Smart Card News • Smart Card News • Smart Card News • Smart Card News • Smart Card News • Smart Card
News • Smart Card News • Smart Card News • Smart Card News • Smart Card News • Smart Card News •
Smart Card News • Smart Card News • Smart Card News • Smart Card News • Smart Card News • Smart Card
News • Smart Card News • Smart Card News • Smart Card News • Smart Card News • Smart Card News •
Smart Card News • Smart Card News • Smart Card News • Smart Card News • Smart Card News • Smart Card
News • Smart Card News • Smart Card News • Smart Card News • Smart Card News • Smart Card News •
Smart Card News • Smart Card News • Smart Card News • Smart Card News • Smart Card News • Smart C
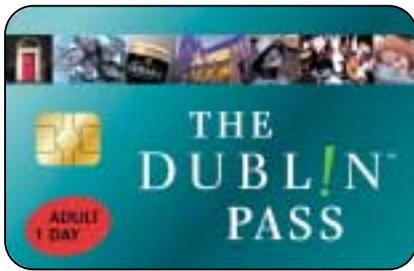
May 2004

Volume 13 • Number 5

Smart Card News

Smart Cards and Biometrics in Government • Finance • Health • Telecoms • Entertainment

www.smartcardgroup.com

04 • *ACT Delivers 'Dublin Pass' Smart Card Solution*

03 • *G&D Signs Agreement with Intercede*

18 • *Healthy Eating on the Cards*

03 • *HK SMART ID Card Wins Industry Award*

This Month's Lead Story

02 Trial Biometric ID Cards for UK

In This Issue

Regular Features

World News In Brief

Featured Articles

The Dublin Pass

The Dublin Pass's website opens with a front page which tells you about the actual pass and its benefits. The Pass brings together the best in attractions and services for the city of Dublin in one complete package. You can receive a discount on the card if you apply online however this is not possible as they are currently upgrading their online payment processing facilities. The website is very simple and easy to navigate.

The information on the website is very limited. This scheme introduced by the website is a good idea for tourists wanting to experience everything Dublin has to offer at a fraction of the price. Anyone one for a Guinness!

www.visitdublin.com/dublinpass

Navigation	
Content	
Appearance	

Atos Origin

The front page of this website is kept very basic with information relating to their latest news. The rest of the website is accessed through the very detailed. The website lays out the industries in which Atos are involved in and all the solutions they provide. The investor's section is also very useful providing the visitors with PDF versions of their accounts and a financial stock breakdown.

A very informative corporate factsheet is also available in PDF format on the website. The site is keep very plain in terms of design and has a good balance of visuals and text. As a member of the press their newsroom is very usful, featuring pictures of executives and cases studies.

www.atosorigin.com

Navigation	
Content	
Appearance	

UK Passport Office

The website as expected is generic to general UK passport information. However the sites navigational bar does have a whole section dedicated to identity cards and biometric passports. The website is completely text based, but does give a brief run down of the different schemes that are being purposed. The UKPS news section gives greater information and provides you with a PDF about the actual biometric trial being purposed for passports.

Apart from this the website provides very little information about the scheme and there are better sites out there providing more information. Anyone wishing to take part in the trial should contact MORI on 020 73473023 or email trial@mori.com.

www.ukpa.gov.uk

Navigation	
Content	
Appearance	

Smart Card on the Web

Trial Biometric ID Cards for UK

UK Home Secretary David Blunkett has outlined the Government's plans to introduce a national identity card scheme throughout the UK. A draft bill has been published that introduces a pilot scheme, set to start in April 2004, which will involved 10,000 UK volunteers. Part of this pilot involves the volunteers having their biometric details recorded including facial scans, iris and fingerprints.

The aim of the card scheme, that if fully implemented will hold the details of 60 million people in the UK, will help prevent ID fraud, human trafficking and illegal immigration, as well as stopping people from exploiting health and welfare services. Mr Blunkett stated "Within three years we will be in a position to start everyone having a biometric passport issued and along with it a biometric card - specific identifiers like the iris of your eye, fingerprint, facial recognition, which because we are putting this on a clean database will not be forgeable. People will not be able to have multiple identities."

This pilot follows a survey broadcasted by the BBC that revealed 80% of people questioned backed a UK national ID card scheme. The survey questioned 1,000 people within the UK using a MORI telephone poll. The main reason given by respondents for the adoption of a new ID card scheme was to prevent illegal immigration. The government is also seeing this poll as a positive step towards another weapon against terrorism. "As we have been saying, it also demonstrates a degree of trust in terms of being able to protect privacy which I'm very pleased about," said Home Secretary David Blunkett on BBC Radio 4's Today programme. However the survey also showed that 58% of the people questioned said they did not believe the UK Government would be able to introduce this ID scheme without problems.

Atos Origin as prime contractor has designed, built and will maintain the trial equipment and software. It is supported by a consortium of technology vendors; NEC are supplying its Automated Fingerprint Identification System (AFIS), Identix will provide the fingerprint capture and facial matching technology whilst the iris recognition technology is supplied by Iridian Technologies Inc.

This trial simulates a potential future biometric collection process; people will go through enrolment and then have their biometrics verified. To make the trial as realistic as possible, the participants' biometrics are compared against a database of anonymised iris and fingerprint images collected outside the United Kingdom and the biometrics collected during the trial. If no match is found the applicant's biometrics are added and the applicant is therefore enrolled.

The cost of this scheme is estimated to be around £3.1 billion and will pave the way for a compulsory national identity card system for all UK citizens

2003 Smart Card Shipments Figures

Eurosmart has published a report that shows the 2003 Smart Card shipment figures by region and sector together with their 2004 forecasts. The report showed that Memory Smart Cards declined by 15% and passed just below 1 billion-mark shipment (919 million units). Microprocessor Smart Cards showed a strong growth of 40% to a shipment figure of 979 million units. This upsurge is the first time in history that Microprocessor Smart Cards have outperformed memory cards shipments.

Eurosmart's report also showed that Wireless Telecom SIM Cards were up 56 % from last year with a strong growth of subscribers in all regions including Europe, development of GSM in North America and the impact of churn in China. Exceptional Q4 2003 volumes were shipped. Banking/ Retail microprocessor shipments reached 205 million units, which is an increase of 17 % on the previous year. Eurosmart's report then went on to state the trends that they predict would occur in 2004. They reported that there would be continued growth in Financial Services with EMV deployment and that Government and Corporate Security Segments will start to take off in volumes with growth rates above 50%.

Chip and PIN Increases use of UK Debit Cards

According to research by MasterCard, the introduction of Chip and PIN within the UK will increase the use of debit cards. MasterCard stated that four out of 10 people said they would use their debit card more often once chip and PIN cards were launched, while nearly a third thought they would carry less cash. They predict that debit card spending will rise by 37% once the new cards are being used, as the use of cash and cheques continues to decline.

