July 2007

Volume 16 • Number 07

Smart Card & Identity News

Smart Cards, Identity Managment, SIM, Biometrics, NFC & RFID

01 • London to Get "OnePulse"

06 • RT Program for Reno Airpott

07 • Visa Says Fraud is Low in Asia

05 • Oberthur Plans Re-Organisation

This Month's Lead Story

London to Get "OnePulse"

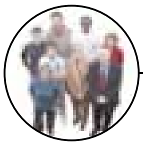
Barclaycard has unveiled its new three-in-one SmartCard that combines the Transport for London (TfL) Oyster contactless travel pass, Visa's payWave contactless technology and a chip-and-PIN credit functionality. The Oyster function on the card will operate independent of the credit facility. This new card, called OnePulse, is on track to be launched across London this September.

Barclaycard is expected to launch a citywide marketing push to promote OnePulse in August and September. OnePulse cardholding commuters will be able to swipe Oyster readers to pay for travel as they already can with the standalone card, using it either on a pay-as-you-go or season ticket basis. OnePulse cardholders will benefit from the cheapest fares on the Transport for London bus, rail, Tube, DLR and Tramlink networks using Oyster, exactly as they do with conventional Oyster cards.

As well as acting as a credit card for transactions over £10 using chip and PIN, the Smart Cards radio frequency identification (RFID) technology will allow cardholders to make low value purchases below £10 without entering a PIN or signature, thus reducing a customer's reliance on cash. These transactions will be listed on the cardholder's credit card statement. This will be the first time the Oyster card system has been added to a bank card, and the first time a contactless payment system, where users do not need to enter a Pin or sign for purchases under £10, has been used in the UK.

Elizabeth Chambers, Chief Marketing Officer of Barclaycard, said: "London is a fast paced, dynamic city that is always looking to the future. We wanted a brand name that conveyed the sense of energy that runs through the city while at the same time highlighting the card's unique three-in-one feature."

Continued on page 3........



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

Head Office: Smart Card Group,
Columbia House, Columbia Drive,
Worthing, BN13 3HD, UK

Telephone: + 44 (0) 1903 691 779

Fax: + 44 (0) 1903 692 616

Website: www.smartcard.co.uk

General Enquiries:
info@smartcard.co.uk

Editorial

Managing Director - Patsy Everett

Editor - Jason Smith

Technical Advisor - Dr David Everett

Subscriptions & Administrator - Lesley Dann

Editorial Consultants - Peter Hawks, Simon Reed,Robin Townend

Contributors to this issue - Accenture, Martin Gruber, "The Squeaker", Laurent Bailly, Bernard Van der Lande and Jason Smtih.

Printers - Hastings Printing Company Limited, UK

ISSN - 1755-1021

Disclaimer

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

Our Comments

Summer holidays are here again and the parents amongst us are no doubt looking forward to the annual trek, camping, caravanning, or why not just hop on that plane. In fact readers in the UK have probably heard that the jet stream this year is running some 200 miles further south than normal and that we can expect a summer washout as a result.

Now this can only make us think about travel, ePassports, ID cards and biometrics, but that is only the start because we then need to add all the security controls before we move airside. This has become a very emotive subject, ideal for the boring party that needs a bit more zap, fill your glass, light the fuse and retire quickly. Governments are of course concerned to identify the traveller but we are more immediately concerned about what they might be up to on our shared journey. The trouble is that terrorists are often unknown until the day they do their business and there is a limit to what the security controls will find as you pass through their enclosures.

Have you come across the millimetre wave body scanners? They have been designed to see exactly what a person is carrying on their body, it will even spot ceramic knives as used by the 9/11 terrorists. The thing here is how much is your personal privacy breached, the images are pretty revealing, another one for that party. Now here is the question, what would make you a happier traveller? Would it be better identification and/or profiling of your fellow travellers or would it be better searches of persons and their luggage? I'll bet you would rather have better identification (and knowledge) of the person, long live the ePassport, eID, National Identity Register and biometrics. We just need to find a way of making them work.

Patsy

Contents

Regular Features

Industry Articles

....continued from page 1

Barclaycard also recently announced London take-out salad bar, Chop'd as the first retail partner to sign up for its in-store contactless payment system. The agreement will see the retailer adopt the new technology this autumn in all three of its central London outlets with the intention to roll out additional contactless terminals in further outlets due to open later this year. Barclaycard is aiming to sign up hundreds of other retailers, including newsagents, coffee shops and cafes, who will install card readers at their tills. They are also in talks with the manufacturers of vending machines to allow people to swipe their cards to pay for drinks, sweets, or car park charges. A debit card version is also being planned. Other credit card providers also plan to launch contactless payment facilities, with the Royal Bank of Scotland and American Express announcing their own versions. The industry predicts that 5 million contactless cards will be issued by the end of 2008 and these will be accepted in over 100,000 retail outlets.

Hundreds of Barclaycard employees have been testing the system at its Canary Wharf headquarters for the past four months. This trial follows the announcement last December of the deal between Barclaycard and TranSys, the consortium which runs Oyster card in partnership with TfL, to combine Oyster and Barclaycard on one piece of plastic. John Stout, Chief Executive of TranSys, said: "Like the Oyster card itself, the key to the success of this initiative is its simplicity. Barclaycard came to us with an idea which could be dovetailed seamlessly with Oyster's existing functionality to deliver added value for Barclaycard customers, without disrupting a service which has become part of London life for millions of people." The scheme has the backing of the Mayor of London. "This new deal will mean that from next year people can buy low-cost items and take advantage of Oyster fares on the same card, reducing the need to carry cash," said Ken Livingstone.

Cameron Olsen of Smart Technology Solutions gave his view of this new launch; "The launch of the Oyster credit card by Barclaycard is an opportunity to get consumers used to using one card with three separate but related features - credit card, small payments and travel card. When buying things like newspapers or sandwiches during a lunch hour, contactless cards offer consumers a great deal of convenience for these low value but high volume transactions. The contactless trials show the potential of extending the EMV technology to run other new applications, such as loyalty schemes, card consolidation, two-factor authentication, post-card issuance management and e-gift cards, the card industry will maximise their EMV offerings and increase their revenue in the long-term. The announcement by Barclaycard is a forerunner of how contactless cards will soon be launched in the UK, following the current practice in the US. The trial in London is consistent with the mind set of a high density of consumers who are already used to the contactless Oyster card."

Elizabeth Chambers concluded: "We believe Barclaycard OnePulse is the future of payments in London and hope as many Londoners as possible enjoy the benefits when it is rolled out in the autumn".

Events Diary

August 2007	
21 - 22	Technology in Government & the Public Sector Exhibition - *Canberra, Australia*
September 2007	
19 - 20	Training on Biometrics - Smart University - S*ophia Antipolis, French Riviera - www.e-smart.eu*
19 - 21	e-Smart 2007 - *Sophia Antipolis, French Riviera - www.e-smart.eu*
19 - 21	World e-ID - *Sophia Antipolis, French Riviera - www.worlde-id.eu*

Smart Cards

Even the Security Experts Get Hit

The US Government's Department for Homeland Security has acknowledged it suffered from more than 800 hacking attacks, virus outbreaks and other malware problems. In one incident, hacker executables for extracting sensitive information, including password files, were found on two internal computer systems at the department. In another case, workstations at the US Coast Guard and the US Transportation Security Administration were found to have malware that attempted to relay information to the outside world. And, as in any large organisation, officials admitted that laptops had gone `walkabout' and various Web sites suffered attacks.

Commenting on the revelations made in US Congress this week, Calum Macleod, European Director for Cyber-Ark said that the fact that the US agency charged with security is getting hit by IT security problems is a warning to everyone. "It highlights the need for extreme vigilance when company and customer data is involved. It is to be hoped that the agency practices what it preaches and keeps its critical data in a digital safe that is heavily encrypted," he said.

AST Accepts Takeover Bid

Advanced Smartcard Technologies (AST), a developer of payment technologies, has announced they have accepted an £18.7 million ($37.4 million) take over bid from Trainline Investments Holdings Ltd, a provider of rail tickets and rail information. The acquisition of Advanced Smartcard Technologies will allow TheTrainline to develop its own Smart Card systems for rail passengers.'One of the ways that TheTrainline provides benefits to rail industry stakeholders is in developing and implementing new methods of rail retailing and information services, designed to reduce costs and enhance customer service,' said TheTrainline's Chief Executive Alan Tomlin.

