with computer fraud, identity theft, conspiracy and device fraud. They could face more than 50 years behind bars as well as being forced to pay back the stolen amount.

It seems as fraudster's methods become increasingly sophisticated, the defence systems in place to thwart them are getting more and more primitive. As long as nobody accepts responsibility, or agrees to do anything about this problem, the crisis will continue to grow. Expect similar reports next month. And even the month after that. Payment fraud is here to stay – we'd better get used to it.

Tom Tainton – Smartcard & Identity News.

Biometrics 2009- Personal reflections

By Dr Peter Hawkes, Independent Adviser on Biometrics & RFID

Peter Hawkes

Biometrics 2009 was the 11th in this annual series. As usual it was held in the QE II Conference Centre in the centre of London. It began on October 20 with the first of the three-day conference. The associated exhibition ran in parallel on Days 2 and 3.

As I noted in my report on last year's event this meant that on those two days, conference delegates had to choose between the Exhibition and one of the two parallel conference streams. This may have been tolerable in the early years. But now the exhibition is attracting more and more significant Exhibitors. I noted that most Session chairmen of the Conference were severely limiting discussion of the presentations. Presumably they were under pressure to get delegates down to the Exhibition.

The end result for me was that I only managed to spend significant time at just a few of the 47 stands. This was a pity. This year's Exhibition exceeded the previous year in both quality and quantity of Exhibits.

The delegate list showed over 200 delegates. This was only a small drop from last year. This is creditable considering the worldwide recession. The delegates came from many countries. American delegates were especially numerous. The proportion of delegates from user organisations was around 20 %. These were mostly from Government departments and agencies.

Selected contributions and themes

1) From Sagem Securite

Sagem had one of the two largest stands in the Exhibition. The demonstrations on the stand included two novel products for biometric identification. These were contactless fingerprint capture and combined fingerprint and finger vein matching.

The former is described as "Finger on the Fly". All four fingers on one hand can be scanned at once. There is no contact between the capture device and the scanned fingertips. Accordingly the pressure distortions of the fingertips associated with "rolled" or "flat" methods of live fingerprint image capture are eliminated. Cross matching between images made by contactless scanning and flats or rolled images will not be easy. However this will not matter for many applications. Given suitable standards matching between enrolled registered samples and bid samples for authentication should be straightforward. I suspect that the technology would be especially useful to people with arthritic hands.

Combined fingerprint and finger vein matching comes about as a result of collaboration between Sagem and Hitachi. Hitachi's finger vein imaging method, "VeinID", is combined in a single device with Sagem Morpho's fingerprint identification technology. Reportedly this results in the only multi-modal biometric system suitable for both one-to-one and one-to–many matching. Given time many Government applications will result.

2) FBI "Empowering our partners to connect, identify and know"

This talk was given by James A Loudermilk II, a Senior Level Technologist at the FBI. His talk concentrated on the current and future database service activities of the FBI. These are mainly provided to the Law enforcement and justice organisation of the various States of the USA. The FBI's own investigations use less than 1% of capacity. The daily throughput of queries can be up to 250,000. Mostly these relate to the FBI fingerprint repository of some 390 million-fingerprint records. About 82 million of these are in automated systems. The DNA database holds 7 million profiles.

The FBI takes a long-term view of criminals. For example fingerprint records are currently being taken of suspect Taliban in Afghanistan. They could be checked if the person concerned attempts to enter the United States at some date in the future. A future "Killer Application" would be scene of crime identification by face recognition.

In the handling of queries automatic face recognition is not yet good enough to give reliable matches from One-to-Many searching. The available algorithms are not yet good enough. The ageing of the human face cannot yet be accommodated. So attention is being devoted to other biometrics. These include iris, voice and palm. For DNA fingerprinting, there has been the problem of the many hours required to produce a profile.

5
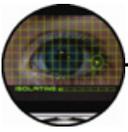
Based on early experiments to speed things up there is now an expectation that DNA fingerprint profiles could soon be measured in a few minutes. Soon means within 2-3 years.

3) On Iris Recognition

After a period in the doldrums, Iris recognition is making a comeback in a wide variety of applications. Apart from the FBI interest mentioned in 2) above there is use by the US Army in Iraq and Afghanistan. Various frequent flyer programmes continue to employ it. Professor Jim Wayman reminded delegates how useful he finds the UK's IRIS system as operated by the UK Border Agency at Heathrow Airport- no queuing on arrival!
For details of IRIS see: - www.ukba.homeoffice.gov.uk/technology/iris

Tienu Tan, Director, National Laboratory of Pattern Recognition, China mentioned in his talk that the country has some 10,000 coalmines. Iris recognition appears to be the most suitable biometric for use in the attendance systems now being operated in the mines. The harsh working conditions make fingerprint and face recognition unreliable.

Iris technology is still evolving. Dr Patrick Grother of NIST, USA, Mr Michael Thieme of IBG and Professor Valorie Valencia of the University of Arizona briefed delegates on aspects of this. Dr Grother reminded delegates that there are now more iris providers than for face recognition. He has tested 19 implementations for interoperability.

4) Biometrics in Schools

Alasdair Darroch is a Director of Biostore Ltd. See: - www.biostore.co.uk/

His talk covered the technology, the practicality and the ethics. He believes that applications in Schools including Library and Register constitute the largest non-government application of Biometrics in UK. He estimates that some 2 million pupils and students use biometrics for the above or other purposes.

Biostore, founded in 2005 is, he believes, the leading player. The market addressed by Biostore begins with a small specialised application. Library is typical. The convenience for the pupil is that a book can be borrowed even if he or she has left their library ticket at home. The Librarian does not need to cope with pupils using borrowed or stolen books. The price for an initial system is between £1000 and £1500. The system is modular. So the cost of adding new applications such as cashless catering to an existing kernel is small.

Student bars for 16-18 year old pupils are provided in some schools and academies. The amount of beer a student is allowed to drink in an evening depends on whether he or she is 16, 17 or 18. Fingerprint matching is the preferred method of Authentication in most applications. However there is a need for face recognition in some situations.

5) On Biometric encryption methods

These techniques are known by several names. Biometric Encryption (BE) is a common one. Others include Traceless Biometrics, Untraceable Biometrics, Revocable Biometrics and Anonymous Biometrics. BE promises to provide a valuable combination of strong authentication and personal data privacy. BE is not a new concept. To my knowledge, BE designs been in gestation since 1976. A good review of the State of the Art to 2007 is given by Ann Cavoukian and Alex Stoianov: - www.ontla.ont.ca/library/repository/mon/16000/271420.pdf

For a simple description of BE see the homepage of the TURBINE research project of the EC: - www.turbine-project.eu

The partners in this project include Sagem Securite (see 1) above), Philips Research (see below), University of Twente (see below) and Precise Biometrics AB (see 6) below).