ORGA'a Restructuring Completed

Juan Carlos Garcia and Oliver Jaster, the CEO and CFO of ORGA Kartensysteme, announced that the restructuring of the company has been successfully completed. Management is certain that ORGA will achieve a return on sales of 10% and recapture the number 3 spot in the international Smart Card industry by 2007. Sales in 2003 also developed more positively than planned.

ORGA concluded the fiscal year with sales of more than 180 million euros - approximately 20 million more than the figure announced last summer. 2004 is also going well, according to management. ORGA intends to continue investing in the future: research and development as well as marketing will be expanded.

Faith Lost in Passwords

The third annual survey into office scruples conducted by Infosecurity Europe 2004 of 172 office workers found that 80% of workers were fed up with using passwords and 92% said that they would rather be able to log on using biometric technology such a Smart Card or token. When asked whether they would feel happier using internet banking if their bank provided biometric and Smart Card technology to verify their identity, 86% of workers said that this would make them feel safer, and most of them said that it would also encourage them to use online banking as they felt it would make their information more secure.

Gibraltar Get Smart

Gibraltar is going 'smart' - thanks to the latest Wayfarer Transit Systems' revenue collections technology that will shortly be installed on the island's bus fleet. Working with the Gibraltar Bus Company, Wayfarer is supplying 26 Smart Card enabled TGX150 units for the bus network, together with card issuing bureau services and management data systems.

G&D Signs Agreement with Intercede

Giesecke & Devrient (G&D) has signed a reseller agreement with Intercede to provide MyIDT card and application management system components. MyID is an essential part of the G&D identity and access management integrated technologies, I-AM IT. The G&D I-AM Integrated Technologies solution incorporates Intercede's MyID products.
i

HK SMART ID Card Wins Industry Award

At their annual Smart Card industry awards the CTST international panel of experts voted the Hong Kong Special Administrative Region national ID project, SMART ID Card, as the breakthrough implementation project of the year.

Rated in terms of the project's technical proficiency, impact on the cardholders and volume of cards, SMART ID Card beat off stiff competition from the Taiwan National Health Project and the US DoD's premier Common Access Card Program.

Visa Wave for Contactless Card Payments

Visa Asia Pacific has announced Visa Wave, a Visa contactless Radio Frequency (RF) Smart Card that is fully compatible with the global EMV Smart Card standard. The first batch of 2000 Visa Wave cards have been issued by MBF Cards in Malaysia to consumers in a trial that runs until the 31 August 2004.

Gemplus Delivers 64K Cards for U.S. Govt's Smart Card Program

Gemplus International S.A. have obtained FIPS 140-2 validation of its 64K Smart Card equipped with the applet required by the Defence Manpower Data Center (DMDC) for the next phase of the U.S. Department of Defence's (DoD) Common Access Card (CAC) program. This makes Gemplus the first company validated to deliver Smart Cards that comply with the requirements for the next generation CAC.

ACT Delivers 'DUBLIN PASS' Smart Card Solution

Dublin Tourism has announced the launch of the DUBLIN PASS. The pass is the first visitor card in Ireland to use Smart Card technology. It was implemented and installed by Applied Card Technologies Ltd (ACT) and will be managed from ACT's Belfast office. ACT has provided Dublin Tourism with a comprehensive tourist package based on its Generic City Leisure (GCL) system.

MasterCard's Smart Card gains Momentum

More than 10 of the world's leading Smart Card vendors have signed MasterCard's M/Chip 4 Development Agreement and are actively developing products in support of M/Chip 4 for 2004 availability. ActivCard, AOS-Hagenuk and Todos Data System have announced support of MasterCard's Chip Authentication Program (CAP) to offer customers chip-based cardholder authentication solutions for

non face-to-face transactions. MasterCard created the Chip Authentication Program (CAP), which is designed to build on the ease of use and security of an EMV-compliant Smart Card for authentication through a user's PC.

European Trial for Multi-Biometric Passports

Precise Biometrics has been awarded a contract for a trial for multi-biometric passports by a European authority. The order is for a number of multi-biometric verification stations, which will be developed by Precise Biometrics and Cognitec. Precise Biometrics is one of four main suppliers awarded a contract for the trial, which has the purpose of evaluating the impact of introducing multi-biometrics in passports.

The multi-biometric verification stations, which will include fingerprint recognition and face recognition, will be used for tests at sites where biometric passports will be issued. The trial, which will encompass 15,000 users in total, is estimated to start during the third quarter of 2004 and will last six months.

e-Passport for Nigeria

ID Solutions has received an order and full payment from IRIS Smart Technologies of Nigeria for a complete biometric solution for the issuance of passports. Nigeria has approximately 140 million citizens and is a major political leader for both the Western African region and the entire African continent.

The major features of this "e-Passport" solution are the utilisation of fingerprints, to ensure that the objective of "one citizen, one passport" is met

World News in Brief

4

Gemplus Reports First Quarter 2004 Results

Gemplus International reported that their first quarter ended March 31, 2004 results. The group revenue was reported to be up 27.9% year-on-year, that gained momentum in all business units. Net income for the first quarter increased by 28.1 million euros quarter-on-quarter, helped by the absence of non-recurring charges and operating profit before restructuring further improved to 4.8 million euros, despite unfavourable seasonality. In the banking & retail segment, revenue was driven by the migration from magnetic stripe to EMV cards. Payment microprocessor card shipments rose 125% year-on-year and 11% quarter-on-quarter. EMV sales continued to gather pace. Shipments increased 38% quarter-on-quarter.

Oberthur's Reports First Quarter 2004 Results

Oberthur Card Systems sales for the first quarter 2004 are showing a 3.8% growth at constant exchange rates. During the first three months of the year, the company has delivered 34.0 million microprocessor cards, showing an 18% increase on a year-on-year basis. With 19.5 million cards delivered (versus 11.2 million the previous year), payment cards sales - 31.6 million euros - increased by 63.5% versus the first quarter 2003. Oberthur Card Systems has recorded its best quarter for this segment with the EMV migration program in the UK and Belgium, significant deliveries in France and an exceptional renewal program of cards in Switzerland. As expected by the company, sales of mobile communications cards - 24.1 million euros - are down 21.8% on a year-on-year basis.

ActivCard Reports First Quarter 2004 Results

ActivCard Corporation reported their first quarter revenues for 2004 were $7.3 million, compared with $6.7 million in the fourth quarter of 2003 and $13.1 million in the first quarter of 2003. In the second quarter of 2004, the Company expects revenues to range between $7.0 million and $8.0 million. In addition, the Company expects to record additional restructuring charges during the remainder of the year as various elements of the restructuring plan are executed and completed by the fourth quarter of 2004.

Gemplus Delivers 64K Cards for U.S. Govt's Smart Card Program

Gemplus International have obtained FIPS 140-2 validation of its 64K Smart Card equipped with the applet required by the Defence Manpower Data Center (DMDC) for the next phase of the U.S. Department of Defence's (DoD) Common Access Card (CAC) program. Receiving the FIPS 140-2 validation on April 9, 2004, Gemplus becomes the first company validated to deliver Smart Cards that comply with the requirements for the next generation CAC.

