Smart Card News

Smart Cards, SIM, Biometrics, NFC and RFID

www.smartcard.co.uk

08 • New Meal Ticket Card for Americans

09 • G&D SIM Cards for Mobile Payments

05 • TanGO Platform for Calypso Cards

10 • Contactless Paper Tickets: When Mass Transit Drives Other Markets

This Month's Lead Story

Greater Security for the UK Border

In This Issue

Regular Features

World News In Brief

Featured Articles

www.smartcard.co.uk

Dear Subscribers,

April has been an unusually warm month in the UK with lots of sun and gentle breezes, all the stuff that holidays are made of. So one can't help think about travel and from our point of view the role of Smart Cards.

Well it's been a bad month from a number of points of view. First of all we have heard more about the card fraud perpetrated at petrol stations. A service area at Weedon on the A5 in Northamptonshire was raided after several local people complained of credit card irregularities. One victim said £350 was taken from her account from a cash point in China.

Others have reported losing £1200 after cards were skimmed using a garage in Great Yarmouth where the money was taken using banks in Thailand. These are just a few examples, there are many more. What happens of course is confidence in the system, people become nervous of using their credit cards particularly in garages. The trouble is that it is not a problem with Chip & PIN as such but the use of the fallback magnetic stripe.

Concessionary travel may escape the notice of the younger smart card enthusiasts but it's actually quite a big user of Smart Cards, Scotland has the Mifare 4K for its National concession travel card scheme with somewhere over 800 thousand cards issued under the ITSO scheme. Unfortunately most are still used in a show and go mode of operation which brings me round to England's National concessionary travel card due to be operational in 2008. Will it or won't it – be a Smart Card that is?

As a potential consumer (well I don't feel I'm that old yet) I don't think I would care whether it's a Smart Card or not, there is no business case for me. From the point of view of the travel operators and the Government it has to be cost savings or in the case of the former increased revenue. The trouble is they can't both win and a Smart Card infrastructure represents a very visible cost. If I were a betting girl.........

Patsy

Greater Security for the UK Border

Through the introduction of a US-style visa waiver programme, the UK Government plans to create a strengthened border control to screen people it wants to enter the UK and to deny entry to those it does not, even before they get here. This border builds on the success of exporting cross channel border controls to France and Belgium, which has resulted in an 88% fall in the number of clandestine entrants detected in Kent in 2006 compared to the same period in 2002. In a UK Government publication entilted 'Securing the UK Border' the Government sets out how the UK will overhaul visitor visas - including consulting on tougher sanctions for sponsors of family visas, consulting on requiring English for spouses as well as installing technology at UK ports to record biometrics of non-EEA citizens without visas. It also proposes that bio-metric technology will play a greater role in securing our borders.

By the end of 2007 frontline staff at all major ports will be able to check biometric data in travel documents against the passenger presenting the documents. Currently, visa applicants from 63 countries are required to provide fingerprint and facial biometrics. Toward the end of 2009, the UK hopes to have a national identity card scheme up and running for citizens and residents. The personal information of millions of people will be included in a computer database, along with biometric details such as fingerprints and facial characteristics. At the beginning, the new scheme will be voluntary for UK residents and compulsory for visa applicants to the UK from 2008. Then by 2014 it is planned that it will be compulsory for all people in the UK to own a card. Foreign national residency permits would account for about 3% of all identity cards. Both citizens and immigrants using social services will be required to have a card, which will also help confirm the immigration and visa status of people. Most foreign nationals living in Britain will have to carry a card in order to help fight terrorism and identity fraud. Identity fraud from Income Support and Jobseekers Allowance funds is estimated to currently be approximately £50 million a year. Additionally, earlier this year the government admitted that it intends for all fingerprints collected for ID cards to be cross-checked against prints collected from approximately 900,000 unsolved crimes.

More people will also face checks before entering the UK to further tighten the UK's borders, said Immigration Minister Liam Byrne. "It is essential that we have a fair and effective migration system, trusted by the public as a whole and those who rely on it. Secure borders help combat illegal immigration, false asylum claims and clandestine entrants by stopping those people from getting near the UK, yet make it easier for the almost 200 legitimate travellers per minute who cross our borders." he continued "Compulsory ID cards for foreign nationals will be a vital buttress of our defences giving businesses and public services the choice to check whether someone is who they say they are. The days when border control started at the white cliffs of Dover are over. Our immigration control needs to start well before people come anywhere near British shores."

By the end of 2008 half the countries in the world, covering three quarters of the world's population will all need biometric visas with their fingerprints checked against the UK Government database, before travelling to the UK. "Biometric technology is integral to securing our borders so identities can be checked and fixed before people leave for Britain. We have to think beyond the idea of national borders as a line on the map. Even guards every 50 yards around our borders would not tackle false identities. Once people are here, ID cards are the only way of tracking them inside the UK" said UK Prime Minister Tony Blair.