A form of BE was commended to the UK Government for use in a National ID card system. This was a strong recommendation of the Review "Challenges and Opportunities in Identity Assurance" by Sir James Crosby to HM Treasury. This was published in March 2008 and a PDF of the Review can be downloaded from: -
 www.hm-treasury.gov.uk/identity_assurance_index.htm

So far as I know neither the Home Office nor the Identity & Passport Service has yet published their formal response to the Crosby Report.

6

At the Conference, two presentations were made on BE. Both originated from research in Philips. One was a research paper by Emile Kelkboom of the University of Twente and Philips Research. His title was "Relating the Analytical Template Protection System Performance with the Theoretical Maximum Key Size under Gaussian Assumption". For this he was, at the Conference, awarded the first prize in the 4th annual Competition run by the European Biometrics Forum. This was for the best Biometrics research paper by a student. Dr Kelkboom is a prolific author. Searching on his name in Google reveals numerous other publications.

The other presentation on a form of BE was given in the Session on "Enhancing privacy and ethics". It was made by an ex-Philips Research worker, Dr Michiel van der Veen. He is now CEO of priv-ID BV. This is a spin-out company from Philips. It formed two years ago. See www.privid.com

It aims to commercialise inventions in Biometric encryption and related matters. Some of these resulted from EC funded projects including TURBINE and 3D FACE.

6) Match-on-card/token

This has long been a speciality of the Swedish fingerprint matching company, Precise Biometrics AB (www.precisebiometrics.com). As proof of this, one of the company's US Patents dates back to an Application first filed in July 1999.

If the only record of a person's fingerprints is one held locally in the memory of his eID card then Match-on-card provides the authorised cardholder with a significant level of personal data protection. However it would be even more secure when combined with the BE method.

The disadvantage of card-only based ID card systems arises from the lack of a central database populated during enrolments. One-to-many searches during enrolment throw up any person with multiple identities. Not surprisingly Law Enforcement and other government departments favour the "de-duplication" thus enabled. When used with a central database of biometric characteristics Match-on- card reduces the volume of message traffic to/from the central database.

This year's contribution to the Conference by Precise Biometrics was entitled "Moving faster with Biometrics". The Author, Oscar Fogelberg, is Project Manager, Match-on-SIM at Precise Biometrics.

He was unable to be present. So the talk was given by a colleague, Mr R Petersen. The proposed system is being designed to speed passenger movement through airports. Since 2007, Scandinavian Airlines (SAS) have been using a fingerprint based passenger baggage reconciliation system. This was developed for it by Precise Biometrics.

Frequent fliers are issued with a smart card. The card chip contains a record of the cardholder's fingerprint template. When baggage is checked in at the airport, the passenger's fingerprints are matched to the card record. This matching is repeated at the Boarding gate. This ensures that items of passenger baggage are specifically linked to the person actually boarding the aircraft. The system meets European regulations.

The presentation then described the results to date of collaboration in marketing and technology development between Precise Biometrics and IER of Paris. IER is a leading supplier of airport gating systems. See www.ier.fr/
Precise has adapted its "Match-on-card to "Match-on-SIM" in a mobile phone.
Some of the advantages of using a mobile phone/SIM combination as an identifying token are spelled out by Jonas Anderson of Precise Biometrics in an article in Card Technology today for April 2009, See: - www.precisebiometrics.com/?id=3800

These advantages include the provision of a display and key-pad for user interaction.

7) Challenges in incorporating biometrics in PC clients for consumer and commercial markets

Vali Ali is Distinguished Technologist in the Personal Systems Group of Hewlett Packard. His talk was delivered with consummate style.

At HP, he has to make decisions on whether and how to incorporate biometric devices such as fingerprint scanners in laptop and desk top PC's. Both commercial and domestic customers expect much from biometric methods for logical access to their systems.

The hardware cost of even slide bar fingerprint sensors erodes profit margins. The biometric software must operate with near zero false non-matches. Given the choice between a $100 graphics card and a $ 0.00 fingerprint add-on the Sales Department tends to favour the graphics card.

7
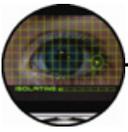
8) Dr Joseph Atick, Chief Strategic Officer, L-1 Identity Systems

Dr Attick delivered a keynote speech "Biometrics: enabling a world without barriers". The World is experiencing unprecedented trans-national population movements. Concurrently, it is going through a period of "hyperfocus" on identification, whereby many daily activities now require proof of identity. Post 9/11 ICAO accelerated plans for biometric e-documents for international travel. The scrutiny of passengers at ports and land border crossings result in delay and frustration. Some amelioration can be expected as Automatic Border Crossing (ABC) is deployed. However, the challenges for National governments are less technical than political. Traditional visa issuance by interviews at Embassies is NOT scaleable. Self-service enrolment methods carried out by local agents such as Retailers are going to be used more and more. In the longer term the passport documents themselves will be replaced by applets in the SIM of the traveller's mobile telephone.

He also reminded us that only some 8% of the world's population ever has a passport. There are huge numbers of people who are homeless. These include migrants, refugees and "street people". One estimate is that there are 100 million people without a home. Many such people are never the subject of records. As many as 1 in 2 births in India are not recorded.

Top of my list would be the scope for Biometric authentication in remote transactions such as fixed line, mobile and Internet banking and shopping.

As an example there are promising developments from a small company called Axsionics AG. Axsionics is based in Biel, Switzerland. It is a spin out from the Berne University of Applied Science. The company/s Website is: - www.axsionics.com

I have not seen a demonstration of the device. However I have read the specifications of company's published patent applications. They include a novel camera for retrieving "Flicker code" from the user's computer or Mobile phone screen.

Also worthy of study is the technology of a Cambridge start-up company called Cronto Ltd. See: - www.cronto.com

The vision here is "Transaction Authentication with Cronto's Visual Cryptogram". The bank customer uses the camera in his mobile phone or a dedicated key-tag token to capture a cryptogram displayed on his computer screen. Cronto software downloaded into the phone or provided in the token is then used to authenticate the transaction.

Hopefully these two companies and their competitors are going to make more and more use of today's and tomorrow's mobile phones to improve security in Mobile and Internet Baking and related fields. Of the mobile phone makers, Apple seems to be in the lead in filing patent applications on biometric features which could be built into future versions of the i-Phone.