'The ability to be able to purchase a rail ticket or have a rail ticket fulfilled to a Smart Card or smart-enabled mobile device in a secure manner is one such important development.' Tomlin says the acquisition of Advanced Smartcard Technologies will allow the company to meet its objectives in that area in the shortest time.

NIST Aims for a Better Smart Card

The National Institute of Standards and Technology is inviting vendors to participate in a feasibility study to determine whether a technology called Secure Biometric Match-on-Card can be used with contactless Smart Cards in government applications. The agency wants to determine whether the resulting transactions would be secure, accurate and fast enough for government use.

Smart Card System Piloted in NY

Mount Sinai Medical Center and nine other New York City metropolitan-area hospitals have launched a pilot program that provides patients with Smart Cards, which can hold the equivalent of 30 pages of medical records. The 64-kilobyte cards, developed by Siemens Medical Solutions, are intended to reduce paperwork, protect against medical errors and improve communication between patients and hospital staff. Information contained on the cards includes current medications and allergies, test results, chronic conditions, a brief medical history and personal data, such as date of birth and insurance coverage. Forty-five New York and New Jersey hospitals eventually could participate in the program.

Chip and PIN for Cyprus

TSYS Card Tech, a wholly owned affiliate of global payments provider TSYS, has announced the introduction of EMV cards to Cyprus through partnerships with three Cyprus-based banks. As part of the Cyprus PIN & PAY initiative that came into effect in March 2007, TSYS Card Tech has been successfully certified for Visa Smart Debit/Credit (VSDC) and MasterCard M/Chip. The first three banks to roll out EMV cards using TSYS Card Tech's PRIME card management system are Marfin Popular Bank (formerly Laiki Bank, Cyprus), Hellenic Bank and Universal Bank. The banks will roll out the new cards during the next two years, as they replace existing magnetic stripe cards with EMV cards as their expiry date approaches.

Sagem Orga Gets e-Health Contract

Sagem Orga has been awarded a contract to provide Techniker Krankenkasse's (TK) almost 6.1 million policy holders with electronic health cards (eGK). Based in Paderborn, Germany, Sagem Orga beat other competitors in an open call for tenders organized by health insurer TK. The contract between TK and Sagem Orga was signed on June 29, 2007.

"Sagem Orga proved to be the most competent partner with the best developed concept for our purposes. We are looking forward to collaborating with them on this project," confirmed Frank Siener, Head of Corporate Development at TK. "The most crucial aspect for us is being able to provide our policy holders with an efficient infrastructure delivering added value. As a family-oriented insurer, we are keen to redefine our customer-friendly online services in conjunction with the electronic health cards and we intend to use Sagem Orga's tried and tested eHealth technology for this."

35m e-Health Cards for Germany

Gemalto has been awarded the tender held by insurance organisation AOK (Allgemeine Ortskrankenkasse) to supply and personalise e-health-cards for their insured in Germany. The contract win comes after Gemalto took part in Germany's first healthcare pilot program based on highly secure microprocessor cards. Gemalto's new advanced digital healthcare solution will avoid duplicate examinations and therefore lessen unnecessary use of healthcare services. In addition, the new health card will be able to carry electronic prescriptions, which will significantly reduce paperwork. Finally, by allowing data update once the card is in the field, the new system enables insurance funds to potentially adjust their cost of ownership.

Nottinghamshire Gets Freedom Card

The first ITSO live Freedom Card has been issued in Nottinghamshire, UK. The scheme, run by Nottinghamshire County Council and using the ACT ITSO HOPS (AMS) managed service is one of a number of innovative transport projects in the UK focusing on ITSO interoperable Smart Card ticketing. The Freedom Card scheme migrated to ITSO early last year, when ACT was selected to provide their Full HOPS (AMS) as a managed service. ITSO will allow greater flexibility of use and further opportunities for expansion into other transport modes (such as trams, trains), integrated ticketing, seamless travel and additional applications. Over 140,000 cardholders will be issued with the card in and around the Nottinghamshire area.

New Organisation SAFRAN Branch

From July 1, 2007, the Defense Security Branch of the SAFRAN Group will be organised in to two main companies, Sagem Défense Sécurité and Sagem Sécurité. Sagem Défense Sécurité will now have has two subsidiaries, Sagem Avionics Inc. and Vectronix AG headed by Jean-Paul Herteman, SAFRAN Executive VP, Defense Security and Chairman and CEO of Sagem Défense Sécurité. The newly created Sagem Sécurité unit encompasses biometric identification systems, secure transaction terminals and Smart Cards.

SCN Consultant Receives Degree

Peter Hawkes, one of Smart Card and Identity News' editorial consultants, has received an honorary degree from the University at Kent. Mr Hawkes led the team pioneering the application of integrated circuits in telecommunications, initiating several projects on Smart Cards, biometric identification and secure network technology.

Smart Cards for Indian Banking

Gemalto has announced the successful introduction of Smart Card technology with biometric authentication for Financial Information Network & Operations Ltd. (FINO) in India. The Gemalto solution securely stores transaction records inside the Smart Card to enable microbanking and simplifies access to financial services for the under-banked population in rural India. Each FINO card developed by Gemalto can hold up to 15 different types of secure applications that facilitate financial services such as deposit remittances, savings, loans, insurance and e-purses.

Oberthur Plans Re-Organisation

Oberthur Card Systems has announced a project to re-organise its industrial sites. Oberthur Card Systems plans to organise itself into major centers in each region, in order to achieve economies of scale while maintaining geographical proximity to its customers. In this context, card personalisation centers in the United States will be re-organised into two centers instead of three. The business of the Naperville site (Illinois), which employs 124 people, will be transferred to the Los Angeles (California) and Chantilly (Virginia) sites.

In addition, in order to maintain production in France in a sustainable way, Oberthur Card Systems intends to implement an industrial reorganisation plan: 1) the production of high added value SIM cards and manufacturing, currently taking place in Caen, will be kept in France and reorganised alongside the manufacture of bank cards at the single site in Vitré, 2) the production of SIM cards with low added value will take place in existing sites outside Europe.

This plan will be the subject of a consultation process involving the company's staff representative bodies. In France and in the United States, Oberthur Card Systems will undertake to introduce a number of measures to promote the geographical or professional mobility of its employees. In particular, every one of the 163 employees at Caen will be offered employment at Vitré or elsewhere within the company, as a minimum. Oberthur Card Systems has decided to maintain productions in France and in the United States.

BoG to Introduce Smart Cards

The Bank of Ghana will soon introduce a national Biometric Smart Card to address the shortcomings of the existing debit cards, which cater for only a fraction of the population. The Deputy Governor of the Bank of Ghana, Dr Mahamadu Bawumia, who announced this at the launch of new products by Amalgamated Bank Limited said the Smart Card would allow financial institutions to deploy products for the bank and the unbanked. "The Biometric Smart Card, for example, is designed to function in locations without electricity and telecommunication equipment and eliminates the need to have basic literacy to operate a bank account," Dr Bawumia said.

Smart Cards for Foreign Spouses

About 70,000 foreign spouses married to Malaysians who have social visit passes for Malaysia will be issued personal identification Smart Cards, possibly by next year. This means they will no longer have to carry their international passports with them when they go out. "We are considering issuing the Smart Cards to spouses in view of the many queries we have received from them," said Auk Tan Chai Ho, the deputy Home Minister of Malaysia.

Smart Card Pilot Project in St-Jerome

National Bank has announced that it plans to carry out a Smart Card pilot project in St-Jerome, Canada in summer 2008. This project will enable the Bank to test the compatibility of its ABMs and systems with this new technology in a controlled environment while ensuring the reliability of various other elements involved in payment and transaction processes. "Smart Card technology is a powerful tool that will open up a world of opportunities. This project is evidence of the Bank's commitment to developing a new line of innovative, user-friendly and secure products for clients," stated Paolo Pizzuto, Vice-President - Electronic Payment Solutions.

Toronto Hospitals Get Smart Cards

Two Toronto-area hospitals are switching their magnetic swipe card system to the installation of the Verex Smart Card readers, with Mifare technology, to read and write to contactless Smart Cards, in an effort to make their systems more secure and reliable. Trillium Health Centre and The New Women's College Hospital have selected Mississauga-based Veridin Systems Canada Inc. to deploy the system. Veridin integrates security systems for buildings, involving card access, video surveillance, and alarm systems.