The Government has already had significant success in exporting and tightening Britain's border. Airline Liaison Officers are in place across the world to provide advice and training on UK travel documents. Their work has resulted in 150,000 people without proper documents being prevented from boarding aircrafts to the UK in the last five years alone. Juxtaposed controls in France and Belgium have contributed to a 70% reduction in unfounded asylum applications for the whole of the UK. The £15 million e-Borders pilot, Project Semaphore, has already captured data on 21 million passenger movements and issued over 9,000 alerts to the border agencies. By 2009 the Government will count the majority of passengers in and out of the UK. Border control agencies will be able to access information in advance of travel about the movements of passengers so resources can be targeted towards those who present a threat, while speeding up travel for those who do not.

Smart Cards

£10m Smart Card Tender

West Midlands Passenger Transport Executive (PTE) Centro has issued a prior information notice inviting suppliers to prepare to bid for a £10 million - excluding VAT - contract(s) to supply a Smart Card system for Birmingham and suburbs. Centro requires a suitably qualified company, or companies, to deliver an ITSO, or equivalent, complaint Smart Card scheme to run for an initial period of two years. The project would include supplying card issuing and validating machines, point of sale equipment, back office systems, and the actual Smart Cards.

The winner of the new West Midlands rail franchise will be contracted to introduce Smart Card technology by 2010. Centro/West Midlands PTA chief executive Geoff Inskip said work by MVA Consultancy and Logica CMG suggested the capital cost of setting up an ITSO-compliant Smart Card system would be around £13 million with annual operating costs of £1.26 million. MVA has recommended the PTA directly procures the on-bus ticketing equipment, matching the approach taken by the Scottish Executive. A contract notice inviting suppliers to tender is expected to be published in June this year.

Payment Card Market Monitored

The Smart Payment Association (SPA), that brings together the largest payment Smart Card manufacturers, completed its first internal market monitoring in order to get a better understanding of the actual situation and trends of the payment Smart Cards market. Their key findings revealed:

1) More than 340 million payment Smart Cards shipped in 2006, complying largely with the EMV standard.

2) Dramatic increase of the share of DDA (Dynamic Data Authentication) within EMV cards - which more than doubled - to now represent more than 27% of all EMV cards shipped in Q4 2006.

3) Open platform cards (comprising cards based on Java Card and Multos) now account for almost 10% of the global shipments.

4) 12% of the cards shipped have their data storage capability enabled at issuance for value-added applications, such as: loyalty, access control & ticketing. In order to standardise data storage, the SPA has released a joint industry specification addressing cross vendor interoperability for contactless datastorage.

"The results of the first global payment cards market monitoring show a clear trend: the move of financial institutions towards higher value-added and more secure cards", said Jerome Ajdenbaum, President of the Smart Payment Association. "The dramatic acceleration of the conversion of Static Data Authentication to more secure Dynamic Data Authentication EMV cards and the growing share of cards enabled with data storage capability are the most concrete signs of this trend".

Desjardins Smart Card for St-Jérôme

Starting in the spring of 2008, members of Desjardins caisses in the city of Saint-Jérôme, north of Montréal, Canada, will be the first to be able to carry out debit and credit transactions using the Desjardins Smart Card. "We are especially proud to announce the launch of the Desjardins Smart Card. A major step has been completed now that we have chosen the city that will serve as the launching pad for this innovative technology for electronic payments and banking transactions," declared Desjardins Group President and CEO, Mr. Alban D'Amours. Desjardins teams are currently working on modifying ATMs and payment terminals in various businesses in Saint-Jérôme.

e-Passport Production in Macedonia

This month, Macedonia will become one of the first non-EU countries to equip its population with highly secure travel documents. A total of 45 data capturing and entry stations in 30 registration offices located throughout the country will be accepting applications from nationals for electronic passports. Besides these 45 permanent stations for entering citizens' photographs, digitalised signatures, and biometric data, five mobile data entry stations will be supplied by Giesecke & Devrient (G&D). Like the fixed stations, they will be equipped with a laptop, a camera, a signature pad, and a fingerprint sensor.

A total of 1.5 million passports should be issued by the end of 2009. The Macedonian e-passport comes equipped with a microprocessor chip and security features, which makes it fully compliant with the guidelines laid down by ICAO and the EU. Since the Republic of Macedonia selected a combined personalization system, it will be able to produce not only electronic passports, but also personal identity documents and driver's licenses on the same equipment. The system comes with two identical personalisation lines that can produce a total of 2,000 passports, 2,400 ID cards, and 600 driver's licenses a day.