G & D Jewel RFID Chip for Transit Fare Cards

Giesecke & Devrient (G&D has licensed the Jewel low-cost contactless Smart Card chip for mass transit ticketing from Innovision Research & Technology plc. Jewel is the smallest and lowest-cost chip ever produced for Smart Card applications, and is already attracting huge interest from the US mass transit sector.

New Patents Make Smart Cards Safer

Cryptography Research, Inc. has been granted several broad patents on technology that reduces fraud and piracy by protecting Smart Cards and other systems from Differential Power Analysis (DPA) attacks. The company developed the technology to help cryptographic device manufacturers, systems integrators, and Smart Card issuers develop secure, DPA-resistant implementations for use in financial, pay television, mass transit, secure identification and wireless industries.

On the Up, Down Under

Australia's first fully-integrated Smart Card system, which uses Wayfarer Transit Systems technology will be going on trial in Perth. The SmartRider system trial involving 225 peak time standard fare commuters and 225 concession users. Passengers will be asked to record their experiences in a diary, while bus drivers involved in the trial will be asked for feedback via regular issue sheets and will be surveyed at the end of the trial. Wayfarer is working with Delairco Bartol to supply the Smart Card system for Transperth's bus, train, and ferry services.

Wal-Mart Begins Rollout of RFID

A new era in supply- chain management begins as Wal-Mart and eight product manufacturers begin testing electronic product codes, or EPCs, at select Super-centers and one regional distribution center in the Dallas/Fort Worth metroplex. This pilot is the next step in Wal-Mart's addition of radio frequency identification (RFID), to improve product availability for Wal- Mart customers. The real-world trial follows extensive testing at the company's RFID lab and months of collaborative preparation by Wal-Mart and its suppliers.

New RFID Learning Lab Opens

ACNielsen U.S. has opened a Radio Frequency Identification (RFID) technology learning lab at its Schaumburg, Ill., office. RFID technology is being tested by numerous industries to help track everything from airline baggage to cattle. Several major consumer packaged goods retailers and the U.S. Department of Defence have issued mandates to their vendors, requiring that all product pallets and cases bound for their distribution centers be RFID tagged within the next one to three years.

The Massachusetts Institute of Technology's Auto-ID Center has been the driver of this technology over the past three years and will continue to enhance RFID with Auto-ID centers in six different regions around the world.

GE Security and XceedID Offer Contactless Security Products

XceedID Corporation has announced that it will work with GE Security, to offer next-generation contactless Smart Card and reader products to the security industry. XceedID and GE Security, along with other industry leading security companies, will offer a range of contactless products and work together toward establishing an open protocol standard for contactless Smart Cards.

Sun and Capgemini Launch RFID Solution

Sun Microsystems, Inc., and Capgemini, have announced the launch of a jointly developed Radio Frequency Identification (RFID) solution.

The solution will help enable retail and consumer packaged goods (CPG) companies to comply with RFID mandates issued by a growing number of leading retailers such as Wal-Mart, Target, and Albertsons.

Italian Ministry of Health Approves VeriChip Healthcare Application

The Italian Ministry of Health has approved a clinical study utilising the VeriChip healthcare application, VeriMed. The study will be carried out at the Instituto Nazionale Lazzaro Spallanzani Hospital in Rome, Italy. VeriChip is a miniaturised, radio frequency identification (RFID) device that can be used in a variety of security, financial, emergency identification and other applications.

Datastrip Introduces New Smart Card Readers with Biometric Sensor

Datastrip, has launched a new generation of handheld Smart Card readers with instant verification of biometric contact and contactless chip cards, called DSVII-SC. This new product was voted the best new biometric product of the year by the Security Industry Association at the ISC West Conference in the US in April.

Keycorp $4m in New Orders

Keycorp Limited has announced that two banking industry leaders in Australia and New Zealand had placed orders worth more than $4 million for its K23 payment terminals.

World News in Brief

CardTech / SecurTech 2004

By Peter Tomlinson Independent Consultant, Iosis Associates

Peter Thomlinson

This April Convention used to be the place to go in the smart card business, but of late its star has waned as Carte's Paris star has waxed. Nevertheless, Washington is closer than other venues such as Las Vegas used by CTST, although to some there may not be the same glamour. Off I went, on a quest to find out what is coming up in the western world's (and Japan's) development of smart card technology. With me was Gore Vidal's Lincoln, bought for a pound in the Amnesty shop, and so I was to read the book and see the places where it happened.

Washington is much improved from the last time that CTST was there. One surprise was that CTST has moved across the square to vast caverns in a new building, but the Convention Centre's prominent triangular mushroom sign didn't go with it - a source of much confusion to delegates. Another surprise was the rain on the Monday, so time for a trolley ride with Lincoln.

On registering, we were given a card, partly transparent. It had in it two aerial coils: one clearly for the Proximity contactless technology (as used for transport tickets, for example). The other had many more turns: the old 125 KHz method, perhaps? There was also a contact chip. Only one Exhibition booth read it for me, but Conference delegates told me that it was used in contactless mode to record your attendance at each session. In the Exhibition, business cards still rule. Several people told me that CTST last year was a waste of time. Certainly the show this year was small, with several exhibitors telling me that a payment systems convention the previous week in Las Vegas had been much better attended. But selling terminals and cards wasn't the driver this year. Where, then, was the action? It's in the public sector, silly. Luckily, I was in contact with another UK attendee - he had a Conference pass.

After a year of watching public sector stumbles over technology Smart Cards, and out and out gaffs by ICAO, reality has set in. The US State Department announced that they had been approached by Master Card with a view to collaboration on tidying up Proximity card (ISO/IEC 14443) technology - Master Card later confirmed this - but that is just a tiny fragment of the wealth of public sector information disclosed. The Japanese New Media Development Association members were clustered around the Sharp stand, and let it be known that they have now documented in English their ideas for Proximity technology. ACG told us that they have made great strides with contactless reader module development, and Japan has some dinky little contactless readers and an internal type approval method for components used in their citizen service card (and now national ID card) rollout.

Sharp and Omni Perception (a company associated with the University of Surrey) both demonstrated very slick facial recognition equipment, in Sharp's case configured as a pass-through gate and using a production ready e-passport. It was soon learned that ICAO is close to releasing a complete e-passport spec, that Master Card has its PayPass (contactless payment) ready to go, and that PC/SC V2.0 is out for review by its members. Delving a little deeper, the US has just been appointed to chair ISO/IEC SC17 Task Force 9 to prepare for bringing together the NIST GSC-IS ID card spec, European ID card work, and the Japanese post-issuance applet download method. They have a year to prepare the material for a formal Working Group. UK input is requested - contact David Everett at Microexpert or Alan Borrett at CESG for more information.