RT Program for Reno Airport

Daon has announced that Unisys Corp has entered into a long-term commitment to standardise on Daon technology as the identity management platform for Unisys rtGO Registered Traveller (RT) program. rtGO will first be deployed at the Reno-Tahoe International Airport in Nevada. Unisys rtGO program allows frequent travellers to provide background information to the Transportation Security Administration (TSA) for pre-screening purposes. When approved, travellers receive a biometric-enabled Smart Card that allows expedited passage through any airport in the nation that is participating in the Registered Traveller program.

Germany Invests in ID Education

Bundesdruckerei GmbH is to endow a professorship in "Secure Identity" (identity protection technologies) at Berlin Free University, selectively promoting the advancement of an important future technology. The endowment professorship is initially scheduled to run for five years. The professorship will be based in the Mathematics and Information Technology faculty, and the successful applicant is expected to take up the post this October. The Chair will specialise in the research and development of security technologies, especially those centred around the reliable identification of individuals and secure communications.

Experts expect this key technology to assume a far more prominent role in the international arena over the next few years, with growing economic significance. Berlin-based company Bundesdruckerei GmbH is already a technological leader in this field. Many countries around the globe use high-security identification systems from Bundesdruckerei to ensure that identities are protected.

The endowment professorship aims to advance the internationally important field of civil security research, specifically the secure identification of individuals, and focus on the development of new solutions. By endowing this new Chair, Bundesdruckerei will be helping to train talented young people in a field of expertise which is much sought-after worldwide.

$1.5m Follow-On Order for ID Cards

LaserCard Corporation has received $1.5 million in purchase orders for the LaserCard Optical/Smart-based national ID card project in a Middle Eastern country. One purchase order, valued at approximately $0.9 million, is for the supply of secure national ID cards under a previously announced subcontract. This follows orders previously delivered bringing the total value received under this subcontract to more than $6 million. Delivery under the current order occurred in June.

ITG Acquires Aontec

Assa Abloy Identification Technologies (ITG) has acquired Aontec, a manufacturer of inlays for secured electronic documents including passports, national ID and driver's licenses. Through this acquisition, ITG will now have a presence in over 15 countries with two certified European production sites for e-document components.

Visa Says Fraud is Low in Asia

Visa International Asia Pacific President and Chief Executive Officer Rupert Keeley said that while fraud for Visa in Asia Pacific has fallen to an historical low, there was no room for complacency as the payment business was always going to remain attractive to the criminally-minded. "While fraud levels in the Asia Pacific are at an all-time low, it is incumbent on all players in the payment industry to continue to focus on protecting cardholders' data," Keeley said at the annual Visa Asia Pacific Risk Management Conference in Singapore. Since 2001, Visa has been working with the industry to roll out secure EMV chip technology across the region.

"The success of Visa's EMV chip program can be seen in the lower rates of counterfeit fraud across Asia Pacific. However as industry players get to grips with counterfeit fraud, we need to remain vigilant against the new ways in which fraudsters are seeking to operate." said Peter Maher, Visa International's executive vice president and general manager for Risk Management, Asia Pacific.

EFTPOS Market to Reach 10,769

Driven by EMV compliance, the world electronic funds transfer POS (EFTPOS) terminals market is projected to reach 10,769 thousand units by the year 2010 according to a new report by Global Industry Analysts, Inc. The fast approaching Europay, Mastercard and Visa (EMV) deadline is stepping up growth momentum in the world point of sale (POS) terminals market. The deadline for migration is encouraging upgradation to EMV compatible POS systems thereby creating new business opportunities in the marketplace.

In the world EFTPOS terminals market, Asia Pacific holds ample opportunities for growth with a CAGR of 14.34%, while in the United States, growth is mediocre with the market forecast to rise by 402 thousand units between the period 2007 to 2010. Europe ranks as the largest market for EFTPOS with a share of a little over 37% in the world market. The region is far ahead of other regions in the implementation of EMV standards, with Germany the largest individual market poised to clock a CAGR of 12.2% until the year 2010.

The largest product group, Smart Card Enabled EFTPOS Terminals market in Europe rakes in a share of above 93%. Shipments of magnetic stripe card readers in Western Europe are negligible with almost all shipments concentrated in Central and Eastern Europe. In Asia, China represents an optimum market for ferreting business opportunities, given China's rush to migrate to the EMV standards before the 2008 Olympics scheduled to be held in Beijing. India trails next as an attractive market largely stimulated by the spectacular growth in organised retailing. Magnetic stripe card EFTPOS terminals market in Asia corners a share of little over 39%, while Smart Card enabled EFTPOS terminals market mirrors the potential to grow at a CAGR of 15.4% over the study's review period.

Biometrics

Biometrics Growing Fast in EAC

New analysis from Frost & Sullivan into the North American Electronic Access Control Markets (EAC) has revealed that revenues in this market totalled $1.32 billion in 2006, and estimates this to reach $4.19 billion in 2010.

"The North American EAC market is increasingly driven by mandates and other standardisation procedures undertaken across the different verticals," notes F & S Research Analyst Janani Sankaran. "Biometrics, in particular, is emerging as the fastest growing segment of the North American EAC market, benefiting tremendously from legislations such as the Aviation and Transport Security Act."

Furthermore, in recent months the biometrics industry has achieved a number of compliance milestones. For instance, INCITS and ANSI have approved the BioAPI standard, while INCITS 358-2002 Information Technology-BioAPI Specification and the Common Biometric Exchange File Format (CBEFF) have been augmented for international harmonisation. Besides biometrics, Smart Card-based EAC segment will also experience growth in the next few years fuelled by the emergence of contactless Smart Cards. However, the shift from magnetic stripe cards to Smart Cards is progressing at a slower than anticipated pace, and this could represent a major challenge for the Smart Card based EAC market.

Biometric ATMs for UAE

An un-named UAE based bank is currently in the process of installing a new biometric security system which will entail its customers needing to undergo fingerprinting and iris scanning in order to withdraw money from ATMs, reported Gulf News. The new system, which will still require customers to punch in their pin numbers, is expected to be implemented within six months.

Biometric ID for Norwegian Airport

Molde Airport Aaroe has become the first Norwegian airport to introduce biometric fingerprint ID checks of airline passengers at the check-in counter. The passengers are first scanned upon checking in, and are then checked for a match before entering the aircraft. In this way it is ensured that the passenger entering the plane is the same as the one that checked in the luggage.

Cost of Cards to Fall

IBM is currently working on a technology which would largely reduce the cost of transactions carried out through biometric Smart Cards, the new engine of growth for the micro-finance sector. A biometric card provides customer authentication through fingerprint and the card is used on hand-held devices to get the entire solution going. However, the cost incurred remains a challenge as the volumes are low and ticket size of the transaction is small. IBM, which has partnered with Financial Information Network and Operations Private Ltd (FINO) to offer the complete backend support, expects that product will make the processing faster. "We expect more than 10 million customers to be on the biometric Smart Cards platform over the next five years. To support the growth, the product will make transactions speedier and leaner thereby reducing the cost," said, IBM Head (Strategic Solutions-BFSI) Subrata Dasgupta.

Iran Unveils New Biometric Passports

Iran has unveiled its first series of biometric-enabled passports for diplomatic purposes, says a Foreign Ministry official. Deputy Foreign Minister for Consulate, Parliamentary and Iranian Expatriate Affairs Mohammad-Ali Shahidi said that diplomatic types of biometric passports had been issued, adding the government has released biometric passports for all applicantssince the end of the Iranian year (March 2007). Given demands by the International Civil Aviation Organisation for the use of biometric passports sine 2007, the Consulate Department of the ministry has made every endeavor to prepare the high-tech documents, he added.

New Products/Services

Datacard Teams with Aconite

Datacard Group and Aconite Technology have announced they have joined forces to offer customers complete EMV migration and smart pre-paid card solutions, including transaction processing, scripting, key generation, key storage and clearing data validation. These solutions bring together both companies best-in-class products: Datacard Affina Issuance and Affina Enterprise software solutions and Aconite's EMV Script Processor (ESP), EMV Transaction Enabler (TRxE) and Pre-Paid Value Manager (PPVM).

UBnics 1st MULTOS Step/One Chip

The MULTOS Consortium has announced that UBnics, a provider of Smart Card operating systems, applications and solutions in South Korea, released its first implementation of MULTOS step/one on the NXP P5SD009 dual interface chip.