4
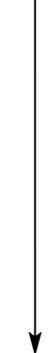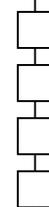
Australia Puts Smart Card Bill on Hold

The Australian Federal Government is heading back to the drawing board after a senate committee found its proposed new Smart Card was likely to become an identity card. The access card was intended to replace the Medicare card and other benefits cards, streamlining access to a wide range of government health and welfare services. The government had explicitly ruled out its use as a national ID card amid widespread concerns that was what it would become.

But in a report the standing committee on finance and public administration said the card was likely to become in effect an identity card, despite measures aimed at limiting its use. "The committee considers that in all probability these provisions will be ignored in practice and will become dead letter law," it said. What's now likely is that the two bills implementing the Smart Card will now be rolled into one.

Dutch Roll-Out New Defence Pass

Bell ID has announced that, in cooperation with the prime contractors Siemens IT Solutions and Services and Getronics PinkRoccade, it licensed its latest ANDiS platform to the Dutch Ministry of Defence for the implementation of a Smart Card-based ID card. The new ID card, known as the 'Defensiepas' ('Defence Pass'), will be replacing the existing ID card within a year and will act as a secure means of identification for all the Ministry's smartcard user groups (400,000 cardholders in total). The card will be used to gain physical access to buildings and rooms as well as logical access to IT systems. PKI functionality will provide the means to authenticate electronic documents and e-mails with digital signatures. Siemens and Getronics PinkRoccade will be priming the project. Bell ID will be implementing its Card & Application Management System (CAMS) and Key Management System (KMS).

e-Driving Licences for Moroccans

A consortium made up of Sagem Défense Sécurité, m2m Group and Attijari capital risque has been awarded the national program of electronic driving and vehicle registration licenses in Morocco. This large scale dematerialisation project is set up to issue over 13 million cards. By opting for multiapplicative contactless Smart Cards, the Moroccan Ministry for Equipment and Transport (MET) aims to develop a strong activity of value added services by leveraging the functional openings offered by this advanced multiapplicative program.

Applications such as "point-record driving licence", tracking driving offences, highway fees payment will be developed around the driving licence card. The consortium has created a Moroccan liability concessionary company called ASSIAQA CARD, 51% held by the Moroccan shareholders and 49% by Sagem Défense Sécurité. ASSIAQA CARD is charged to manage the implementation, deployment, financing and maintenance of the new management system of electronic driving licences and vehicles registration cards. The contactless Smart Cards will be supplied by Sagem Défense Sécurité and personalised locally in Morocco within processes that ensure the highest levels of security. The delivery of the new cards will begin within six months.

TanGO Platform for Calypso Cards

ASK, a provider of Calypso dual interface and contactless Smart Cards for the transportation sector, has announced they have signed a license agreement to benefit from ASK TanGO Operating System. "This new strategy strengthens transport operators decision to implement Calypso based fare collection systems. They are now offered multi-source Smart Card manufacturers. TanGO can clone such legacy cards as GTML, GTML2 and CD97 to carry on existing systems as well as provide new features and interoperability, says Patrick Sure, Transport and banking Business Line Manager."

Oberthur Finalises I'M Acquisition

Oberthur Card Systems has announced that the acquisition of I'M Technologies has been finalised for a purchase price of S$34 million (around 17 million euros). As part of the transaction, the key managers of I'M Technologies have joined Oberthur Card Systems. The two companies have identified significant synergies which should have a net impact on the operating margin in the Telecom segment and further reinforce their positions in the Asian market.

New Chemist Cards to be Tested

Another milestone has been reached in what is currently the world's biggest IT project, i.e. the establishment of a new telematics infrastructure for the introduction of the electronic health card (eGK) and the medical profession ID card (HBA) in Germany. On behalf of Werbe- und Vertriebsgesellschaft der Apotheker (WuV), D-Trust GmbH, a wholly owned subsidiary of Bundesdruckerei, is supplying all chemists in a test region with a chemist card. These cards are produced by Sagem Orga GmbH.

Starting in April of this year, the task of setting up the new telematics infrastructure in Germany's health care industry will enter into another important phase of testing. The aim of the field tests currently underway is to try out step by step the complex interaction between the around 190,000 licensed doctors, 2,200 clinics, 21,000 chemists, almost 270 health insurance companies and around 80 million health insurance members, who are to be integrated into the telematics infrastructure at a later point in time, and to optimise this in the best possible manner until the electronic health card and the medical profession ID card are introduced nationwide. The roll-out of the test chemist cards is scheduled for May 2007.