Despite the ups and downs of the Smart Card and related systems market, it was pleasing to see how many people have been hanging in there and are now pushing quality developments forward. But it was also noticeable that big companies such as Infineon and Gemplus had given this one a miss - big order books meaning no need to fly the flag, perhaps? All in all, a very productive week, and the best food experience was that Bison steak in the amazing Union Station.
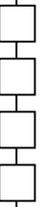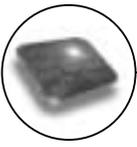
Turn On SIM Browser

By Pauline Jacqueline Aloysius, Gemplus

Nowadays the built-in infrastructure demands a Smart Card in everyone's hands to use everywhere for everything. The SIM (Subscriber Identity Module), which was once only the security module fitted in a GSM mobile phone, now acts as the phone's brain as well as the interface to Internet connectivity. This operation of the SIM is achieved by the SIM Application Toolkit (STK), which provides mechanisms for mobile electronic commerce applications and value added services on the SIM to interact with the external world.

Pauline Jacqueline Aloysius

Usually the terminal handsets are master, while the SIM is the slave, but with STK design specification the ME & SIM works in client-server mode, where the STK drives the mobile phone by issuing commands ranging from setting up & displaying menus to getting user inputs for sending and receiving SMS messages. This SIM Application Toolkit has been agreed and incorporated in the GSM standard as GSM 11.14, titled as <Specification of the SIM Application Toolkit for the Subscriber Identity Module - Mobile Equipment (SIM - ME) Interface>. A few years ago, the memory capacity of Smart Cards was enough to hold basic STK applications but now due to the demand for high capacity applications, the Smart Card manufacturers move towards mass production of 32K cards and high expensive 64K and 128K cards have also come into the market.

Why this move? Is it just to display menu and send SMS? Or is it the SIM card wants to offer a multi-application framework to the end-users. Yes, the smart move is to provide a multifunction capability platform for hosting fully fledged, wide range of applications on the Smart Card. One such application is to browse the Internet with the use of Wireless Internet Browser (WIB) through STK mechanisms from even "non-smart" mobile phones. The installation of this micro-browser WIB on the SIM card needs a 32K memory capacity card to store it in the form of an executable application.

According to SmartTrust, the WIB Applications appear as STK menu items on the mobile terminal, and typically points to locally stored WML applications or a URL address on the Internet. The Wireless Internet Browser (WIB) access the URL on the server to retrieve information and receives compressed web pages from the server and converts the byte coded WML decks to SIM Toolkit commands as per the standard defined for client/server communication protocols. Moreover the WML decks which are stored locally on the SIM can be updated Over-The-Air, which makes it possible for the operators to add new services as and when there is a demand from the market thus enabling the mobile operator to have control of the value added services.

The STK supported SIM browser utilizes the existing technology and infrastructure enabling the application developers to develop and extend WIB functionality for new applications on the SIM card. This combination of WIB with STK mechanisms gives the flexibility of updating & altering the SIM with new services, which can be downloaded over the air. Though the implementation of WIB requires the Smart Card manufacturers and operators to migrate to high memory capacity cards, it turns out to be an advantage for a subscriber who enjoys the benefits from WIB, by merely purchasing a new SIM card, for a fraction of the cost of new mobile equipment. Further to note is that, the SIM Browser implementation based on SmartTrust WIB technology shows 300% growth in the mobile industry, which clearly justifies not to wait but to go for it. Thus the future of WIB with STK is well entrenched & it is forecaste to retain its market as a value added service, facilitating the service providers to deliver customised content to their subscribers.

www.gemplus.com

Greater Public-Private Sector Co-Operation May Boost Functionality and Uptake of Smart ID Cards

By Caroline Walpole and Pieter Hoogendoorn, ACI Worldwide

ID cards to benefit governments or consumers? In late April, David Blunkett published his draft ID Cards Bill, which sets out the legislative framework for introducing biometric ID cards in the UK. A key point in the bill is that by 2013 Blunkett expects 80% of the population will have one of these smart ID cards, at which point ministers will make a decision on whether to make the card compulsory.

Caroline Walpole

Many UK citizens are sceptical about the introduction of ID cards given they will largely hold government applications for government purposes. But there is a real possibility for these cards to provide practical applications for the everyday citizen beyond public sector access, in areas such as payment or loyalty schemes. And the technology already exists to manage the multiple applications from different issuers that could reside on these Smart Cards. Several countries around the world are already running national ID card schemes with relative success. Hong Kong is home to the most innovative ID and Smart Card projects to date. The initial launch of its smart ID card in June 2003 was primarily to replace the laminated paper ID card required by all residents in the special administrative region (SAR), but the scheme has progressed well beyond this point.

Library access and digital certificates for identification in e-commerce are already enabled by the cards and the next likely application to be introduced to ID cards in Hong Kong is the driver's licence. Other possibilities include global PIN management. Further down the track, for Hong Kong and other countries issuing smart ID cards, is the inclusion of financial applications on the cards. Providing such functionality on a universal card could potentially bring the most benefit in terms of payment convenience and overall fraud reduction to citizens and the community. But one reason that financial applications will not be appearing on the cards in the short term is the requirement for collaboration between government departments and commercial entities.

Hong Kong citizens may wonder why the driving licence will be installed sooner than e-payment. The answer may be as simple as both the Immigration Department and the Ministry of Transport are government departments hence the card issuer is the same organisation. It is therefore easier for the driver's licence to 'piggy back' onto the smart ID card than e-payment. An open platform for commercial applications is a harder challenge because of the business arrangements -- a bank is a different card issuer to the government and has different reasons for becoming involved with universal smart ID cards.

Moving towards e-payment capability on cards. But e-purse functionality in a card need not involve bank partners directly. Besides the smart ID card in Hong Kong, many citizens there also carry an Octopus card issued by the local public transport body. It is a contactless, stored-value Smart Card that speeds up entry to the public transport network, and is the model for London's similar Oyster travel card. Besides public transport, the money stored on the card can also be used to purchase low-value items at stores such as 7-11 or Starbucks. Even parking stations now accept payment in this form. Interestingly, the Octopus is not limited to the card format, and can also be purchased as a ring, worn on the finger. The Octopus card proves that the technology exists to get multiple businesses accepting a common Smart Card format. '

Combi cards' - where government and commercial applications reside side by side on Smart Cards - are technologically viable, but are dependent on agreements being put in place between the public and private sector organisations involved. Imagine you are a lorry driver travelling regularly between international borders. On your smart ID card could reside your passport, your petrol loyalty card, and even a means for paying your road tolls. With one card, you can securely make all your contact and contactless payments, as well as the interactions with government infrastructure required for your journey.