The UBnics / NXP MULTOS step/one chip comes with 12K of E2PROM programmable memory, sufficient to support a range of applications including Paypass, M/Chip, VSDC, ATM, Mifare and others, and is one of the most cost effective modules for contactless payment on the market. The chip is fully interoperable with the existing range of MULTOS modules from other MULTOS implementers, bringing the choice of silicon families supporting MULTOS to four: NXP, Infineon, Renesas and Samsung.

SCM Card Reader Approved by GSA

SCM Microsystems, Inc has announced that its SCR3310v2.0 Smart Card reader has been approved by the US Government Services Administration (GSA) as compliant with Homeland Security Presidential Directive (HSPD)-12. As a result, the SCR3310v2.0 Smart Card reader is now included on the GSA's FIPS 201 Approved Product List that governs which products and services may be purchased by federal agencies for the HSPD-12 program.

Atmel Qualified by FIME

Atmel Corporation has announced that FIME, an external and independent third party laboratory, has certified that Atmel's AT90SC12872RCFT secure microcontroller is compliant with ICAO (International Civil Aviation Organisation) and ISO 14443 specifications (contactless interface for Smart Card).

PAYware For Hong Kong's Gift Card

VeriFone Holdings, Inc has announced that stored value gift card program provider ValuAccess has selected VeriFone's PAYware GiftCard as the technology platform for its gift card system. The system was initially rolled out in ValuAccess's home city of Hong Kong and is planned for other major urban areas across China and the rest of Asia.

New Biometric Smart Card Keyboard

Athena Smartcard Solutions is introducing the ASEDrive IIIe USB Bio KB, a combined biometric Smart Card keyboard which incorporates the UPEK TouchChip TCS2 fingerprint sensor, enabling strong user authentication and password-free logon to PCs. Security is further enhanced by the incorporation of the ASEDrive Smart Card reader for multi-factor authentication in this new USB keyboard.

On The Move

New Managing Director at G&D

As of July 1, 2007, Jean-Louis Dieu has taken the helm of the French subsidiary of Giesecke & Devrient (G&D). Mr. Dieu has worked in the field of Smart Cards since his career began in 1977. The next step for the new G&D affiliate will be to integrate Smart Card based solutions for industry and local administration into its portfolio.

SCM Microsystems CEO to Leave

SCM Microsystems Inc has announced that Robert Schneider, the company's founder, Chief Executive and Director, will leave at the end of the month. Schneider, 56, is leaving to pursue other opportunities although nothing specific has been announced, according to a company spokesman. SCM's board has started a search for a new CEO and Stephan Rohaly, SCM's chief financial officer, will take on the role of interim CEO.

New Chairman at Ingenico

Ingenico has announced the appointment of Jacques Stern as Chairman of the Board of Directors. Ingenico has benefited from Jacques Stern's expertise on its Board of Directors since April 2005.

EMV Specialist Joins Bell ID

Bell ID has appointed Wynand Vermeulen as Manager Financial Solutions to further strengthen their position as market leader with the ANDiS4EMV solution. In his new position, Mr. Vermeulen will be responsible for the strategic direction and continued development of a suite of products based around ANDiS4EMV.

Two New Vice Presidents at Zebra

Zebra Technologies Corporation has announced that Donald F. O'Shea and Chester J. Trocha have joined the company as Vice Presidents in newly created positions.

New Director at Cubic

Cubic Corporation has announced the appointment of David W. Liddle to the position of Director, Corporate Communications. Liddle will be responsible for managing development and administration of all aspects of Cubic's communications.

The Future of Identity

By Accenture

A knock at the door, followed by"Who's there?" This most basic question of identity is older than the tale of Little Red Riding Hood. But with new virtual doors opening online-and as a growing number of clever cyberwolves hide their identities-the answer has become more complex and costly. The stakes are rising dramatically as far as identity fraud is concerned. Identity theft is the fastest-growing crime problem in the United States, according to the Federal Bureau of Investigation. In the United Kingdom, the Home Office estimates 100,000 citizens are affected each year. A report from the Aberdeen Group forecasts the global cost of identity theft will have reached $2 trillion by the end of 2005, and "traditional access and integrity controls will do nothing to stem the tide."

People whose identities have been stolen can spend months-and sizable sums of money-clearing their names and cleansing their muddied credit histories. Also, consider the knock-on effect on costs and image for businesses and governments alike. "Phishing" lures Internet users to what appear to be trusted bank or government sites through spam and pop-up messages. At the fake sites, unsuspecting users enter in bank account information, credit-card numbers, passwords and other confidential data. Thousands of people have been hoodwinked in such scams, and their revealed data can be used to apply for credit, obtain mobile phones, print fraudulent checks on personal computers, or apply for government benefits.

Identity also looms large on the radar screens of governments concerned about illegal immigration and terrorism. But there is a delicate balance to maintain. Lax controls may appear to roll out a "welcome mat" for international criminals. But border controls that are too tight can slow international trade and tourism to an irritating crawl. Increasing globalisation, terrorist threats and online fraud are prompting governments and businesses to search for more intelligent identity solutions. Technology developments and scientific progress are paving the way for new solutions with biometrics. Biometrics help strengthen identity systems by adding in physical or behavioral characteristics (e.g., fingerprints, facial structure, iris structure, signature, gait) to the identity information. Accenture Technology Labs, the technology research and development organisation of Accenture, has been researching this technology to understand the impact of biometrics based systems that deliver greater accuracy, speed and convenience for enhanced performance of governments and businesses.

What is identity? - Our sense of identity is assumed so that many of us take it for granted. We expect people to know us and trust what we tell them. But what exactly is identity, and how do we go about determining if the stranger seeking access to our offices or website is truly who he or she says she is? "Simply keying in some personal data-which can be stolen in a phishing scam or fishing through garbage and finding old credit-card and bank statements-is no longer enough to assure identity and deter fraud." Identity can be thought of as a set of characteristics uniquely associated to a person. There are three attribute types: primary (e.g., name, date of birth), biographical (e.g., schools attended, marriage) and more recent biometric methods (e.g., voice, hand geometry, iris, ear shape).

Businesses and governments employ systems, usually electronic, to store data to establish whom to include or exclude. In these systems, a process of enrollment records characteristics of individuals in a data store. Once an individual is enrolled, he or she receives a token-a passport, driver's license or Smart Card with printed or embedded information-as proof of identity. Because Internet transactions continue to increase, organisations are upgrading their online ID systems. Consequently, organisations should look to biometrics to add another layer of assurance to establish and confirm identity.

Increasing complexity, fragmentation and frustration - Whether by accident or design, identity schemes have grown in complexity and diversity. Efforts for standardisation are under way by various organisations-including the BioAPI consortium and International Standards Organisation-but guidelines are not yet ready or being widely followed. Local and regional government agencies (e.g., health, motor vehicle, voting) follow protocols and require different tokens to national identification schemes (e.g., passports, visas, residence permits). Consequently, people's wallets and purses bulge with a growing number of cards and identity papers. Accenture has identified four broad models among national governments to establish identity:

❐ Common law (US, UK, Australia, Canada), with no national ID card or identifier, and people relying instead on drivers' licenses and passports.

❐ Civil law (most of the original European Union countries), with a mostly compulsory national ID card.

❐ Nordic model (Denmark, Sweden, Norway and Finland), with a centralised unique identifier, and optional digital certificates on private-sector cards (e.g., banks).

❐ Asian model (Malaysia, Hong Kong and Singapore), with compulsory multipurpose electronic ID cards.

Several South American countries use the civil law identity scheme, as do many African nations, where biometric ID techniques are growing in acceptance. Mauritania and Nigeria require fingerprints for citizen identification, and Uganda uses face recognition for voting purposes. In South America, Peru stores fingerprint information in bar codes. The weakest link of current systems is enrollment. In other words, if an individual can easily be entered into an identity system by submitting false documentation, the system has serious flaws. Ahmed Rassam, who confessed participation in a plan to bomb the Los Angeles airport during New Year's 2000, obtained a valid Canadian passport after having obtained a blank, stolen baptismal certificate. (An historical note, by the way: birth certificates were introduced to record life-expectancy statistics and were not intended to form the basis for strong personal identification.) In addition, seven of the 19 hijackers in the 2001 terrorist attacks in the United States held valid drivers' licenses that were obtained with phony documents.