Accreditations for Gemalto in S.Africa

Gemalto has announced the successful completion of American Express, MasterCard and Visa certifications of its Johannesburg-based banking facility for the personalisation of magnetic-stripe and EMV Smart Cards. It is intended to locally support the roll-out of EMV banking cards across South Africa, scheduled to start in Q3 this year. Gemalto has already secured an exclusive contract with a major South African bank for EMV personalisation. The Gemalto Johannesburg-based facility has been personalising SIM cards for seven years, with a current capacity of 10 million units per year. It is now expanding into personalisation of banking cards to boost its local activities in the financial sector.

HID Acquires IE

HID Global has acquired Integrated Engineering (IE), the Amsterdam-based contactless Smart Card reader manufacturer. Integrated Engineering is known for developing high quality contactless Smart Card solutions including MIFARE/DESFire products and solutions for security, identification, e-Passport and e-Payment applications.

e-ID for German Federal Authorities

Bundesdruckerei GmbH are to produce an electronic office ID card for Germany's federal authorities. Starting in the summer of this year, this card shall be gradually introduced for the Federal Armed Forces. This may be followed by other federal authorities. Bundesdruckerei developed the office ID card together with the Federal Criminal Police Office (BKA) and the Federal Office for Information Security (BSI). The hybrid card features both a contactless memory chip as well as a contact processor chip.

EasyFuel Solution for North America

On Track Innovations (OTI) has received orders from an energy company in North America for OTI's EasyFuel pay-at-the-pump contactless payment solution. The initial plan is to rollout 130 gas stations with a pay-at-the-pump infrastructure supporting contactless payments programs from major financial institutions, such as MasterCard PayPass including EMV M/Chip, Visa contactless program, Express-Pay from American Express and Discover Zip as well as loyalty programs and third party applications. Initial installations are expected in the second half of this year.

Unisys to Deploy eToken Smart Cards

Unisys Corporation is to deploy more than 28,000 Aladdin eToken Smart Cards to provide employees with integrated physical/data access. This roll-out is later scheduled for eventual deployment at 300 of Unisys' worldwide facilities.

Sagem Orga Open Two New Offices

Sagem Orga has expanded into Southern and Eastern Europe with the opening of new offices in Madrid and in Vienna. Spain is one of the key countries for Sagem Orga in which it intends to develop a strong customer base. After being present already in Portugal, the new office in Spain will complement Sagem Orga's position in the Iberian Telecommunications market.

VA Smart Cards Get HSPD-12 Update

The US Department of Veterans Affairs will begin expanding its interoperable smart identification card pilot in June under Homeland Security Presidential Directive-12 to some of its more than 225 sites. At the same time, VA will stop issuing transition cards - those purchased before the HSPD-12 mandate - and begin handing out cards that meet the National Institute of Standards and Technology's Federal Information Processing Standard 201, said Brian Epley, VA's Personal Identity Verification program manager.

US Issues MULTOS FIPS 140-2

The MULTOS Consortium has announced the entry of MULTOS into the US Government market with the Hitachi dual-interface MULTOS Smart Card with StepNexus PIV Application. Hitachi is the first MULTOS implementer to receive certification for FIPS 140-2 from the US Government.
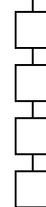
Turkcell Selects Gemalto

Gemalto has announced that Turkcell, Turkey's leading mobile operator , has selected its SIM-based identification solution to implement a large-scale mobile signature program. The program is based on qualified digital certificates by E-Guven, a Turkish Certificate Authority. Digital certificates are created under Turkish Digital Signature Law that is also in accordance with EU's Digital Signature Directive. The Gemalto solution will allow Turkcell subscribers to securely access services that require strong authentication, such as internet banking or e-government applications, using their mobile phone to generate a legally binding electronic signature.

Infineon Chip for Turkish "AKIS"

Infineon Technologies AG has announced that the National Institute for Electronics & Cryptology of Turkey (Tubitak Uekae) has selected Infineon security chips as the hardware basis to develop a Smart Card operating system. Tubitak Uekae developed their Smart Card operating system coined "AKIS" by applying the Infineon crypto-controller SLE 66CX680PE. AKIS was mainly designed for use in applications focusing on eGovernment and PKI (Public Key Infrastructure) Smart Cards. The National Institute Tubitak Uekae is responsible for developing, checking, certifying and implementing Smart Card based security services in Turkey, which currently has an average population of about 90 million citizens.

New SIM Card Spec for NFC Phones

Vodafone and Giesecke & Devrient (G&D) are teaming up to develop a secure storage element for NFC-enabled mobile phones. This element, intended for trusted applications in NFC mobile devices, is the SIM card, with Vodafone and G&D driving the necessary standardisation forward. NFC is a new, wireless-based technology that enables contactless transmission of data between two NFC devices over short distances (i.e., a few centimeters). Vodafone and G&D will continue developing the specification before making it available to a wider audience in the middle of the year.