Once again Mark Lockie and Elsevier organised an excellent show. I learned a lot about a fast developing Industry and its customers. I have a feeling that next year's event will feature important new developments based on SIMs and mobile phone handsets.

The Landscape of eID programmes in Europe

By Infineon Technologies

This article will review at a national level the various projects for eID, eGovernment services, eHealth and eDriving License and on international/European level, and discuss related cross-border programmes. It will explore the impact of new standards on the technical requirements, e.g. security frameworks, biometrics data and data management. Finally it will consider the challenges for the eID market from a secure semiconductor point of view.

1. National Programmes on Biometric Passports in Europe

Back in June 20th, 2003 the European Council decided in the "Thessaloniki Declaration" on a coherent approach in the EU to biometric identifiers and biometric data for all EU citizens´ passports, for non-EU / European Economic Area (EEA) nationals and for the back office information system. In the Council Regulation (EC) No 2252/2004 of 13th of December 2004 the roadmap was published for the security features and biometrics in passports and travel documents, issued by the EU Member States (EU-MS). Since August 2006 all 27 EU-MS have switched to this new technology and issue only passports with an embedded security microcontroller with a contactless RF interface (ISO/IEC 14443) combined with at least one biometric feature, the facial image of the holder. A new generation of passports requires two fingerprint images by all EU-MS within the Schengen area to be stored. The deadline for implementation in passports was June 28th, 2009. The core data is protected by Basic Access Control (BAC), while the fingerprint data is secured by Extended Access Control (EAC) security protocols defined by International Civil Aviation Organization (ICAO 9303, part 1) and Brussels Interoperability Group (BIG), a working group under the article-6-committee.

The frontrunner for the migration to electronic Machine Readable Passports (eMRP/BAC) was Belgium who started issuing in November 2004, followed by Sweden in October 2005, Germany in November 2005, United Kingdom in March 2006, France in April 2006, Iceland in May 2006, Austria in June 2006 and Portugal in July 2006. Frontrunners for the second-generation eMRP/EAC are Germany with November 2007 and Latvia with March 2009. For the second implementation, finger scanners are needed in the document enrolment/issuance offices as well as the secure data channels to the office of the personalizing place of the booklet. Border posts may also be equipped with finger scanners for automatic entry to registered travellers, and for second level verification in some cases.

The annual replacement rate of MRP with eMRPs is round 10% with around 25 million pieces across all 27 EU-MS, meaning that from 2016 only eMRPs will be in use by European citizens.

2. National Programmes on eID/eGovernment in Europe

The main driver for eID/eGovernment programs is increasing of services (e.g. 24/7) and the target to decrease fraud. The result is that only data should be run between citizen and government and not the citizen themselves. Main applications are e-Government, e-Democracy, e-Voting and e-Business. To allow this process, the citizen needs to have some form of electronic identity (eID)

Eight of the 27 EU member states will have started electronic eID cards schemes by end of 2009. Starting with Finland in 2002, 2004 saw Austria and Estonia (2004), in 2005 Belgium and, Sweden and most recently in 2006 Spain and Italy and in 2007 Portugal. Besides EU-MS, Serbia has started a program, running in 2007. All nine eID programs are based on 2-factor authentications with a secure token ("to have" = identification factor) and a PIN ("to know" = authentication) or with Match-on-Card ("to have" = authentication factor). Portugal's government has decided that the citizen can use PIN or Match-on-Card for authentication.

Since 2003 a new application standard has been in development, (CEN TS 15480) for identification, authentication and signing (prEN 14890) the so-called European Citizen Card. Parallel to this standard for the secure token, a new standard (ISO/IEC 24727) is in progress covering the data on the token, the security for data and access to the data on the token and the protocol between token and reader addressing the middleware on the client-PC or on the card-reader in case of classe-3 reader. Some EU member states, like France (for 2009), Germany (for 2010) and Poland (for 2011) have announced plans to implement this standard in their upcoming national eID Card programs.

9

Some EU-MS define eHealth as a subset of eGovernment services. In this case the secure token supports more services. This is currently the case with card programmes in Austria (eCard), Italy (CNS) and Portugal (PEGASUS).

Some EU-MS have single factor authentication for eGovernment services in use, like UK (GATEWAY), The Netherlands (LIMOSA) and Norway (myPage). In this case only a PIN or password is requested via a website with no token required.

Many governments within the EU member states believe that a national electronic ID (eID) card should only be implemented after the second-generation ePassport is issued, because it would use similar technology to the ePassport. There are two key reasons for this approach:

- Reuse of infrastructure, such as data capturing, PKI, IT-Network, border control systems, will be more efficient and cost effective

- To increasing security inside the Schengen area, since ID cards will be more difficult to counterfeit

In Europe, typically 20 percent of residents have ePassports and about 80-90 percent of residents hold ID cards. In most of the member states, ID cards are mandatory. For travelling in Europe, the ID card is the typical and most popular travel document. Therefore, to increase security at the borders, the ePassport can be an alternative to the eID card for EU residents when the new border control process is in place.

The first example for a national eID card program was started in Sweden. This document includes the new ICAO technology, with eID/eGovernment Services on national level but with two physically separate devices in the card.

Contact-less (ISO/IEC 14443)
= Travel Function (ICAO 9303)

Contact-based (ISO/IEC 7816)
= eID/eGov Function (CEN TS 15480)

3. National Programmes on eHealth in Europe

Economic aspects are the key driver for eHealth programmes. eHealth means change from paper based data management of citizens, insurance, medicals and services to paperless workflow. eHealth systems require health professionals and insurance organisations to work with digital data of the citizen. Based on this approach, cost reduction in operation and reduction of fraud must be balanced with privacy and security.

A second important aspect is the political perspective, i.e. to protect human capital on a national level and improve services to the citizens.

Two mainstreams for data management are in use in Europe:

1) Central data management system (data on host)

2) De-centralised data management system (data on secure token)

Examples for the former are in UK with health professional "spine" cards that permit access to patients electronic health records held on a secure national extranet called N3 and Spain, called TASS for patients and health professionals to identify and access some health records.

Examples for the latter are France (Sesam Vitale 1G/2G), Germany (KVK, eGK), Slovenia (HIC), Poland (KUZ) and Italy (CNS) used a token to verify identity for medical insurance payments and access medical records

Beside the data management policy the data content is a characteristic of the eHealth program. Each EU-MS have selected its own application framework.