Secure ID to support payments and fraud reduction. Security is a must for smart ID cards, even more so if financial applications reside on the card. Smart card technology already enables secure payment and authentication. With EMV, the financial industry has added security through enhanced authentication (cryptography) and verification (PIN). PIN is a quantum leap forward from signature, but it is still vulnerable, notably with 'shoulder surfers'. A secure ID beside the PIN, be it a photo or biometric, will prove that the cardholder is conducting the transaction. Secure verification is ensured because the cardholder has unique physical characteristics that are very difficult to replicate. Today, counterfeiters can fake the card but not the cardholder. With smart ID cards, it will be a harder challenge to fake either the card or the cardholder.

A photo or biometric on a smart ID card could also benefit citizens unable to tap in a PIN due to disability, for instance. People who have difficulty entering or remembering their PIN creates a challenge for banks/card issuers to deliver a service that caters for the whole community. The verification and security that resides on a smart ID card could potentially make it a viable real estate for financial applications.

The main benefit of smart ID cards for financial institutions is that they will have a positive impact on fraud such as identity theft, which costs the UK more than £1bn a year. The extra security layer makes it harder for the criminal to procure information. This refutes the claim by sceptics that the security on smart ID cards is compromised because it is a single point of entry for the criminal. The technology is in place to prevent this. Announcing the draft legislation, Blunkett said: "Multiple or false identities are used in more than a third of terrorist related activity and in organised crime and money laundering. It is crucial that we are able to robustly ascertain and verify our own and others' identities."

Learning from banks and other governments. In the UK, banks could use the smart ID card alongside payments to assist in a referral situation. A merchant could relay details from the ID card to the referral agent to verify the cardholder. Moreover, as pre-authorised debit and e-purses become more prevalent, the ID can be used in situations such as checking on under-aged children purchasing alcohol from off licences. These situations could potentially work more smoothly if the government's ID and bank's financial applications resided on the same card. But whether or not financial and government applications end up sharing physical card real estate, there is one immediate area of co-operation that would be beneficial to all concerned. Unlike banks, the UK government does not have experience of mass issuance of cards. The estimated £3.1bn cost of the UK smart ID card scheme could be lessened if the government could collaborate with the financial community and use infrastructure that is already in place.

The potential benefits of greater government co-operation with banks and other commercial partners are illustrated in a round about way by the example of Scandinavia, where the smart ID is purely for government purposes. The Scandinavian government has now recognised that this approach is too stand-alone and admits it should have worked with other commercial partners. In Hong Kong, this is precisely the approach that is being taken. If the UK learns from the Hong Kong experience, UK citizens will not only benefit from government applications on smart ID cards, but also from further commercial and financial applications that can improve security and convenience in their daily activities.

www.aciworldwide.com

Smart Cards Draw Influential Adopters for Access Control and IT Security

By Randy Vanderhoof, Executive Director, Smart Card Alliance

Randy Vanderhoof

Smart Cards continue to draw influential adopters in the U.S. for IT security, access control and identity credentials, as CardTech/SecurTech, the industry's largest conference and exhibition, kicks off in April in Washington,D.C. One notable example is Microsoft, who has standardised on Smart Cards for network logon security for its own systems and is using the same card for physical access control

Another example is the U.S. federal government, which is making excellent progress implementing its vision of a single access control and identity credential for all its employees. The fact that organisations of this stature and technical sophistication are standardising on Smart Card technology for security is a good indicator of where the market is headed.

For its part, Microsoft selected smart card technology for securing access to its intranets and delivering digital certificates to its 55,000 employees used for remote authentication, digital signatures and encrypting emails. "The use of Smart Cards has significantly increased the security of our corporate network by improving our ability to authenticate each employee and business partner as they remotely connect to Microsoft," said Greg Wood, general manager of Microsoft Corporate Security. "IT chose to deploy Smart Cards over other technologies because of the reliability, cost, features and mobility. The Smart Card platform is also extensible as a platform to other applications, whereas the other technologies are typically singular in their application."

Microsoft joins a growing roster of blue-chip technology companies that are using Smart Cards internally for logical and physical access control. When organisations get serious about eliminating passwords for IT security, increasingly they are turning to Smart Cards because of their security, multi- application capability, standardisation and portability. Industry watchers are now predicting that the rapid growth in the use of smart cards for strong authentication in the public sector will ultimately lead to widespread adoption in the enterprise market. With millions of cards already issued, the U.S. federal government is sold on Smart Cards for strong authentication and as highly secure identity credentials, and is marching toward the goal of a common identity credential that is used for both physical and logical access control across all of its branches. Programs are already planned or underway to issue new smart ID cards in numerous federal agencies, including: GSA, Defense, State, Treasury, Homeland Security, Veterans Affairs and NASA. In a newly released draft document, the Federal Identity Credentialing Committee is strongly recommending that federal agencies follow a framework, or roadmap, that it defines for strong authentication for physical and logical access, moving toward governmentwide standardisation of credentialing.

Another important milestone in the government's use of Smart Cards is the recently published Government Smart Card Handbook developed under the joint sponsorship of the General Services Administration Office of Governmentwide Policy and the Smart Card Interagency Advisory Board (IAB). The purpose of the handbook is to share lessons learned and to provide guidance to federal agencies contemplating the development and deployment of smart card-based identity and credentialing systems. The handbook is based on contributions from experts in government, industry and academia, and includes input and review by members of the Smart Card Alliance Leadership Council. The handbook is available on the Alliance's web site and at GSA's public web site. The Transportation Security Administration Transportation Worker Identification Credential (TWIC) passed a significant milestone earlier this year by completing the technology evaluation phase of the pilot. Chip technology was selected over all other technologies tested, including optical stripe, 2D barcode and magnetic stripe.

The prototype phase for this program is imminent in this extensive identity credential program that will eventually lead to a smart ID in the hands of more than 12 million transportation workers in the United States.

Another very high-profile government project involves contactless smart chips and U.S. passports. This project, recently delayed due to bidding issues, is expected to resume shortly with its plan to incorporate contactless chips into the more than 7 million passports issued each year in the United States. Currently under U.S. law countries participating in the Visa Waiver Program must put a program in place to issue tamper-resistant, biometrically- enabled passports by October 2004; however, it is widely expected that this date will be extended in order to give countries more time to comply. The U.S. Passport office is aggressively working to meet deadlines for U.S.-issued passports.

There are several factors common to both U.S. enterprises and the federal government causing this convergence on Smart Cards. Both want more security at physical access points and for computer networks. Both want ID credentials with greater security against counterfeiting or use by someone other than the person to whom the credential was issued. Finally, both sectors increasingly see the risks associated with relying on password protection for securing information systems and databases.