DoCoMo Recalls Defective Cards

NTT DoCoMo has recalled Smart Cards fitted in 240,000 of its mobile phones because they could malfunction when used abroad, making it impossible for users to talk or access the i-mode Internet service.

DoCoMo are replacing the cards with new ones free of charge to enable overseas calls and will ask its foreign partners, which offer Internet access to DoCoMo phones users travelling abroad, to take the necessary steps to prevent any trouble, Japan's largest mobile phone carrier said.

Mobiles Become Payment Tools

Visa USA plan to push the concept of turning the mobile phone into a credit or debit card. During a keynote speech at the CTIA Wireless trade show Visa's President and Chief Executive John Philip Coghlan discussed Visa's investment in Ecrio Inc., a privately held software company, as well as in dot-Mobi. Visa's investment in Ecrio will help them develop NFC technology. It will also help develop technology called MoBeam which allows handsets to beam barcodes to laser point-of-sale terminals.

Visa said it hopes the investment into dotMobi will further integrate the mobile commerce and mobile Internet experience. The company is also partnering with Qualcomm Inc. and Kyocera Corp. to create phones that can make payments. Visa is hoping its mobile platform will bring the carriers and the credit card companies together.

Its move comes after AT&T Inc. and banks such as Wachovia Corp. unveiled a partnership to allow customers to pay bills on their handsets. "Given the striking similarities in the paths our two industries have travelled, it is only natural we have arrived at a moment of convergence," Coghlan said in a statement. "In fact, the convergence of payments and mobile communications is not just logical.....it is inevitable."

Biometrics

Biometrics Check Dual Citizenship

Malaysia and Thailand will use the biometric identification system to check on the movement of people with dual citizenship along its common border. Prime Minister Datuk Seri Abdullah Ahmad Badawi said the two countries had already agreed to exchange the name lists of people suspected to be having dual citizenship. "By exchanging the name lists of both sides we will be able to determine how many people actually hold dual citizenship," said Abdullah. He said the use of biometric identification system would considerably help in resolving the issue of dual citizenship.

Traveller Program for Albany Airport

Verified Identity Pass Inc has been picked to run the Registered Traveller Program at Albany International Airport in the US. The company, which does business as Clear Registered Traveller, conducts a security pre-screening of airline travellers and issues them a biometric card that allows them to use a special lane at airport security checkpoints.

The lane speeds up security checks and allows travellers to keep their shoes on when passing through security. Albany International Airport is one of 20 US airports participating in the Transportation Security Administration's registered traveller test program.

Biometrics for Canadian Airports

Security is soaring at Canadian airports with the rollout of a dual biometric-based airport identification card program by the Canadian Air Transport Security Authority (CATSA), reportedly the first of its kind in the world. The Restricted Area Identity Card (RAIC) program, implemented across 29 Canadian airports, was an initiative by the Ministry of Transport that began in 2002. To date, some 100,000 Canadian airport workers are enrolled in the RAIC program, which involves a two-factor biometric-based authentication system.

The program uses chip-based Smart Cards, issued to all airport personnel, and biometric readers for fingerprint or iris verification, according to Peter Burden, RAIC program manager at CATSA in Ottawa. CATSA chose fingerprint biometric technology from Bioscrypt Inc. Leveraging the existing chip-based smart cards used by airport employees for identification and authentication, CATSA added on Bioscrypt's fingerprint matching algorithm to provide a two-factor authentication platform for airport employees.

Japanese Push Biometric ATM Cards

Financial institutions throughout Japan, including the Bank of Tokyo-Mitsubishi UFJ, which have adopted biometric cash card technology that uses the pattern of veins in a person's palm for identification purposes, are to allow each others' customers to use their automated teller machines, according to sources.

The Japanese banks have established a council to work on details of the plan, and some members of the group may allow other banks' customers to use their biometric-compliant ATMs as early as May.

Another block of Japanese financial companies, which have adopted a technology that uses the pattern of veins in a person's fingertips, including Sumitomo Mitsui Banking Corp., Mizuho Bank and Japan Post, is also to accept interbank ATM users. The number of people in Japan with biometric cards is estimated to be more than 5 million, and the banks' move is expected to provide additional convenience for customers.

Biometrics for Swiss Passports

Since the end of 2006, Swiss citizens have been able to apply for passports which contain an electronically stored copy of their passport photo identifying the passport holder. Siemens IT Solutions and Services was commissioned to provide the entire solution for recording the biometric data and processing it for the production of the new passports. Each year about 100,000 passports can be issued.