10

Examples in the G5 are

- Spain: Patients insurance data and employer

- Italy: Patients prescription, insurance data, e-signature

- France: Patients and clinicians services: prescription, emergency data, insurance data, medical records, e-signature

- Germany: Patients and clinicians services: prescription, emergency data, insurance data, medical records, e-signature

- UK: Clinicians access to medical records, e-signature

Single applications with secure token on eHealth are running in Europe in Spain, France, Germany, Poland and Slovenia.

International standards capture electronic health record (ISO/IEC 13606); communication standards (ISO/IEC 18307), framework for identity management (ISO/IEC 24760) and on eHealth card (CEN TC 251).

4. National Programmes on eDriving License in Europe

Feasibility programmes have been done in the past e.g. in the Netherlands (2009) based on the new international standard for eDriving licenses, ISO/IEC 18013. Discussions at the transport ministries on e-driving license have also taken place in Spain and Sweden. The UK has declared it may set up a feasibility study in 2009/10. The business case for an eDriving License will be defined at the national level by EU-MS and might for example be linked to driver entitlements, road tolling or traffic law infringement "points", plus the need to identify the driver when an eID is not available.

5. European Programmes with focus on cross border services

Within the EU MS citizens may move freely to visit, work, study, live and retire. The services of their native state must be available to them in any location with functions provided by the local government services. To facilitate this service, different directorates and units of the European Commission have various programmes running. The following table is not complete, but gives an impression on the topics the EU is working on:

- ICT/LSP STORK: (Secure idenTity acrOss boRders linKed) eID/eGovernment Services cross border project funding; started 2008 is working on electronic gateways for identity credentials to be authenticated across the EU

- ELSA: European Large Scale Action; is the programme beyond STORK; starting 2010 looking at electronic identity management (eID) infrastructure http://ec.europa.eu/information_society/tl/research/documents/ict-rdi-strategy.pdf

- ICT/LSP epSOS: eHealth Services cross border interoperability; funding; started 2008 has 26 members from 12 countries to develop a practical eHealth framework infrastructure that will enable secure access to patient health information patient summaries and ePrescriptions between different European healthcare systems

- PEPPOL: eSignature Services cross border; focus on B-2-B; funding; started 2008 (Pan-European Public eProcurement On-Line) has 8 countries looking at using eID for facilitate online authentication of transactions

- NetC@rd: Cross border cost reimbursement of health services; funding; started 2004 to introduce an pilot eEHIC: electronic European Health Insurance Card (previous E111 document); application by a consortium of 15 EU MS in 2010 (see www.netcards.eu)

- HPRO: is investigating the creation of a federated network of health professional registration; the feasibility study; by a French and Belgian consortium started in 2008 for 18 months to allow free movement of clinicians and recognition of their expertise by different health authorities. (http://www.hprocard.eu/)

- MEDEA+/BioP@ss: biometric authentication for internet services with secure token, funding; started 2008 to look at the standardising the European Citizen Card program (www.medeaplus.org)

- TURBINE: TrUsted Revocable Biometric IdeNtitiEs is working on improving the quality and

11

reliability of fingerprints for use in eID applications started 2008 with a consortium of 10 partner organizations www.turbine-project.eu

- EPAIC: an initiative and working group (The PortIDS Consortium) including Trasys and Qinetiq to increase the security at sea ports in Europe. They are looking at the development of a European Port Access Identification Card

This list is a sample, the EU via such programmes as the EU IST 7th framework and EU justice directorate fund numerous projects to improve the lives and security of it citizens. The overall implication is that there will more effort and funding in this sector in the next decade.

6. Challenge for the security industry, from a semiconductor point of view

Identification of new market requirements on memory size, performance, interfaces and security is the key. One example is memory size: First generation biometric passports in 2005 needed 32k bytes EEPROM in a contactless microcontroller for store basic data and a photo of the face, the second generation biometric passports required around 64k bytes EEPROM to store additionally two finger scans and an access key in the contactless microcontroller. The new national eID card programs in France (2010), Germany (2010) and Czech Republic (2010) request 100k bytes or more EEPROM to allow space for more applications which maybe loaded post issuance.

On the security front the lifetime for RSA_1024 and SHA_1 is being considered by authorities and there is a trend to move from 3key/3DES to AES. In addition, the attacks on the basic silicon to extract keys and data are becoming more sophisticated. As a reaction to this need for more powerful security, Infineon developed a the new family of crypto-controllers, called SLE 78 family, having a dual CPU, full error detection over the complete data path and full internal encryption. This innovation in architecture represents a paradigm change for the secure silicon industry. The SLE 78 family supports RSA_2048, ECC_256 and AES with 16 bit processor and crypto co-processors, and is designed to meet the highest security demands from current and new applications in the public sector for and provide a secure platform for identity products.

World News In Brief

World's First Commercialised Light-emitting Payment Card, Winner of SESAMES Award 2009

Oberthur Technologies has launched Smart Lumiere, an innovative light-emitting contactless card, which has emerged as the winner of this year's Loyalty SESAMES Award.

Available in either dual contactless-EMV or pure contactless configuration, Smart Lumiere emits light when it is entered in the field of a contactless reader to inform the cardholder when a transaction is taking place.

Smart Lumiere is the next evolution in Oberthur Technologies' pioneering work in the field of contactless payment devices. Comprised of a translucent plastic core, antenna and illuminating light apparatus, this commercialised payment card meets ISO 14443 dual interface contactless payment standards. It is also the first light-emitting payment card to be ready for use in pilots.

FEEL-ID Finally Unveiled

The Munich based security specialist, Giesecke & Devrient (G&D) has developed an interactive feature known as FEEL-ID, which systematically combines multiple security technologies in order to achieve maximum protection against counterfeiting. This exciting new product from G&D is already been presented at this year's CARTES & IDentification exhibition in Paris.

FEEL-ID is a feature that reacts to changes in temperature by utilising the thermochromic properties of the materials employed. Identity documents such as national ID cards, driver's licenses and passports can be authenticated rapidly and reliably using techniques as simple as rubbing them with your finger.

ViVOtech Partners with Citi in Largest Global NFC Pilot

ViVOtech has announced that its NFC mobile payment wallet, Over-the-Air (OTA) provisioning, smart posters, coupon delivery and redemption technologies have been successfully deployed in Citi Tap and Pay. It is a pilot service that brings to India next-generation contactless credit card payments based on this emerging technology.

Infineon Microcontrollers are used in China's New e-Passports

Infineon Technologies AG has announced that the Chinese government is using the company's security microcontrollers for its new electronic passports, which is volume-wise one of the world's two biggest electronic passport projects. The delivery of microcontrollers has already been started by this company.