We need security, but what about privacy? - Identification is not always required nor wanted. People expect anonymity at certain times: walking down a city street, seeing a movie, telephoning for quotes to compare prices, participating in surveys or clinical trials. At other times, establishing identity may be required initially (to determine voting eligibility, for example) but not later on so as to keep private the choices made by an individual. As with other technologies, biometrics are not intrinsically good or bad. Their application needs to be judged by intent and usage. In the futuristic movie "Minority Report," the law-enforcement officer played by Tom Cruise has his retinas scanned to gain access to high-security areas. This seems to be a worthwhile and convenient application of biometrics for work-related security. But the film also depicts a "Big Brother" environment as sensors scan the hero's eyes in public spaces to establish his identity and personalise holographic advertising messages. Since he seems unable to escape being bombarded by promotional messages, this application of biometrics seems invasive and offensive.

Privacy issues are not exclusive to biometrics, and businesses and governments have recently tightened procedures and regulations to keep personal data from being misused or falling into the wrong hands. In Accenture's view, it is in the best interests of organisations to regulate themselves through the systematic development of trust. A company that is known to violate the privacy of customers is likely to lose business to competitors as word of ethical lapses spreads. The Organisation for Economic Co-operation and Development has an Information and Privacy group working to promote a "global, coordination approach to policymaking … and to help build trust online". In addition, the BioPrivacy Initiative of the International Biometric Group seeks "to increase the likelihood that biometric technologies, when deployed, will be as protective of personal and informational privacy as possible". Biometrics, for example, can strengthen privacy by denying access or release of confidential information to the wrong people.

Best practice relies on multiple factors - How will organisations deliver a stronger, more reliable ID infrastructure? Amid the increasing volume and speed of international travel and commerce, governments must perform a balancing act. They must weigh security concerns with the needs of business people and the desire of tourists not to spend half of their trips abroad clearing security. Similarly, when venturing online, some users have so many passwords and user names to keep track of that secret-access codes end up written on Post-It notes stuck to computer terminals-so much for network security. The emerging wave of new systems aims for triple strength. In simple, non-technical language, they require something you have, such as an ID card or token; something you know- a PIN or password, or a shared secret; and something you are, supplied by biometric applications. When it comes to biometrics, no one system is best in all cases, and acceptability is an obvious concern.

Fingerprinting, for example, is often associated with criminal behaviour, although the development of inkless fingerprinting removes some of this muddy taint. Members of some religious groups might not consent to a photograph of an unveiled face. Other people might wonder if there are health risks to iris scans (more accurate than fingerprints), and people with eye diseases might be excluded from being enrolled with this metric. Consequently, Accenture believes the future lies in multimodal biometrics, which consists in using a combination of several biometrics, depending on the application, individual and interaction channel. More in-depth study needs to be conducted to identify the most suitable biometrics for specific applications. No technology is 100% foolproof, which is why multimodal solutions are advisable, and why human intervention will be required in exceptional cases.

For speed and efficiency, identity needs to be recorded in electronic format for automation and network based validation. Fortunately, content technologies enable the storage of biometrics data in digital format. In addition, Moore's law is still valid, and storage capacity and speed continue to race ahead at a remarkable pace. While the costs are relatively high now, they will come down with time and large-scale deployment. As businesses and governments head toward electronic solutions, it is important to keep in mind there needs to be a transition (i.e., backward compatibility) with paper. This can be achieved in the near term, for example, by travellers carrying a Smart Card version of a passport along with a traditional paper version. A likely success factor in biometric solutions is giving people a choice to opt-in for more advanced technologies and convenience. In Spain, the Baja Beach Club in Barcelona offers patrons a choice between a standard access card and a radio frequency identification (RFID) chip, about the size of a grain of rice, implanted under the skin of the triceps.

A scanner reads the microchip and sends out a radio frequency signal. The chip enables patrons to jump the queue for club entrance and to have drink purchases tracked and paid for without carrying cash. Innovative biometrics applications in government and industry - Another example can be seen at Galp Energia, an oil and gas company formerly owned by the Portuguese government. Galp Energia set out to become the world's first petrol-station operator to install a thumbprint biometrics payment system. Accenture was part of the team that helped develop this solution. Within four months, customers who elected to join the scheme conducted transactions 75% faster and company performance has improved, as have customer satisfaction ratings.

Additional biometric applications can be found in fleet management. International attacks on fuel-laden tankers have prompted security officials to include trucks on their lists of potential terrorist targets. To help prevent dangerous and costly incidents, Accenture has developed Transport Security Services, a prototype to provide security throughout a truck's journey from manufacturing plant to delivery point. Biometrics, in the form of fingerprint technology, are used to identify the driver before the truck door can be opened, thus ensuring that only authorized personnel can drive the truck. A large number of biometric trials and full-scale deployments are under way for national identity and specific government functions. They are proving that electronic ID schemes are feasible and deliver tangible benefits. For instance, the US-VISIT program, which is taking digital photographs and index finger scans of visitors at a number of US ports of entry, processed nearly 4 million foreign national applicants for admission in the first year.

Since inception, US-VISIT has prevented 372 known criminals and visa violators from entering the country. While people tend to think first of public safety, identity systems with biometrics will provide a wide range of advantages for individuals, businesses and governments. Citizens and businesses stand to face a reduced risk of identity theft. They will also benefit from greater convenience in access to services and benefits, which will be made easier for honest citizens and more difficult for those who aren't. In terms of government operations, citizens can expect to see more efficient use of tax money, with better detection of fraud and more accurate control of service and benefits.

The future of identity, after all, is not only to keep the wolves from the door, but to deliver innovative, high performance solutions that efficiently speed the delivery of products and services to trusted individuals.

www.accenture.com

Interoperability: The Ticket to Smart Card Success in Public Transport Systems

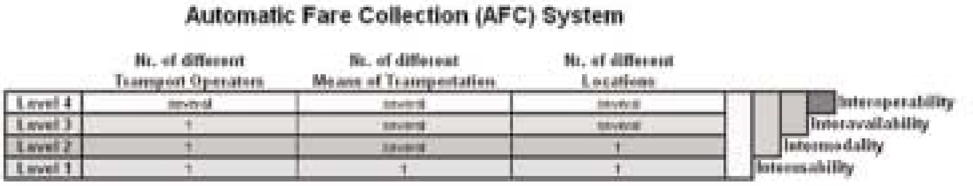
By Martin Gruber, Marketing Management, NXP Semiconductors

Martin Gruber

Millions of people use public transport every day. Some to go to work and back, some to visit their relatives, some to pick up their new iPod in a store outside of town. Whatever reason they travel, it is obvious that for those living in a city, where a contactless Smart Card scheme is deployed, the contactless Smart Card (CSC) in their wallet provides them with a simple, convenient and user-friendly solution, which makes their mobility and life much easier, safer and enjoyable.

Transport operators also benefit from CSC technology, because it helps them to improve safety and efficiency, reduce sales and distribution expenses, and create enhanced customer relationship opportunities, which leads to increased ridership and contributes to clean, efficient, affordable and effective inter-urban mobility. However, a critical factor in making public transport systems successful - and realising the full benefits of contactless Smart Cards over the long term - is to ensure interoperability.

Understanding interoperability: The term "interoperability" itself can create confusion, since it can be defined in more than one way. To understand what we mean by "interoperability," it's helpful to explore four different levels and definitions of the concept:



Automatic Fare Collection (AFC) System

	Nr. of different Transport Operators	Nr. of different Means of Transportation	Nr. of different Locations
Level 4	several	several	several
Level 3	1	several	several
Level 2	1	several	1
Level 1	1	1	1

Interoperability
Interavailability
Intermodality
Interusability

Level 1 - Interusability: On its lowest level (level 1), where the CSC is only used on one means of transportation operated by one transport operator in one location, it is essential that the ticketing media (supplied by various suppliers) is accepted by all front end equipment (supplied by various suppliers). To guarantee such interusability (the usage of ticketing media supplied by various suppliers on infrastructure deployed by various suppliers), transport operators should consider the following: *1)* contactless interface compatibility - à acc. to ISO/IEC 14443; *2)* functional testing & certifications - by independent test houses; *3)* test methods for proximity cards - acc. to ISO/IEC 10373-6:2001.

Level 2 - Intermodality: On level 2, where the CSC is used on several means of transportation (such as buses, trains, trams, subway, and ferry boats) operated by one transport operator in one location, we have to make sure that interusable ticketing media and front end equipment is used and that the data from all stationary computers (subway stations, bus depots, etc.) is collected at a central computer system and updated in an appropriate and secure way. Hence, intermodality implicates an increased need for more advanced: *1)* security - usage of secure application modules (SAMs); *2)* sophisticated backend systems and application software.