During the pilot project, applicants' biometric data is being recorded and processed in eight Registration Centers in Switzerland and at eight Swiss representations abroad. The centers are equipped with ID readers, cameras and a software solution that is based on the "Siemens Homeland Security Suite" originally developed in the Siemens IT Solutions and Services Biometrics Center in Graz, Austria. The pilot project will run at least until 2009, by which time Switzerland should have reached a final decision about the general introduction of biometric passports.

New Products/Services

New Meal Ticket Card for Americans

ACT's Discovery city card solution continues to show its multi-function technological abilities with VISI-Ticket launching the all new 'MealTicket' available primarily in New Orleans, Las Vegas and New York. The MealTicket will enable users to have breakfast, lunch and dinner for one low price.

National restaurants, local favourites, cafes and cooking schools are all included and cater for all tastes with world cuisines to choose from - whether it's gumbo or beignets in New Orleans, bagels and BBQ in New York, or the best buffet in Las Vegas. Among the participating restaurants are Planet Hollywood and the Bubba Gump Shrimp Company.

World News in Brief

G&D SIM Cards for Mobile Payments

Proximus, BASE, Mobistar, all telecommunications operators in Belgium and Banksys, are now offering their clients a mobile payment service. Thanks to the Mobile banxafe application from Banksys, wireless customers can conveniently use their mobile phones to make payments on a day-to-day basis, for example, when taking deliveries at their front door.

Mobile banxafe is stored on a G&D 128 KB SIM card, which meets the especially strict security requirements and has been officially certified at security level EAL 4+. With Mobile banxafe, all Belgian customers can conduct the same transactions using their mobile phones that they have previously been able to carry out via card terminals located in stores.

New ANDiS4Mobile Solution

Bell ID has launched ANDiS4Mobile, a new solution for complete end-to-end life-cycle management of SIM applications and cryptographic keys based on Global Platform specifications. ANDiS4Mobile loads applications and keys in the most secure manner over the air (OTA) directly onto the SIM of a mobile device.

Upgraded Card Readers for Vista

Omnikey has upgraded its complete line of PC-connected contact Smart Card readers for Vista, the new Microsoft operating system and successor to Windows XP.

Datacard Printers Recieve FIPS 201

Datacard Group has announced at the ISC West conference that they have received approval for its SP75 and CP80 card printers for compliance with the US General Services Administration (GSA) Evaluation Program for certification of the Federal Information Processing Standard (FIPS) 201 card printer specification.

New 3D Face Technology

Bioscrypt Inc has unveiled its new 3D face recognition solutions at the ISC West Conference. With the acquisition of A4Vision, Bioscrypt has now become the first company to offer off-the-shelf finished readers for both finger and 3D face biometrics for use in physical access control.

Keycorp CEO Resigns

Keycorp has announced that its chief executive officer Bruce Thompson has resigned after disclosing that the company was struggling to make a comfortable profit. Mr Thompson announced in the company's half-year results report, that Keycorp has seen a 26% fall in revenue and they have more than doubled their net losses to $4.1 million.

New VP at Inside Contactless

Inside Contactless has appointed Mr. Brent Bowen to its North America business development team, to help address the growing demand for its contactless payment technology. Brent has been named INSIDE's new Vice President of Sales and Business Development for Canada, East Coast and Midwest. He joins INSIDE from Oberthur Card Systems, where he was VP of Financial Sales from 2002 to 2007.

New Managing Director at HID

HID Global has named Anthony Ball as the new Managing Director of HID Global--EMEA region (Europe, Middle East and Africa), reporting to Steve Wagner, Chief Operating Officer.

New Head of SiVenture

NDS has appointed Simon Milford as new head of SiVenture, the NDS-owned consultancy organisation involved in silicon chip security. Simon replaces Graham Higgins who is leaving SiVenture after four years in this role to pursue personal interests.

New Commercial Director at ACT

Applied Card Technologies (ACT) has appointed Nigel Cullum as Commercial Director. Nigel will be responsible for delivering new business into ACT in the areas of retail / hospitality and transport.

New UK Director at Intermac

Intermec, a provider of RFID, mobile computing and bar code technologies, has appointed Ian George as UK managing director. He joins the company from Zebra Technologies, where he was regional director EMEA.

World News in Brief
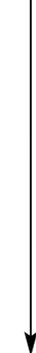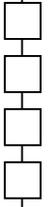
Contactless Paper Tickets: When Mass Transit Drives Other Markets

By Claire Boyer, Communication Manager, ASK

Clair Boyer

C.ticket, contactless paper tickets were launched in 2001 by ASK. They have spread all over the world in Mass Transit AFC systems but their use has gradually been extended to other market segments to enhance the overall contactless-based teleticketing systems offer. Asia is historically the early adopter of contactless technology with Octopuss card in Hong Kong, a multi-application card on the field since September 1997. Nevertheless, contactless paper tickets paved the way to a brand new set of services on the market and the opportunity for public transport operators to implement full contactless AFC infrastructure and address all clients with the same technology, filling the gap between more expensive plastic based Smart Cards ideal for subscribers.