The ease with which passwords can be stolen and distributed puts the integrity of virtually all of our nation's information systems at risk. Any system where access is protected only by passwords is rich with fraud possibilities. Including a Smart Card in a properly designed security system is the best solution to that problem, because it adds something you must have, the Smart Card, to something you know, your password. Then even if some trusted but disgruntled employee decides to steal or distribute a file of passwords, no one can use them without also having the Smart Card.

www.smartcardalliance.org

Events Diary 2004

June

1 - 3	Smart Card China 2004 - *Bejing, China*
9 - 10	Contactless Cards - London - *www.smi-online.co.uk*
10 - 11	Smart Healthcare 2004 - *California- www.idtechex.com/smarthealthcareusa/index.asp*
22 - 24	Credit Card World - *London- www.worldofcards.biz/2004/ccw_uk*
28 - 29	The ASROC Alternative Payment Processing Conference- *London- www.asroc.com*

July

7 - 9	CardTech Korea - *Korea*
8 - 9	CardEx Asia 2004 - *Kuala Lumpur - www.egytec.com*

August

5 - 6	Cards Australia - *Australia - www.worldofcards.biz/2004/cards_au*
4 - 6	Prepaid Markets Expo 2004 - *New York City, USA - www.prepaidmarketsexpo.com*

Industry Insight ○ Events Diary

12

Biometrics: Ready for Prime Time?

By Mary Kirwan, Lawyer and IT Security Expert

Biometric technologies have a certain cachet - a distinct allure. Hardly a movie comes out of Hollywood these days, but the protagonists are enveloped in a maze of biometric gizmos, from iris and retinal scanners to face and hand print readers. Tom Cruise in the futuristic movie Minority Report has his eyes surgically removed to evade iris scans and detection, but nonetheless is able to re-enter his previous place of employment, as a wanted felon, by using his own bloodied, extracted eyeballs. His access privileges had not been cancelled. This is the reality even Hollywood can't expunge, and almost certain to ruin a good flick for all security- conscious moviegoers.

Have biometric technologies finally taken off? Despite all the hype, biometric technologies have been slow to take off. Cost issues, instability, lack of portability, interoperability problems and multiple standards have made them a hard sell. However, since Sept. 11, 2001, as a result of massive lobbying efforts by biometrics companies offering the holy grail of security in the fight against terrorism, they seem to be finally coming into their own. Numerous government initiatives around the world are in place to augment identity and travel documents, such as passports, with biometric identifiers. There are even calls for national ID cards in Canada, as well as in the U.S. and U.K. As of Sept. 30, 2004, citizens of all 27 countries (including Ireland, the UK, Australia, Japan, Italy, France and Germany) considered visa-waiver countries by the U.S., must be fingerprinted and digitally photographed before they can gain entry to the U.S. This is a stop- gap measure until these countries can issue biometric enabled passports to their citizens. It is expected that the US Congress will roll back the original date for implementation of these measures (October 26, 2004) to December 2006, as many countries expressed an inability to comply within that time frame.

According to the U.S. Department of Homeland Security, the biometric data obtained will be compared against 'watch lists' to decide admissibility for entry. One can only hope that U.S. 'watch lists' are in better shape than those in Canada, as highlighted in a recent Report by the Auditor General of Canada on National Security, where they are described as "in disarray" and rife with errors and missing crucial data. It is also by no means clear that any fingerprint matching system can scale up to deal with such a volume of prints, without a significant increase in 'false reject' error rates (where legitimate persons are rejected by the system), or 'false acceptance' rates (where rogues are authenticated and accepted by the system). In addition, a recent article in the New Scientist magazine reveals that many scientists and legal experts are concerned that fingerprint technology, long considered infallible, is based on flawed scientific and statistical assumptions, and that it needs to be subjected to independent scientific scrutiny, a move strenuously resisted by the law enforcement community.

Biometrics in Canada: In Canada, the Canadian Air Transport Security Authority is piloting the use of biometric Smart Cards by airport workers to improve airport security. The CANPASS Air program implemented at the Vancouver International Airport in July 2003, and at the Halifax International Airport in November 2003, is to be expanded across the country. CANPASS Air will use iris scanners to allow pre-approved travellers speedy clearance through customs. They must complete an application form, provide photocopies of certain 'proof of identity' documents, such as a passport, or birth certificate, and attend an in person interview.

How secure are biometric devices? Vendors have made extravagant claims that biometrics "virtually guarantee network and facility security." Such statements tend to incur scepticism from seasoned security commentators, and often do more harm than good. Most commentators have focused on the privacy issues, concerns about 'function creep', and the advent of a global 'Big Brother' surveillance society. However, far less attention is paid to security issues. It is often tacitly assumed that the various biometric technologies are stable and security threats minimal. This is not universally the case, and successful attacks on biometrics by researchers and academics, and less frequently by hackers, have made that abundantly clear. In addition, international standards are fractured, and interoperability issues far from resolved.

Environmental factors can also impact the reliability of these technologies. Vested interests often lead standardisation efforts, and independent evaluations of products is not yet widespread. Biometric companies have been loath to expose proprietary technology to outside expert review, which in turn leads to concerns in the security community about 'security through obscurity'.

Who will guard the chicken coop? Lack of security at the back end has been a concern often written about in this column. This concern is heightened with extensive use of biometrics. To create a biometric matching system, a template is created from raw data, such as a fingerprint, and stored for use in either a 'one to one' verification system, or a 'one to many' identification system (where a user's identity is checked against a large database of stored templates). Templates must be encrypted and stored, either in a database, or on a magnetic chip card, Smart Card or token. It is highly preferable that the template be stored on a Smart Card, and not transmitted for verification or identification purposes. If the template is stored on a smart card, for instance, the attacker must hack the card as well. Not impossible by any means, but another hurdle to overcome. However, where there are many users, and remote verification is needed, central database storage is often used. Such databases are, of course, susceptible to insider attacks, and weak cryptography to various brute force attacks.

Who can we trust to secure biometric data? If large banks of biometric data are left to government to secure, what a glorious target for hackers and organized crime that will be? The private sector has shown itself to be frequently unable to protect personal data. Government has repeatedly exposed SIN numbers in Canada, and SSN numbers in the U.S., and scored poorly on internal security audits of their own practices and procedures. Are they really up to the task of protecting the master key to our identity? It remains to be seen. The reality is that there is no such thing as 100-per-cent security, and human ingenuity dictates that as soon as we build it, someone will break it down. Claims to the contrary breed complacency and are anathema to progress in the security field. Claims of infallibility for any technology can also lead to false convictions, and serious miscarriages of justice.

Will biometrics obliterate identity theft? It has also been widely claimed that biometric technology is essential to stem the tide of identity theft. Several of the 911 terrorists had legitimate drivers licences, and as they were largely unknown to law enforcement, all the biometric scanners in the world would not have made any difference. According to Privacy International, an international privacy watchdog organisation, a lesson learnt from countries with national identity cards is that the technology gap between governments and organised crime is so great that even the most secure cards "are available as blanks weeks after their official introduction". The problem of identity theft will not be solved with a smarter ID card and more stringent registration procedures to get such a card. Insiders, private outsourcing companies, organised crime and hackers will be highly motivated to expose biometric identifiers, and sell them, as they do all other valuable commodities. And the result may be criminals with stronger identification, unlikely to be challenged. Biometric technologies have, indeed, been shown to be useful to deter welfare fraud and opportunistic crimes, but are unlikely to perturb determined adversaries.