From 2010, the Chinese government will issue electronic passports expected to number about 6.5 million annually, to citizens, diplomats and government workers. As of the first quarter of 2010, all new Chinese passports will be e-passports. Chinese citizens at present hold about 30 million passports, usually valid for 10 years.

Only 15% of Indian Enterprises have Proper Data Loss Prevention Measures

A study made by the intelligence marketing firm IDC (India) Ltd. has revealed that the increasing use of IT infrastructure has led to growth of security risks such as loss of critical data, besides enhancing productivity and expanding a company's operations within and outside the country.

"About 80% of Indian enterprises have agreed that loss or theft of critical data is a serious information security risk they face after threats from viruses and hackers", according to the survey commissioned by security solutions provider Symantec India.

Though enterprises have been investing heavily in building their IT infrastructure for end-to-end efficient operations, adoption of technologies to prevent or detect data loss has been very low due to lack of awareness or seriousness over the consequences of the risk.

The survey, conducted in August 2009 involved heads of IT infrastructure in verticals spanning banking and finance, manufacturing, media and entertainment, telecom, and IT and IT-enabled services.

Is U.S.A Willing To Pay Less for Online News?

It seems that Americans are less willing than people in many other Western countries to pay for their online news, according to a survey conducted by the Boston Consulting Group in October this year. When asked how much they would pay, Americans averaged just $3 a month compared to the Italians who are ready to pay less than half of $7 on an average.

The study was done based on a survey of 5,000 people. It found that among regular Internet users in USA, only 48% prefer paying to read news online, including on mobile devices. That result tied with Britain for the lowest figure among 9 countries, where Boston Consulting made surveys. Compared to this, in several Western European countries, more than 60% said they would pay for digital news.

Human Recognition Systems, First Time at AOA's 2009 Annual Conference and Exhibition

For the first time, Human Recognition Systems (HRS), a leading provider of biometric and identity management solutions, will be showcasing their technology - the latest advances in 'at a distance' iris biometric technology, exhibiting how this unobtrusive form of biometric capture and identification is ideal for mass iris recognition at the airports. It will be displayed at the Airport Operators Association (AOA) annual conference and exhibition 2009, to be held on 7-8 December at the London Hilton Metropole hotel.

Sagem Orga and Twinlinx offer World's First NFC Sticker with Phone Connectivity

Sagem Orga and Twinlinx have presented a mobile contactless sticker powered by the Twinlinx "MyMax" and Sagem Orga Java Card(tm) technologies at Cartes 2009. This interactive "SIMply Mobile Wallet" sticker adds Near Field Communication (NFC) capability to existing and future mobile phones and can be managed securely over the air (OTA). Compliant with ISO 14443, SIMply Mobile Wallet solution is providing help in kick-starting the market and the mass deployment of NFC applications in the near future.

Gemalto Announced its 2010-2013 Development Plan

Gemalto has announced its Development Plan for the period 2010 to 2013. Through revenue growth and margin expansion the company sets for itself an objective of expanding by more than 50% its Profit from operations, to €300 million in 2013.

Gemalto also announces intention to initiate a dividend distribution to complement its existing share buy-back program. The company even plans to propose a dividend of between €0.20 and €0.25 related to fiscal year 2009 at the next annual general meeting of shareholders to be held in May 2010.

Each business segment - Mobile Communication, Secure Transactions and Security, is expected to expand its profit from operations. Secure Transactions and Security are expected to contribute significantly to the company's profit expansion throughout the period, and to deliver high single digit profit margin from operations in the next year.

13

Smart Cards: Asset or Expense?
By Stan van Haasteren, Bell ID

Stan van Haasteren

Until recently, it was relatively inexpensive for banks to issue credit and debit cards to customers. With the migration to EMV, banks are however now faced with higher expenses as EMV cards, which contain a chip, have the value of 10 traditional magnetic stripe cards combined. Suddenly, production costs are sizeable. With many banks under pressure to cut costs, it is very tempting to go for the least expensive option. However, this might turn out to be a false economy.

With the low production cost of a magnetic stripe card, it is no surprise that most people own an abundance of magstripe cards given to them by banks, shops, employers, libraries, and loyalty schemes. Magstripe cards are personalised only once and cannot be changed afterwards. If the card is lost, the PIN is blocked, or is compromised due to fraud, and the customer gets a new card for free.

Accountants treat items that are cheap, plentiful and disposable as expenses; they have no book value after being purchased.

Nowadays, many banks are upgrading to the EMV standards in order to improve card security. EMV cards contain a chip as well as a magnetic stripe and are therefore not as cheap (between one and four US dollars). For banks, the fact that all of a sudden they issue cards that are more than ten times as expensive requires a different mindset.

Now, banks cannot carelessly issue as many cards as they like anymore. They have to think about the number of cards they issue and maximize their potential. Instead of treating cards as expenses with no book value, they should treat cards as assets with growth potential. Cards are investments that must be managed in order to maximise return on investment.

EMV Example

Let's consider an example of two banks upgrading to EMV. Both banks have one million customers. Bank A goes for the least expensive option; customers receive a $1 chip card with a proprietary operating system. It buys an EMV data preparation engine (to generate the commands necessary to personalise the cards) and leaves the card validity as it is: three years. Initial system upgrade costs are relatively low: $300,000 (180,994 GBP).

Bank B decides that the EMV upgrade is an opportunity to invest in the future. It issues more expensive $2 smart chip cards with an open platform operating system and a cryptographic processor (to enable RSA cryptography). It buys a card management system with the capability to add applications or change paramaters on cards after issuance. It extends the card validity to four years and decides that customers that own a debit card as well as a credit card will now get one card containing both applications. Total system upgrade costs: 1 million dollars.

The first impression is that Bank A got the bargain; it performed a relatively cheap upgrade and can continue with business as usual. It has lower initial costs and issues less costly cards. The truth may be, however, that Bank B saves more money in the long run. This is due to three reasons: less cards, longer card validity, and less re-issuance.

By combining debit and credit card applications on one card a bank can reduce the number of cards drastically. All customers who now own a debit card and a credit card will have only one card. Since the popularity of pre-paid debit cards is on the rise in many countries it could be a very attractive option to issue 'combi-cards'.

Extending the card validity means that the bank has to renew less cards every year. And because of its capabilities to change a card's parameters or add applications 'post-issuance' Bank B has to re-issue less cards. Currently, roughly 35% of all cards have to be re-issued before the expiry date. This was never a problem for the banks previously, because the cards were so cheap. Not anymore.