User-friendly, cost effective and environment-friendly, contactless paper tickets have attracted a lot more clients in various sectors and applications whether they be operators, agencies, authorities or travellers and participate to cities sustainable policy development. In a world where quicker is better in terms of traveling and commuting, contactless paper tickets are a great asset to both issuers and end-users. While it decreases drastically the infrastructure costs due to contact based or mag-stripe based systems maintenance, it also cuts down boarding time, cash handling and fraud. Travellers can take the metro, hop in the bus or even ride a bike with the same limited-used ticket on interoperable networks.

Traditional mass transit modes extended to bike rental - In Lyon, France, and other cities including Paris, France capital city, citizens are now offered a modern and convenient transit mode with JCDecaux Cyclocity system. In Lyon, this contactless bike rental is based on ASK contactless paper tickets, offering a new way to travel freely within the city and between different transportation modes. City sightseeing is a new experience whereas going to work does not involve daily traffic jams for those who choose to use the metro, bus, tramway or trolley and pick up a bike to go to the office.

C.ticket buys both entertainment and travel - During the XXth Olympic Games in Torino in February 2006, Torino decided to go full contactless for the overall mass transit and highway toll systems. GTT manages the public transport networks in Torino and its suburbs. Whilst season ticket-holders tend to use new GTT dual interface card, there are 4 different contactless paper tickets to meet the needs of other users: a pass for school children, a multimodal pass, a pass for tourists and tickets to museums and galleries. Four different artworks have been designed to identify each ticket and fare and make it an attractive and new marketing tool. This new system not only helps to combat fraud but also enables the operator to collect data so that they can offer customised fares and value added services to travellers. During China 2008 Olympic Games, contactless paper tickets have also been selected as the best media to make the games a seamless and enjoyable event.

C.ticket for new Mastercard Pay Pass services - Mastercard and ASK joined to develop a Pay Pass contactless paper based card. MasterCard PayPass is intended for environments where speed is at a premium. Transit is a perfect example and contactless based cards are a new asset for a mass transit and banking application. In a subway environment, limited-use, paper-based contactless fare tickets can replace standard mag-stripe fare cards for riders who don't have a PayPass-enabled payment card. This solution enables all riders to tap their way through the turnstile. MasterCard's development arrangement with ASK extends beyond contactless payment cards for transit. The possibilities from paper-based solutions leveraging contactless payments are endless and merging contactless paper tickets with MasterCard' PayPass payment technology provides a cost-effective and user-friendly solution with a brand new product that combines limited use packaging and highly secure Operating System of a microprocessor chip. In sports events banks are often sponsors of clubs, teams or events and contactless paper tickets will no doubt give them a new media to open up extra services to their clients.

Technology Insight

Contactless paper tickets have now extended their use to other market segments than mere public transportation in multimodal, multi-application, interoperable and global environments with a broad portfolio in terms of chips and packaging, C.ticket comes with wired logic or microprocessor chips, in die cut, rolls or fanfold packaging.

Biometric Encryption Vs Biometric Data

By Ann Cavoukian, Information and Privacy Commissioner of Ontario and Alex Stoianov, Ph.D, a biometrics scientist

Biometrics are unique physiological characteristics of an individual, such as a fingerprint or iris scan, that can be used to recognise and verify their identity. As the use of biometric technologies become more widespread, so does the risk to individual privacy. The creation, growth and data linkage of biometric databases may enable new forms of surveillance, profiling, discrimination, and identity theft. While widespread adoption of biometric technologies is on the horizon, it should not come at the cost of personal privacy. Biometric data - fingerprints, DNA, or irises - are unique identifiers, far superior to social insurance numbers in that they are a unique and permanent characteristic of individuals. This makes biometric data a very powerful tool for matching different pieces of information held about individuals across multiple databases. Biometric data can also serve as a password in that it can be used to gain access to physical spaces (restricted areas) or to electronic systems (databases). The security risks of large centralised databases of biometric passwords cannot be underestimated, and unlike passwords, biometric data is permanent - you cannot change your fingerprints or irises if your biometric data is lost or stolen.

Fortunately, biometrics can be deployed in a privacy-enhanced way that minimises the potential for surveillance and abuse, maximises individual control, and ensures full functionality of the systems in which biometrics are used. Building privacy-enhancing technologies into biometric-enabled systems will also create greater confidence in those systems, leading organisations and the public to place greater trust in their use. Our white paper sets out the privacy, security and trust problems of current biometric information systems, and explains how an emerging new technology, called Biometric Encryption, can address those concerns. With Biometric Encryption (BE), instead of storing a sample of one's fingerprint in a database, you can use the fingerprint to encrypt or code some other information, like a PIN or account number, or cryptographic key, and only store the biometrically encrypted code, not the biometric itself. This removes the need for public or private sector organisations to collect and store actual biometric images in their database. Thus, most privacy and security concerns associated with the creation of centralised databases are eliminated.