Level 3 - Interavailability: On level 3, where the CSC is used on several means of transportation operated by one transport operator in several locations (such as districts, regions, counties, states, etc.), we face the same needs for interusability and intermodality, but as we make the contactless Smart Card scheme available for transportation of users in different and maybe remote geographical areas, transport operators must consider solutions for the following: *1)* interavailability of services and information; *2)* reloading of ticketing media (e-purse); *3)* downloading of contracts and application; *4)* key management - distribution of keys.

Level 4 - Interoperability: On the highest level (level 4) of an automatic fare collection (AFC) system, where the CSC is used on several means of transportation operated by several independent transport operators in several locations, we are challenged with many new and completely different tasks. It is the only level, definition or configuration of an automatic fare collection (AFC) system, where we should use the term "interoperability", because it is the first time that several transport operators cooperate in one and the same CSC scheme.

Hence, interoperability can be described as the extent to which a travel card issued by one public transport operator can be used by other public transport operators. Whereas the usage and availability of system and application objects should be analyzed and discussed on level 1 (interusability), level 2 (intermodality), and level 3 (interavailability), level 4 (interoperability) focuses more on commercial issues rather than on the CSC technology itself. (Remark: on level 1, 2 and 3, commercial agreements are normally only necessary if tickets are distributed and sold through sales agents). The fact that several transport operators work together has a significant impact on the backend system, data model and security framework that goes from the backend right the way out to and into the CSC underlying data model.

To guarantee interoperability, all involved transport operators must agree on the following: *1)* business rules; *2)* rights and duties; *3)* roles and responsibilities; *4)* clearing - to apportion revenues; *5)* security & key management. Other topics that have to be taken into consideration with respect to system-wide interoperability are: *1)* card formats; *2)* system interfaces. Many countries have started to be active in this area - see these two examples: *1)* Australian state governments - Australian Transport Interoperability Protocol (ATIP); *2)* American Public Transportation Association (APTA) - Universal Transit Fare System (UTFS).

In Europe, many associations and public institutions such as the Public Road Administration in Norway, Resekortsföreningen i Norden (RKF) in Sweden and Denmark, ITSO in the UK and the Verband Deutscher Verkehrsunternehmen (VDV) in Germany have put significant efforts into the standardisation of interoperable fare collection systems and therefore, achieved substantial progress.

Besides these national and transnational initiatives, new standards evolve and try to provide transport operators and authorities with a conceptual framework for interoperability on a European as well as on an International level: *1)* EN15320 - Interoperable Public Transport Application (IOPTA); *2)* ISO 24014-1 - Interoperable Fare Management System (IFMS).

What's the impact for my business? - If a transport operator is not sure about which level he is confronted with or which level he needs a solution for, he might end up with a completely over-qualified or under-qualified automatic fare collection (AFC) system. This can create exceedingly high costs at the beginning of an e-ticketing project or extraordinary expenses at a later stage of a project for updates and modifications.

Or you get involved in continuous discussions over what solution on what level to use creating an incredibly long time to market for your CSC based public transport system. As a consequence, users don't benefit from this simple, convenient and user-friendly solution, which could make their mobility and life much easier, safer and enjoyable and don't ride public transport more often than before.

Thus, it is highly recommended that transport operators use available ISO or CEN standards and open specifications on all 4 described levels (incl. security, data model, transmission, etc.) as much as possible to avoid costly implementations of proprietary and non-compatible systems, which make interoperability impossible. In other words, interoperability is the real ticket to success for contactless Smart Cards in public transport systems. Isn't it about time that we discuss interoperability, its challenges and its real-life implications for public transport operators and users?

Rumours From the Front Line

By "The Squeaker" (*a source who wishes to remain anonymous*)

This month Oracle has agreed to buy Barossa Inc, a privately held company founded in May 2003 and headquartered in Santa Clara, California. Bharosa offers online security solutions to protect against the rising risks of Phishing, Trojan and Proxy-based fraud. Their Tracker and Authenticator products offer purely Web-based, multi-factor authentication and online fraud monitoring and detection. Bharosa means 'Trust' in Hindi and the core of their products is that it uses secure virtual authentication devices for entering passwords on-line even if the terminal can't be trusted. The value of the sale is so far undisclosed.

In 2005 Oracle also bought Oblix, specialists in Single Sign On technology. The question here is still whether Oracle can compete with companies such as IBM, CA, Microsoft, BEA Systems and HP. In recent years CA bought ID Management specialist Netegrity for $430 million, HP acquired Identity Management software producer TruLogica while BMC acquired SSO supplier OpenNetworks for $18 million.

Identity Management is at the heart of the acquisition trail of these major players but they are all working on soft solutions and Bharosa is just the latest in a long line. Look in the next field and we have the likes of Gemalto who quite clearly are pursuing a hardware token solution to Identity Management, who is right?On a scale of operations Gemalto is barely scratching the surface but given the regulatory requirements of Sarblanes-Oxley, FFIEC, PCI, GLBA and others who demand that companies determine higher levels of assurance for user identities and authorisation we can ask the question whether a soft solution can be adequate?

Moving back to Bharosa we can start by challenging whether it is possible to trust actions taken at an untrusted terminal. Clearly this is a contradiction, if the terminal is subverted by an adequately resourced attacker then any operation can be compromised even the browser where Bharosa places its trust. Clearly this is not adequate, there has to be some level of trust in the terminal and the Bharosa tracker product also sets out to identify the PC, its location and the user's behavioral profile.

Conversely it seems perfectly reasonable to trust a modern cryptographic Smart Card token. It represents an effective tamper resistant module and can be evaluated under Common Criteria and the like. What you can say is that under this model any action taken at the terminal had to be in the presence of the Smart Card. But are you any better off than the software only schema? I shall leave my security experts to pronounce on this one but what I know is that users don't like carrying widgets.

I would feel that just carrying a Smart Card is OK but not if you have to carry the reader as well, unless that is it just happens to be an object I already have in my pocket like a mobile phone. Coincidentally this also happens to have a Smart Card as well as the reader. This to me makes the Finread terminal with its trusted keyboard and display obsolete because in principle I could achieve the same thing with the phone particularly if the architecture of the phone is based on ARM's TrustZone.

Now all that's left is how do I couple the phone to the PC? Not ideal perhaps but we already have the relatively insecure Bluetooth or infra red if you have the patience and then there is the up and coming (?) NFC. Where would I put my money? Well for the moment I think ARM has a lot more mileage in this end of the market. Gemalto has a long history in mobile phones or the SIM card at least but is NFC worth all the effort?

Mobile Payment on the Move

By Laurent Bailly, Telecom and Media Director, Atos Worldline in France and Bernard Van der Lande, Head of e/mPayment, Atos Worldline in Belgium

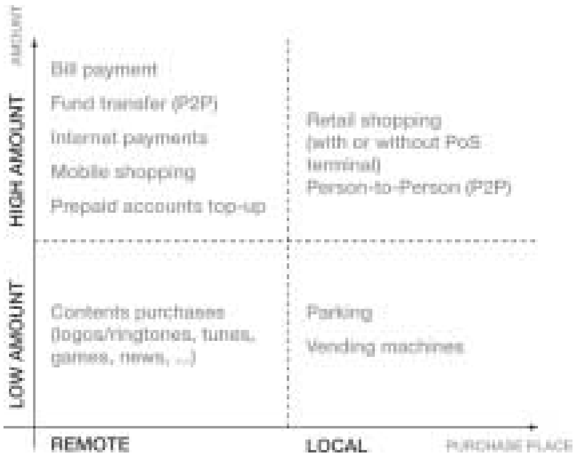
Laurent Bailly

Despite misfiring for a number of years, mobile payment (m-payment) is finally set to come in to its own. But after so many false starts, how can we be so? After all, we've already witnessed a number of high-profile initiatives - remember DualSlot handsets and Simpay? - fail to get out of the starting blocks. The market has seen a number of changes that have made the mobile payment proposition more attractive and more realistic than ever before.