Bank B would only have to re-issue a card if it is stolen or lost. If a PIN is blocked, it can reset the PIN on the card's chip. Bank A would have to replace cards with a blocked PIN. Besides, BANK B's customers would not have many blocked PINs because the bank bought a card management system with PIN change

14

facilities. Therefore, customers can change the PIN generated by the bank to a number they can remember more easily (for example their date of birth).

Post Issuance Personalisation (PIP)

If card parameters would change (for example because the credit profile of the customer is upgraded) Bank B can modify the existing card because it supports scripting. The next time the card is entered in an ATM the bank sends a script to the card to change its parameters. Bank A, however, would have to re-issue a new card.

Bank B can also add applications to an existing card. Let's say a debit card customer applies for a credit card, then the credit card application can be added to the card by entering it in a 'post issuance personalisation' (PIP) kiosk in the bank's branch building. Bank A has no such facilities and would have to issue a separate credit card.

For these reasons Bank B will spend less money on card issuance and will save more money in the long run, even though its initial costs were higher.
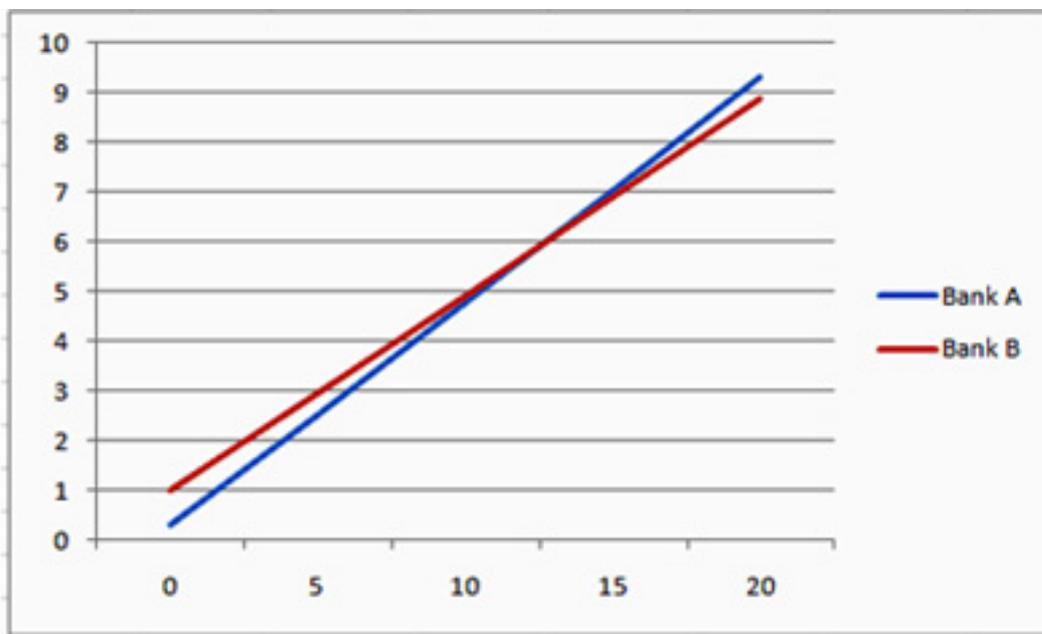
This is just a calculation example to illustrate how an initial investment can save money in the long run. However, in the real world, Bank A would probably have to spend a lot more money sooner than expected. It has bought chip cards with a proprietary operating system. This works fine initially, but once the honeymoon period is over the system will turn out to be very inflexible and not future-proof.

Bank B's chip cards have an open platform operating system and can therefore upgrade easily should business circumstances or technological changes dictate this. Thanks to the facilities to change parameters and add applications post-issuance Bank B has given itself the flexibility to respond to changing circumstances quickly without having to re-issue existing cards. Bank A lacks this flexibility and will probably have to invest money soon after the EMV upgrade to update it again. An additional problem is that the bank will be locked into the vendor, meaning that desired upgrades could be expensive or technically impossible. It could be better to buy a brand new system.

Another benefit of the ability to make changes to an existing card is that customers appreciate it. They do not like having to wait until their new card arrives.

Customers also value the improved security of their card thanks to its RSA-enabled crypto processor. It means the cards can be used in offline Point of Sales (POS) terminals, vending machines or parking meters. Customers of Bank A will not be able to use their cards here.

PIP facilities also open up all kinds of other opportunities. The bank could decide to load loyalty applications such as Airmiles or Welcome Real-time to the card. Other applications, such as health care applications, are also a future possibility.

15
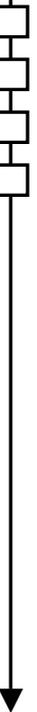
Card Management System (CMS)