What does the future hold for biometrics? Biometric technologies have great potential, especially in attended operations (where a physical security guard is also present), or in conjunction with existing technologies to create a multi- layered approach to security management. Multi -modal biometrics also show promise (where different types of biometric technologies are layered and used together). They are also useful to protect encryption keys in a Public Key Infrastructure (PKI), and, of course, can remove the need for users to remember a multitude of PINs and passwords, an enticing prospect in itself. But any suggestion that biometrics alone will stop terrorism, obliterate identity theft, and convert hardened criminals to Buddhism is likely to be an expensive and vain exercise. Giving law enforcement and the intelligence community the funds they need to fight crime and engage undercover operatives to garner real intelligence is currently likely to be a better use of always scarce resources. The same applies in the corporate environment. If you have no security policy, a discontented and poorly motivated workforce, no amount of biometrics will plug the hole in that particular dam.

opinion

14

Finger on the Pulse of Identity

By Carl Norell, Gemplus

The contours of the finger, the patterns of the iris and the shape of the hand can all be used to provide strong authentication, but are these - and other - biometric technologies sufficient to provide good security while also ensuring the privacy and trust of end users? Biometric technology, which is now being deployed in a number of application areas including immigration and national identification, has the security advantage of not being able to be borrowed, lost or stolen. It is also reaching a state of maturity, with accuracy levels improving, costs falling and template sizes shrinking. To the average media pundit in the immediate aftermath of September 11 2001, biometrics became the panacea for a host of security problems. Today, much of the hype has gone, and people are more realistic about the strengths and weaknesses of the technology.

The choice: Numerous decisions need to be made when considering the deployment of biometrics. First, which type of biometric should you adopt? Do you opt for a biometric that examines your target's physical characteristics, such as face, fingerprint, iris, hand or retina? Or do you adopt a behavioural biometric such as dynamic signature, keystroke or voice? Your decision will be determined by a number of factors, including how important accuracy is to you. Some situations - such as access to highly secure government areas - may require the highest levels of security regardless of cost. In other situations, a few individuals being falsely rejected from, or falsely accepted to, a system may be acceptable. If accuracy is a key priority, iris technology may be the most suitable.

Second, what's your budget? Typically, fingerprint technology is cheaper than iris or face biometrics in a small-scale rollout. However, it's worth bearing in mind that cost differences between biometrics depend largely on where they are deployed. In a border control setting, cost differences are not always significant because other infrastructure costs will be larger than that of the biometric technology. Third, who will be using your system? Ease of use is particularly important, especially if a large percentage of users aren't technically savvy. Added to this, how does your target audience perceive the technology? Do they see some biometrics as more dangerous or invasive than others? Fourth, what are your throughput demands? If the biometric system is being deployed in an airport environment, it should be robust, quick and easy to use.

Finally, what are your data storage requirements? Does the owner of the biometric maintain ownership of his or her template? Or is it held in a central database elsewhere? For some systems, a central database may be considered sufficient. However, this raises questions about privacy - who has access to the database? - as well as security - how do they gain access to the database? In addition, is it sufficient for a person to present him/herself to a system to be authenticated purely by their biometric? Here, smart card technology really comes into play. With falling costs and increasing memory sizes, Smart Cards have a lot to offer the biometrics industry. They can be used in conjunction with the biometric and a PIN to provide three-factor authentication: something you have - the card; something you know - the PIN and something you are - the biometric.

Storage requirements. By storing a template directly on a smart card, organisations can also overcome the potential privacy and portability problems of a centrally stored database of templates. Although memory requirements vary between biometric technology vendors, typical template rates are currently 4-20Kb for face recognition, 2-4 Kb for fingerprint, 9 bytes for hand and 512 bytes for iris; all sizes that are easily managed on a Smart Card. Taking the privacy discussion a step further, matching algorithms can be implemented on the smart card. This means that instead of reading the template off the card, the biometric is read and given to the card to do the matching in a process known as on-card matching. This technique ensures there has been no tampering with the matching process and also means that the enrolled biometric data never leaves the card. The portability of the biometric enables the card owner to have control of his or her template, while also supporting offline processing.

15

National ID - a big market: With many governments now considering - or upgrading - their identity cards, biometrics and smart cards are coming of age in a variety of countries. Malaysia, Brunei, Oman and the United Arab Emirates are just a selection of countries that have recently adopted national ID smart cards using fingerprint technology. In the Sultanate of Oman, a smart card-based citizen ID programme has been deployed using the "ResIDent" smart ID card system from Gemplus, and fingerprint technology by biometrics vendor Sagem. The new system provides advantages to government and citizens alike. The government is able to enhance its identification processes, improve its infrastructure, modernise its national registry system, increase homeland security and provide better quality services to citizens. Cardholders, meanwhile, can identify themselves electronically.

And, as time progresses, these cards will be used for a host of government applications, including driving licences, passports, work permits, PKI authentication and digital signatures, domestic e-purse, healthcare cards and electronic voting. Approximately 1.5 million smart cards will be issued to Oman's citizens and expatriates above the age of 15 between 2004 and 2007. In neighbouring United Arab Emirates, a nationwide ID programme using Java Card-based technology from Gemplus and Sagem's AFIS technology has been launched. The scheme, which goes live this year, will see more than 2 million cards rolled out for personal identification purposes. Using the power of multi-application Smart Cards backed up by biometrics, this card will also eventually combine identification with driving licence, border control and emergency medical data.

Public opinion shift: Even in the UK, where public opinion has typically seen identity cards as an infringement of civil liberties, there now seems to be something of a sea change. In April 2004, a Mori poll of 1,000 people indicated that 80% backed a national ID card scheme. With public opinion growing, the UK government is now drawing up plans for a compulsory ID card combining biometrics with a smart card in an effort to tackle the identity fraud which costs the country UK£1.3bn each year. Trials involving 10,000 volunteers have been launched from the passport office in London and three other centres around Britain. The government is expected to publish draft legislation and a bill paving the way for the scheme before the next general election. With the number of biometric and smart card schemes for national ID increasing, media and analysts are beginning to realise that biometric technology is a good tool in the fight for security and authentication. However, with the combination of biometrics and Smart Cards, organisations have access to a great tool that enables even higher levels of security while promoting privacy and portability.

A World of 'Open' Opportunity

By Richard Crookston, Head of Marketing, VeriFone EMEA

Richard Crookston

The payments industry has been searching for the crucial revenue generating application that resolves the 'open purse' conundrum; one that enables innovative payment methods to be established, new cardholders to be embraced, and that takes advantage of the industry's extensive investments in EMV. To date, the banks have explored a variety of applications, but each of these uses just one of a number of competing technologies, making universal introduction expensive and almost impossible to achieve. However, there could be a resolution that overcomes these challenges, opening the way to a wealth of new opportunities - Pre-Authorised Debit (PAD).