Bernard Van der Lande

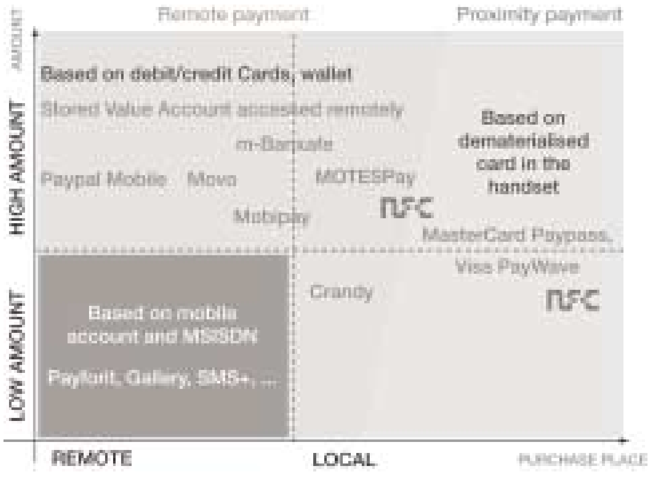
Firstly, contactless technology is now a reality and is already used in millions of cards worldwide, such as debit and credit cards, and for underground tickets, such as Oyster Cards in London. Making it available on mobile phones is the obvious next step. Secondly, there have been a significant number of regulatory changes, such as the introduction of the Electronic Money Issuer license in 2000 and the Payment Institution (PI) status in 2007.

These changes have eased restrictions on payment operators and have created a fertile and innovative market, prompting the emergence of new entrants in the m-payment area i.e. those other than banks. These new players will be able to offer such services as cash deposits and withdrawals; direct debits; credit transfers; payments initiated by a card or a similar device; credit (for a maximum 12 month period). Thirdly, network capacities and device capabilities have increased substantially; and the adoption rate of mobile phones has reached almost saturation point in Europe. Today, mobile phones are an integral part of daily life for many people and have joined keys and wallets as 'must have' items before leaving the home. With such a lucrative market attracting so many players, where will they all fit in the m-payment value chain?



M-payment can be segmented in to categories and into a combination of micro/macro-payment and remote/local m-payment scenarios, each representing different opportunities for the different players involved.

We differentiate between remote and proximity payments:


Remote payment
Proximity payment
AMOUNT
HIGH AMOUNT
LOW AMOUNT
Based on debit/credit Cards, wallet
Stored Value Account accessed remotely
m-Banquate
Paypal Mobile
Movo
MOTESPay
Mobipay
NFC
Based on dematerialised card in the handset
MasterCard Paypass, Visa PayWave
NFC
Crandy
Based on mobile account and MSISDN
Payforit, Gallery, SMS+, ...
REMOTE
LOCAL
PURCHASE PLACE

Mobile Remote Payment - Mobile remote payment covers payments that take place online, in which the mobile phone is used as a device to authenticate personal information stored remotely. Remote payment solutions can also be used for transactions that take place locally, such as face-to-face and vending machine transactions. Mobile remote payment can be made either at the micro or macro level; each level requires very different technology and levels of security. Micro-payment (payments worth 10 euros or less) for goods and services, such as ring tones and games, is already a mature market in most European countries. They are provided by mobile operators, with payment being made mostly via premium SMS/WAP using mobile operators' billing infrastructures. Micro-payments have proved to be an extremely lucrative source of revenue.

New payment schemes have appeared either proprietary to one mobile operator or are the result of collaboration between mobile operators. One of them is UK-based Payforit, which allows mobile phone users to purchase low-value goods and services from the internet and charge them to their mobile phone. Under the Payforit scheme, mobile internet billing requests are no longer handled by individual mobile service providers, but by a trusted party, known as an Accredited Payment Intermediary. Beyond mobile content and services, micro payment initiatives have appeared across Europe allowing subscribers to pay for parking at vending machines and for bus rides. In the future, competition in the Internet and mobile content micro-payment space will increase. The introduction of new payment solutions could bypass mobile operators' 'billing-on-behalf-of' systems, and instead will be based on stored-value accounts, with lower fees for merchants.

For remote macro payments, the mobile is linked to a payment card (credit/debit card) or an account (bank account and/or store account) via an activation/enrolment process and is used afterwards as an authenticator of remotely-stored information. There are various opportunities for mobile remote macro payments, such as topping-up a mobile pre-paid account; mobile shopping; mobile banking; international money transfer; mobile point of sale (mPOS); and person-to-person (P2P) payment.

Different initiatives have already been launched in remote macro-payment areas, either by Internet payment providers, such as Paypal Mobile or Google Checkout Mobile; or by new electronic money issuers such as Crandy, Luup, and Tunz. Others have been initiated by banks, such as Paybox in Germany and Austria and MOVO (Caisse d'Epargne) in France; and some have been collaborations between banks and mobile operators - Mobipay in Spain and mBanxafe in Belgium, for example. Mobile operators can build a strong case for remote mobile payment by proposing a single, secure and convenient solution, generating traffic both at the point of purchase and at the point of payment authentication. Remote mobile payments could also offer significantly lower pre-pay top-up costs compared with traditional top-up scratch cards and e-vouchers.

Collaboration with at least one financial institution would enhance the business case for mobile operators, as they have little experience in risk management for high-value payments and would boost consumer confidence. Banks can also cash in on the new generation of electronic transactions, as they are based on their traditional payment methods, on which they will be able to claim acquisition and interchange fees. Additionally, mobile devices could offer them a new, convenient and secure banking channel. To ensure the success of mobile remote payment, any application must be secure and also convenient for the user, which means the registration and activation process must be free and simple. Collaboration between mobile operators and financial institutions is also crucial, as both would be able to re-use their existing infrastructures and help share the significant cost of developing new payment solutions. Finally, local-level standardisation is required, whereby the stakeholders adopt the same technical platform at national level or define a common 'standard technical interface.

Mobile Proximity Payment - The second key area of mobile payment is mobile proximity payments. Proximity payments generally refers to contactless payments, in which the payment credential is stored in the mobile and is exchanged over the air, based on near field communication (NFC) technology, with a dedicated and compatible payment terminal. In other words, the mobile acts as a contactless payment card. NFC is an easy-to-use, short-range wireless technology. It is quickly becoming the technology of choice for operators, handset manufacturers, credit card companies and public transport operators around the world for contactless transactions, including secure payment and ticketing, because of its strong consumer appeal and ease-of use. There are millions of contactless cards in circulation all around the globe, including credit cards, access devices, travel and event tickets.

In the payment sector, Visa, MasterCard and Amex have already established their own contactless protocols - PayWave, PayPass and ExpressPay respectively. In Europe, the pilot phase for mobile contactless payments began in 2006 with payment, transport and loyalty applications. Recent applications include MOTESpay, launched in 2007, which is an NFC payment pilot that involves French banks Caisse d'Epargne, Banques Populaires and Arkéa; and P□gasus, another 2007 joint initiative between the French mobile operators, Visa, MasterCard and major banks to experiment with universal contactless payment

The NFC eco-system is extremely complex, with a lot of different stakeholders aiming to take their share of the revenue. For mobile operators, mobile contactless payment allows them to add value to their commercial offering with new services that will, potentially, increase their Average Revenue Per User (ARPU). New revenue could come from other sources, such as transaction fees, renting space on the handset or SIM card, data traffic (mainly from over-the-air downloads), and managing service providers' applications. For banks, mobile contactless payment will reduce cash handling (for micro-payment) and plastic card issuing costs (for macro-payment). But it also offers the opportunity to offer more interactive services, linked to online banking services, like providing credit at the point of purchase. For retailers, contactless payment helps to speed up transaction time as well as generating more transactions, especially for micro-payments, and also reduces cash handling. For transport operators, contactless cards could be used across their networks. Also, event organisers, museums and cinemas that sell tickets via the Internet or over a mobile network can now send tickets directly to the purchaser via their NFC-enabled handset, making the purchasing of tickets much faster and possible from any location.

To achieve this, key success factors are:

❒ Collaboration between stakeholders to define a clear business model that maximises for all parties the return on investment, which is required to provide NFC-enabled handsets and readers, especially in Europe where the payment infrastructure has recently migrated to EMV.

❒ Trust between stakeholders to ensure security and quality of service. Both financial and telecom companies are encouraging the creation of a "trusted third party" role, which would provide a single point of contact for all service providers wanting to put their applications onto NFC phones.

❒ Standardisation to enable mass-market uptake. There are still some issues to be solved, such as the definition of the contactless EMV protocol and where to store the application in the handset (in the SIM card or in a separate secure element).

❒ Customer experience - whatever the business model, the resulting solution should improve the existing payment methods, or at least equal them.