A good Card Management System (CMS) is essential in order to be flexible and future-proof. Without it, a bank does not have a handle on its cards and the applications they contain. The role of the CMS is to be the spider in the Web between all the different elements involved in banking; the cards, their applications, application providers, cardholders, ATMs, card personalisation bureaus, card printers, EMV templates, cryptographic key material etc.
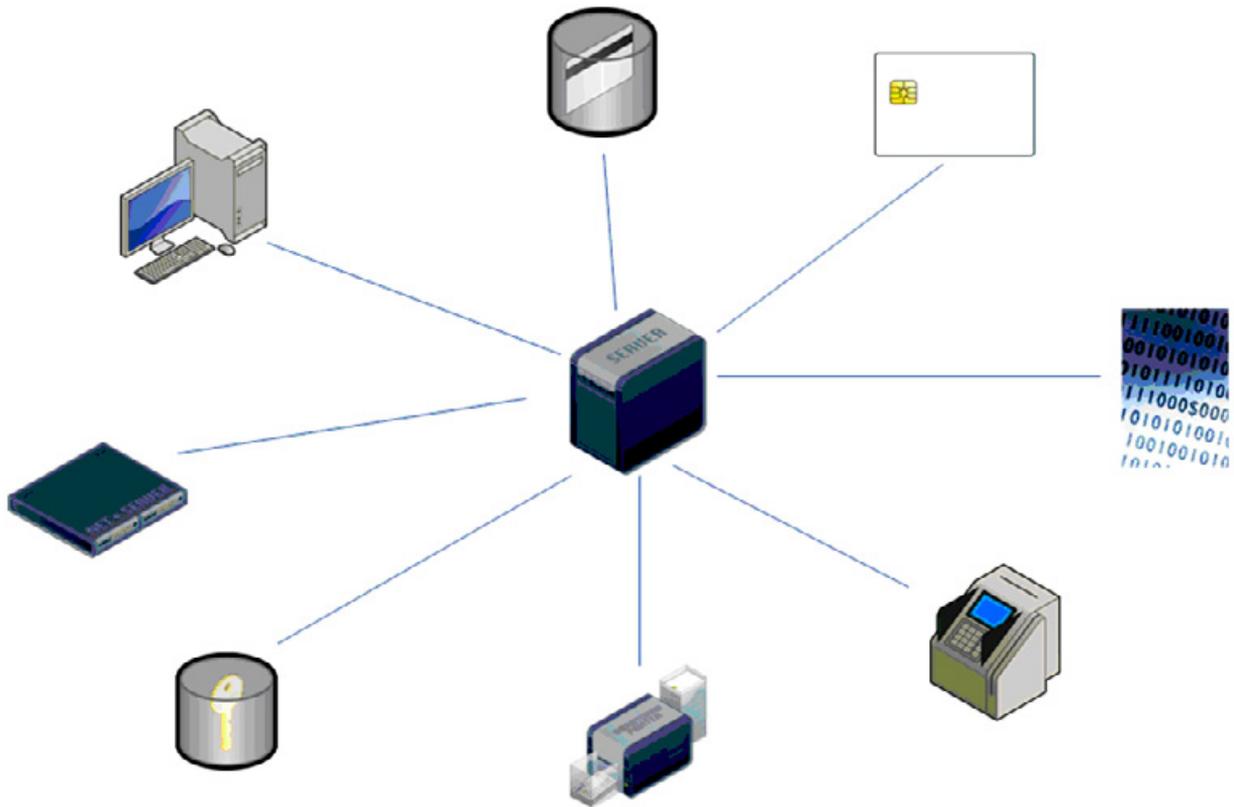
The CMS keeps track of all the related data and manages the lifecycles of cards and their applications, from the moment a customer applies for their first card until the card's end of life. It provides standardised interfaces to all elements. Should one of these elements be upgraded or replaced the system will not fall apart. A simple adaptation in the CMS will ensure all elements keep working together.

Without a CMS, maintenance could turn out to be a nightmare. If one element changes, it will be hard to know where to start making the other elements compliant. Because a quick fix could lead to different problems somewhere else.

Upgrading from magnetic stripe cards to smart chip cards is a complicated operation. It requires a long-term view and a change in mindset. Cards should no longer be seen as cheap and plentiful, as expenses with no book value. They are assets that open up many new opportunities. Therefore, they should be carefully managed.

16

SESAMES Awards 2009 – The competition watched by the whole industry

By Tom Tainton, Smartcard & Identity News

Tom Tainton

Every year, 10 SESAMES Awards are presented to the industry's most innovative products, celebrating the best projects on the market. Selected by a panel of experts, the awards will be presented on the eve of the opening of Cartes & Identification 2009, at a prestigious ceremony in Paris. The accolades are regarded as a global standard for card manufacturers and give the winners a reputation and credibility that guarantees the success of their project. The event is a unique opportunity for the finalists to showcase their achievements to professionals, exhibitors and journalists attending from all over the world.

It's no surprise that the competition attracts a growing number of candidates every year and 2009 was no exception. A total of 309 applications were filed for this year's SESAMES across a variety of categories. These include the Hardware SESAME, awarded to the industry's most ground-breaking card, token, chip, electronic component or terminal. The winner in this sector was Gemalto with Contactless VDHR, a high-data-rate application standard which ensures secure transfer for contactless smartcards. The other finalists were Oberthur Technologies with Smart Lumiere, a dual interface payment card, and Twinlinx with MyMax NFC Sticker, a thin electronic sticker designed to upgrade Bluetooth phones with NFC functionality.

The second award, the Software SESAME, promotes a sector that lies upstream of the market and includes operating systems, algorithms, software for access management, and test or audit tools. The winner for the software category was Sagem Orga with T2TIT, a self-configuring wireless network that enables communication between a web portal and other objects. The other finalists were Collis with NFC proxy concept, an NFC application and Oberthur Technologies with Chrysalis Fly EAL4+, a dual interface payment card.

The Identification SESAME showcases the strongest biometrics, RFID and identity management products. The award was won by JDSU with HoloFuse, a product that integrates holography with clear polycarbonate, effectively eliminating the need for adhesives. The other finalists were Oberthur Technologies with ID-One Sky, a physical polycarbonate security feature, Inside Contactless with MicroPass 5100, a cost effective solution for creating driving licenses and Infineon Technologies with SLE 95050 ORIGA, an authentication device.

The IT security SESAME recognises logical control access and electronic signature applications. The winner was Neowave Sas with Weneo ID Corporate Bundle, a smart object that helps organis

ations protect their informational and physical assets. The runners-up in this category were both Gemalto products -.Net Bio for Windows 7, and digital signature adoption, an online authentication application.

The Transportation SESAME acknowledges products in the fleet management and transport sector. The winner was ERG Transit Systems with eO, an account based fare collection system. The other finalists were Neowave Sas with Weneo Duo, a contactless smartcard chip, Watchdata with CEPAS 2.0, a transport card trialled successfully in Singapore and Xiring with The Smart cardholder, a dynamic security solution.

The Banking and Finance SESAME was won by Hypercom with the HyperSafe Remote Key System, a solution that enables PIN encryption keys to be downloaded remotely. Finalists included Gemalto with Ezio Touch Reader, an authentication device for online transactions and Giesecke & Devrient with Convego Air Mobile, an NFC sticker for making contactless payments.

The Health Care SESAME was awarded to Gematik with their unique eHealth-Portal, a web-portal solution to authenticate patients. Runners-up were Xiring with Prium-3S Barcode, and Laerdal Medical with the CPR Card.

The Mobile SESAME category includes mobile commerce and GPRS applications. The winner was Gemalto with Massim, a machine-to-machine SIM card that detects theft. The other finalists were NXP Semiconductors with PN 544, an NFC handset chip, Oberthur Technologies with SIMsense, a motion detection SIM card and Toro with Akami, an NFC mobile wallet product.

The e-transactions SESAME recognises e-government, virtual payment and secure transaction applications. The winning product was Monext's Sign4Pay, a payment method using WPKI services. The other finalists were Crealogix e-banking with CLX Sentinel, an e-banking token, Hypercom with HyperSafe, a PIN encryption solution and Xiring with Connectable Xi-Sign solutions, a solution designed for visually-impaired users.