The PAD payment system has the capability to address a number of key requirements. Card scheme members can offer their customers national currency, e-purse-like products that can be associated with debit and credit products. In addition, they will be able to build on the rollout of EMV chip-enabled cards, to provide a single currency payment system that can be targeted at both the banked and unbanked population. In addition to being able to support both the on-line and predominantly off-line payment environments, the PAD payment system offers true system integrity and acceptable risk management thresholds. Finally, settlement and clearing between participating banks is undertaken using existing procedures that have long been established by the international card schemes.

The PAD payment method provides electronic purse-like features based on the EMV debit and credit specification. Unlike the competing electronic purse schemes tried by a number of banks, EMV has the inherent advantage of being designed to be interoperable and internationally accepted, which means PAD will work within other EMV-based national card systems. It also enables banks to take advantage of the banks and retailers' infrastructure investments and, because it utilises the EMV technology as a platform, it is secure for cardholders, acquirers and issuers, making it ideal for other payment environments such as the Internet, e-commerce and m-commerce.With PAD, the achievement of a cost-effective single currency payment system that is smart card-based and viable for both banked and unbanked users becomes a reality. Named customers - those linked to bank accounts - can take advantage of a secure, personalised low-value debit payment method, optionally secured by a PIN that is capable of enabling off-line cash transactions as well as direct fund transfers from the user's account to the card. The PAD payment system can also be accessible to those in the population that do not have a normal bank account through the provision of an "anonymous" payment card. By simply associating the card with a unique numbered holding account, banks can securely load values onto cards using on-line terminals in exchange for a cash payment (effectively putting a deposit on the card).

Bank branches and other authorised locations will be able to operate on-line value-load devices. Once loaded, cardholders can undertake purchases and merchants simply deduct payments from the balance held on the card itself. Once the balance is exhausted, a cardholder will once again need to 'recharge' its value at an on-line terminal.So how will this operate for retailers? Point of sale (PoS) devices can use the standard EMV kernel application. The merchant terminals will be able to approve transactions based on the available card value; updating balances automatically and providing off-line balance enquiries. Clearing and settlement procedures will utilise defined processes already in place for standard credit or debit transactions. Therefore the merchant end-of-day process automatically initiates PAD settlement between the retailer and the acquiring bank.The PAD application does not require any online authorisation for a purchase, making it ideal for environments where telecommunications are difficult or expensive to implement.

All transactions are 'authorised offline', generating an EMV transaction certificate, which also provides the audit trail. This gives us an interesting option for some totally offline merchant sites to transfer transactions to a memory card for presentation at their acquiring online bank; each memory card becomes a virtual terminal with a unique ID to support central verification and value assignment. For totally offline merchants, the bank uses its branch terminal to read transaction records from the merchant card, using normal EFTPoS submission processes to transmit transactions to the clearing centre for posting against individual retailer accounts. This offline technique brings other potentially interesting applications for PAD.

In the vending arena, it could eradicate the risk of cash theft from machines storing cash and, with the growing interest in Internet, e-commerce and m-commerce, PAD will also be able to provide secure, authorised, low-value transactions within these payment environments. The PAD system opens the way forward to a new world of payment opportunities and overcomes the issues of implementation and solution-proofing by adopting EMV-based technology that ensures banks are not tied to a single card type or platform. And because PAD complies with EMV, it can operate with other EMV-based national debit card systems.

Transactions are easily switched between participants, with full reporting on all transactions that are processed through the switching process.For banks, PAD offers a payment scheme capable of supporting low-risk products for a new customer base not familiar with, or trusting of, banks. For retailers, the system uses an EMV-enabled PoS device and removes the risk from transactions by guaranteeing that funds are available, providing PIN-based identification at the PoS to verify cardholder authenticity. The PAD system could overcome all the business issues associated with providing cash-less transactions by providing banks and retailers with a cost-effective route that takes advantage of existing infrastructures to undertake transaction reconciliation and distribution in a secure fashion. This is no 'pipedream'. MasterCard and Visa are already in the process of implementing plans to support PAD as an extension to the credit and debit services supported by EMV. The payments industry has long sought a crucial revenue-generating application that could create a rapid return on investment in EMV. With PAD, the search may well be over.

EV Event Special

17

Healthy Eating on the Cards
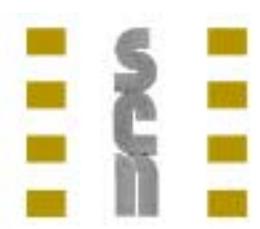
By Patsy Everett, Managing Director, Smart Card News

Last month there was a lot of publicity from the UK government about obesity and the cost of treating diseases related to over-eating and lack of exercise, to the National Health Service, so the launch of the Torfaen "Total Access Card", which encourages healthy eating by students was most opportune. The TAC - Total Access Card scheme was funded with UK lottery money and is run by the Torfaen County Borough Council. Year 8 and 9 pupils from the Fairwater High School, Torfaen, Cwmbran in the UK took part in the scheme, which should be rolled out to the whole school later this spring.

Pasty Everett

The idea behind the scheme is to promote healthy eating by rewarding students with points if they choose a healthy option diet from the cafeteria or vending machines. The card can be loaded with funds electronically which means student's do not have to carry cash to school, readers strategically placed around the school enable students to verify the amount of money and points they have on the card. Students are also able to print off a voucher which can be exchanged for a raffle ticket for the end of year prize draw for things such as bikes and skiing lessons supplied by local companies.

The use of the TAC card means that students who are normally entitled to free meals can purchase food in the same way as other students without identifying their free meal status. The card is also a library lending card and allocates rewards points for all book returns. According to the cafeteria staff the main advantage of the card, as far as they were concerned, is not having to handle money which make the transaction faster and more hygienic. Students had a different view, they felt transactions took longer and subsequently felt they should have a longer lunch break.

Although any scheme that encourages healthy eating and promotes exercise is to be encouraged there are issues around encouraging the idea of gambling and of course if a student normally eats healthily or has a medical condition that forbids high fat or salt, they would accrue more points without trying. There is also the goody, goody element that might not be seen as cool. by the other children.

The project was managed by Smartex Limited, a CCA partner company, with software for the schools system from MH Systems Limited, terminals from General Information Systems Limited, library terminals and software from Electronic Reading Systems Limited, and the security and card internal structure designed by Microexpert Limited. ACG (UK) Limited provided the cards, of single-chip, dual-interface microprocessor architecture, with 16KB of EEPROM. This is a further successful example of suppliers cooperating to provide a complete solution.

The system has been supplied by partners of Citizens' Card Alliance, whose Chairman Len Saunders said: "It has been a great pleasure to assist in the implementation of a smart card scheme offering real and immediate benefits to the community in Torfaen, and this visionary concept is sure to be replicated widely throughout Wales and elsewhere, as it conforms so closely to the Government's aspirations to encourage children into a healthier lifestyle" The total project cost £60,000, £43,000 coming from the lottery and £16,000 from Torfaen County Borough Council.

18