This article has spoken about remote and proximity payments as separate entities and opportunities; however, synergies between the two can bring additional opportunities. A typical scenario is the smart poster: the mobile phone reads the NFC tag located on a poster for a concert, and then redirects to a WAP site on which the user can buy a ticket for the concert. A dematerialised eTicket is then stored securely in the user's handset. The final step is for the user to wave the mobile phone in front the NFC-enabled concert gate, which will then grant access to the arena and allows the user to by-pass queues.

In summary, we are entering a pivotal moment in the history of m-payment, which is set to take off thanks to mobile penetration, technical maturity and regulation breaktroughs. The technology for mobile remote payment is already mature, and can be used for many applications, such as pre-paid top-up, electronic bill payment, mobile point of sale terminal (mPOS), international fund transfer and for making internet payments. Internet giants are exploring remote payment opportunities, and with Paypal and Google Checkout arriving on mobile phones, they represent a common threat to mobile operators and banks.

The long-term future,of mobile payment will likely belong to contactless technology. NFC contactless payment is a huge entity, as it addresses both the cash and cards payment markets. However, it will take some years before it becomes a reality - standardisation and business model issues need to be resolved. This can only be achieved through strong collaboration between stakeholders, including mobile operators, banks and retailers. Without this collaboration, rival solutions and technologies could proliferate, which would inhibit the adoption of mobile contactless payment solutions.

miSense - Biometrics Are "Key" for Airline Passengers

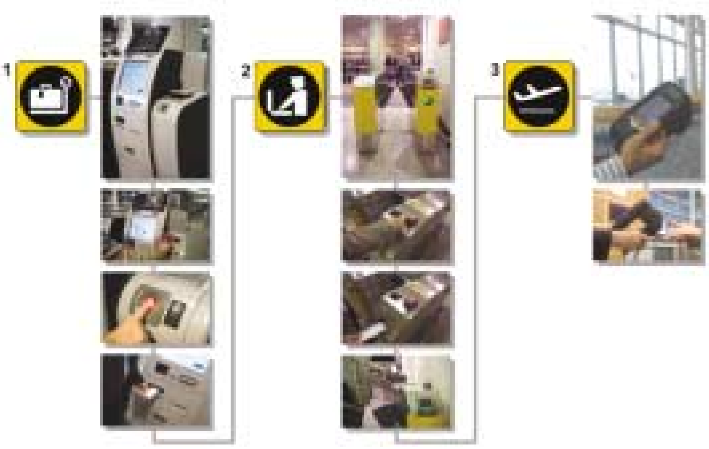
By Jason Smith, Editor, Smart Card News Ltd

Jason Smith

During a 16-week trial held at London Heathrow Airport, 3,166 travellers participated in what is widely regarded as one of the most comprehensive trials of biometrically enabled access control to be conducted in an operational transport environment. miSense was developed and delivered by a consortium of organisations - BAA, Border & Immigration Agency, five technology partners (Accenture, IER, Raytheon, Sagem and SITA) and two airlines (Cathay Pacific and Emirates). Each organisation self funded their elements of the trial including time, materials and equipment. The trial stands as a tribute to a deep-rooted spirit of innovative collaboration between nine organisations.

The aim of miSense and the consortium was to better understand how the use of biometric technology might help simplify traveller journeys while maintaining high standards of security and identity miSense was also designed to test the principles contained within the Ideal Process Flow (IPF) developed through IATA's Simplifying Passenger Travel (SPT) Programme. One of the underpinning principles of the Ideal Process Flow is to collect and verify traveller identity information as early as possible and by using the same information throughout the remainder of the airport journey, facilitate easier air travel while maintaining high standards of security and identity management. Several journey stages are linked together to create a single travel experience including check-in, entry to security screening, aircraft boarding and automated self-service border clearance. Through collaboration with the Immigration Authorities in both Hong Kong and Dubai, options for an interoperable self-service border clearance service were also explored.

The trial, which ran until the end of January 2007, consisted of three linked services that where developed to test different aspects of the Ideal Process Flow system. Passengers travelling on selected Cathay Pacific and Emirates flights were invited to participate in the first part of the miSense trial at check-in by scanning their passport and right index fingerprint into a specially designed miSense self-service kiosk. This information then became the passengers secure 'virtual key' that allowed them swift access through security control and aircraft boarding using their fingerprint. This stage operated at Heathrow Airport's Terminal 3 (T3) between October 2006 and February 2007 and 2,159 participants where involved.



The second part of the trial, miSense plus, also used biometric information, to trial an international registered traveller programme and fast path on departures and arrival immigration in the UK. Anyone flying out of T3 could enroll in miSense plus as long as they were a European Economic Area National, held a passport which was valid for at least six months, be aged 18 or over and satisfy UK Government background checks. Passengers had 13 biometrics captures taken of them - 10 fingerprints, 2 irises and 1 facial image. Participants then received an RFID Smart Card that allowed them to use the self-service border clearance gates for fast track immigration clearance when arriving and departing. This stage ran between November 2006 and February 2007 and involved 1,007 participants.

The third part of the trial, miSense all clear, involved the testing of interactive Advance Passenger Information (iAPI) for the UK authorities. iAPI is the capability of automatically providing border control agencies with intelligence prior to passengers boarding a plane.

As each passenger checks-in, this system enables real-time interaction between airline and government systems. miSense all clear provided an opportunity for Government to explore the practicalities of processing data and to generate in real-time Authority to Carry (ATC) responses as a result of background checks. This stage ran between February 2007 and March 2007 and 3,097 travellers where recorded. IAPI is already well established in countries such as Australia, Bahrain, Kuwait and New Zealand, where it is used to issue the "authority to carry" at the point of check-in.

The trail project was officially opened by the UK Minister of State for Immigration, Liam Byrne MP, and Heathrow CEO, Tony Douglas. Having enrolled in miSense himself, Liam Byrne MP said: "Biometric ID systems are fundamental to securing our borders in a more mobile age. They are crucial to our plans for counting everyone in and out of the country. This proof of concept shows just how well the technology can work."

Overall, passenger feedback on the trial was positive. Travellers where impressed with the new system and found it straightforward to use and generally it offers the chance to speed up the airport process. Face to face research revealed that travellers valued the opportunity to reduce waiting times at security.

Each miSense plus participant was invited to complete an online questionnaire designed to record service performance and user acceptance. Of 982 email requests distributed, 345 (36%) responses were received. The research showed that; 87% of travellers found the enrolment process easy, 62% of travellers found the self-service gates easy to use, 66% said that it took them less than 15 seconds to use the gates, 72% said that the most important benefit that miSense provided was faster journey times. Overall 81% believed the service was excellent and 89% said they would recommend the service to a fellow traveller.

The use of the RFID Smart Card was also considered to be a success. Travellers preferred the ability to control access to their data ("if I don't want to share my data I won’t show you my card") and the use of such a device may facilitate greater international collaboration - especially where transmitting biometric data between countries is prohibited.

The self-service border clearance gate was used 307 times by miSense plus participants with a recorded average engagement time of 17 seconds and in some cases as little as 12 seconds. Of those miSense plus participants who used the dedicated immigration lane on arrival at Hong Kong, 71% said the use of miSense plus shortened their journey time. In a report on the miSense trial, Liam Byrne summed up the trial by saying; "To strengthen our borders in the years to come we need Government, international partnership and industry to work together. New technology, particularly biometrics, and new approaches to managing risk and intelligence will play a fundamental part of making it easier for good travellers to travel - but bad for those we are concerned about. The miSense trial demonstrated an excellent example of how the Border & Immigration Agency can play its part in achieving these goals. I am very proud of the UK Regional Group's accomplishment and I look forward to taking what we have learnt from the trial to help in the future."

Robert Gibbs, Senior Executive, UK Government Practice, Accenture said; "Close collaboration between organisations like Accenture, BAA, Emirates, and the UK Immigration Service is vital in enabling fast and convenient passage through immigration for travellers. As we work together to develop new tools for more accurate traveller identification, this close collaboration will be key. miSense draws on information gathered into the business application of biometrics technology to help build faster and more accurate passenger identification systems, improving border security and overall airport operations. miSense also will help inform future initiatives in e-Passports, e-Visas and other identity management programmes."

This miSense trial has provided an insight into how iAPI could be implemented in the UK. The trial has also shown that the advancement of technology has meant that biometric information can now be captured quickly, unobtrusively and as observed during the trial, with a high degree of traveller acceptance. miSense has demonstrated that biometric technology is now developed and sophisticated enough to begin to be integrated into everyday travel journeys.