The Loyalty SESAME was won by Oberthur Technologies with Smart Lumiere, a dual interface light card technology. The runners up in this category were MasterCard with PASS-MasterCard, a wireless merchant terminal and ATOS Worldline with Multi Product Cards, a multi stage payment module.

17

Public Transport and the wider scene: Rollin Rollin Rollin

By Peter Tomlinson - Smartcard & Identity News

Pe*ter* Tomlinson

Move 'em on, head 'em up,
Head 'em up, move 'em out,
Move 'em on, head 'em out Rawhide!
Set 'em out, ride 'em in
Ride 'em in, let 'em out,
Cut 'em out, ride 'em in Rawhide.

(Ack. Ned Washington)

Public transport has been exciting conference organisers this year. Not surprising, for many feel that we should do it better, including better harnessing the skills that we have. As a result, there have been several fires smouldering in the background for some while. Some keep bursting into flames, but one, like at a remembered bonfire party in the pouring rain, failing to ignite – and the firelighters appear to have run out. Too many spectators are out in the cold, while others think they are being taken for a ride, and Lord Adonis is half way into a 12-month crusade to lead from the front. Where this year's series of conference reports particularly apply is in the area of tickets, other permits to travel, payment, journey management and reporting, but first a look at the bigger picture.

When we study the use (or not) of secure tokens for both public transport and more general citizen services, we see four government departments variously involved. Three such support low cost, useful, medium security tokens in the hands of citizens: Department for Transport (DfT) first, then Department of Communities and Local Government (DCLG) and Department for Work and Pensions (DWP). Separately, Home Office with DWP are placing quite secure tokens in our hands and wanting to do more: passports, eBorders cards, and now ID cards. But we are out of line with several other EU countries and with the Commission's plans: we don't do eID here (not yet, anyway: Meg Hillier, honest and straightforward Minister, at the autumn 2008 Porvoo conference: "we have to walk before we can run"). Uniting the various schemes and aspirations is not yet possible, so here we concentrate on the medium security tokens.

The fire gone cold is in DfT – they started with a Vision. A summary of that came recently from Trevor Crotch-Harvey (Fenbrook Consulting), who worked on the Detica study for the recent DfT ticketing strategy consultation. Here is the summary – and a critique.

ITSO smart ticketing on all public transport

That doesn't mean full capability in every scheme. London's TranSys scheme upgrade leads here: full function Oyster, but acceptance only (no sales) of selected ITSO format Products. ITSO's current core specification is 6 years old, ticketing for high traffic volumes in metropolitan areas can now be done better – but first the Integrated Transport Authorities / Passenger Transport Executives (ITAs/PTEs) want simpler, fully interoperable transport services (with "fair fares"). And the straitjacket into which DfT put ITSO a long time ago (see below) causes great difficulties.

Local integrated ticketing schemes with multi-operator tickets widely available

ITAs/PTEs want universal tickets within their areas, and "fair fares"; other metropolitan areas want the same

Schemes interoperable with each other to allow seamless travel

Again the DfT straitjacket makes that impossible at the moment

Contactless [bank or eMoney] payment cards may increasingly be used for low value transport transactions

Three ways to do this: as a method of payment only (as Stagecoach are doing on their buses in Liverpool); storing the ticket in the payment chip via an EMV specification extension; storing the ticket in a separate

18

application in the payment chip (ITSO or proprietary)

Mobile phones could in time replace smartcards

No: they are another carrier, often more useful than smart cards (visibility of the ticket, pre-selection of the ticket or payment method for the next journey, over the air purchase and download)

Increasingly innovative price structures, loyalty schemes, etc

Most passengers want simplicity, not commercial jostling for position

Provision for cash transactions and 'the unbanked'

Of course – but get the cash off the buses in urban areas

14 months ago, DfT approached ITSO Ltd to buy the Company. Not so: can't – it's a Membership Company and its M&As restrict what the Members can do with it. DfT came back, proposing taking control of the Company's Board, to direct and fund the Company to really, really enable integrated and smart ticketing across all of surface and sub-surface public transport in Great Britain. Last June, a significant majority of the ITSO Members who attended an EGM voted for DfT to have a go for three years maximum. Almost 6 months on, there is only a Vision, but no plan and no money. Maybe never more than a token amount of money, apparently recalled as part of the current cost reduction exercise in DfT – but hold the printing presses: the very latest is that there is funding for 4 months (to the end of the financial year) for an extra body in ITSO Ltd.

Yet the ITSO methodology of linked, interoperable schemes, with its supporting goods and services (security module, key server, VPN, certification service) has recently developed a momentum of its own. Rolling out across Scotland, already there in some LAs in England, starting up in Wales. The baseline is concessionary travel on buses. Around 10 million ITSO-enabled smart cards issued, 2 million more in London in 2010. No matter that only about 10,000 buses are smart enabled, because the commitment to many more is there. Supporting this is the loose co-operative of scheme owners: ITSO Licensed Operators Group (ILOG), as recommended to DfT as long ago as 2004 during a wider but unpublished study for DfT and Office of the Deputy Prime Minister (ODPM). To fully support this growing deployment, the three administrations (England, Scotland, Wales) should arrange to directly regulate ILOG, rather than going through ITSO Ltd with its built-in conflict of interest caused by its 4 classes of members: public sector, two classes of service operators, and suppliers.

The wider desire is to combine further citizen service data and public transport data on medium security tokens. For England, ODPM kicked that off, but DCLG seems to have gone to sleep. Now DWP has come in, with the all-in-one card concept introduced in 'Building a society for all ages' – if they can bring the necessary expertise on board (DWP is in general a very competent dept in Information and communication technologies (ICT), they will specify several common platforms (cards and mobile phones).

The DfT straightjacket? All cards must be usable everywhere, and terminal implementations are the responsibility of operators. But station gates cannot decide which Product to use when there are several available! And interoperability requires common methodology in off-line terminals.

The big organisational task not done is key management at the secure platform level. Granted, when you start with a mindset for Mifare Classic®, you only have one level of keys: the data sector level – but most of those keys are in the databases of the contractors who do the personalising of the card. ITSO defines only the application level, not the smart media platform level.

There is an opportunity now to move on: within five years most relevant Mifare Classic® cards will be replaced by Mifare DESFire® or more general multi-application platforms, and many functions will become available via NFC mobile phones. There is a supply chain ready to go, here in the UK. It has invested and wants a return, has skilled and expert people, is ready to invest more if the market is there, and now has a trade association to speak for it (based at AIDC, now in Barnsley) www.aidc.org.

The lesson from Rawhide is that you have to both lead and drive - drive from behind and the sides.