BE allows an individual's biometric data to be transformed into multiple and varied identifiers for different purposes, so that these identifiers cannot be correlated with one another. Better still, if a biometric identifier is somehow compromised, a completely new one may be easily generated from the same finger or iris of an individual. BE also promises other exciting new possibilities. One such possibility is the creation of anonymous databases. Another possibility is the promise of enabling individuals to use their biometric identification for direct and secure access to their own files. Still another possibility is to place strong and easy-to-use encryption capabilities at the fingertips of millions of individuals, without the need to literally memorise any passwords, PINs, or carry around physical pass-keys. BE technology not only holds the promise of superior privacy and personal control for individuals over their own biometric data, but also stronger information security and greater user confidence and trust in biometric identification systems.

The public, policymakers, information security professionals and technologists everywhere need to examine Biometric Encryption, with its numerous privacy and security advantages, and consider its adoption and deployment as a privacy and security-enhancing alternative. We also wish to inform people that there are more preferable alternatives to the existing privacy-invasive security technologies (zero-sum, win/lose) currently being deployed by government and businesses - positive sum (win/win) alternatives which can deliver both privacy and security. User confidence and trust in the privacy and security assurances of any information system that relies upon biometrics will be critical to the acceptance, use and ultimate success of that system.

Transferring Mobile Solutions From Pilot to Roll-Out

By Oliver Burke, General Manager, Bell ID

Oliver Burke

An increasing number of organisations is discovering the convenience of mobile phones for their business processes. Mobile phones combine a number of very useful attributes which present these devices as a convenient infrastructural component for many businesses. Most people carry a mobile phone; phones have an interactive display; they allow use of PIN for authentication; they are connected to a mobile network; they can communicate 'contactlessly' via Bluetooth, infrared or Near Field Communication (NFC); and (most importantly) in most countries they carry a secure Subscriber Identification Module (SIM), providing the basis for a secure solution.

Many organisations around the world have identified the potential benefits of mobile technology for their business processes and decided to launch trials and pilots in which mobile phones are used as season tickets, loyalty tokens or payment devices. Today nearly every week a new NFC pilot is announced. Most of these pilots are focusing on the application side and user acceptance with regard to these new services. The infrastructure, in the shape of a new NFC-enabled mobile device, is usually distributed manually to the participants of the trials. This makes perfect sense for pilots, but will be inappropriate for scalable roll-outs. To understand industry requirements and learn how existing components need to be adapted to serve the mobile market, Bell ID participated in the deployment of two mobile pilots; the Roda JC - mobile ticketing pilot and the Payzy - OTA Application Distribution pilot.

In a roll-out situation, the mobile subscriber will usually already have a mobile device. Service providers will be faced with a diversified hardware infrastructure. New services and applications must be loaded onto SIMs from existing phones or to a secondary NFC-enabled chip residing in a mobile phone. Mobile subscribers will change their network operators. Network operators will change the memory size of their SIMs. We will see new versions of SIM Operating System (OS) deployed and service providers will adapt their applets to the increased memory size and features supported by the chips. While these issues generally have no impact on pilots, roll-out solutions must be prepared to address these issues. The systems that are addressing these issues are card/SIM and application management solutions.

Over time, millions of NFC mobile devices with the ability to store multiple applications will be in the hands of consumers worldwide. For each of these applications, the ability to install, upgrade and delete an applet in a secure manner will be required. Managing the application portfolio linked to the SIM and the subscriber is a "must" and has been identified by markets that have rolled out large quantities of chips.

Today, most sophisticated chip-based solutions have been deployed with card, application and key management systems, whether in the banking market or in the ID market segment. Put simply, a SIM is also a chip, and therefore has very similar technical requirements. A multi-application Smart Card (SIM) management solution forms the basis of any strategically designed over-the-air (OTA) solution. Considering the potentially large number of subscribers, these solutions must be extremely scalable and robust. Vendors that are considering entering the mobile market are well advised to pay some extra attention towards the scalability aspect. The lack of large roll-outs at this point in time will make it impossible to find SIM management systems with a track record of large mobile implementation. To overcome this issue, vendors such as Bell ID have based their solutions on components that have been proven robust and fast in projects that issued several millions of chips.

Another important goal for the design of a mobile solution is the maximisation of application deployment speed. Bell ID anticipates that one of the success criteria of a real roll-out system will be the capability of deploying new services/applications as quickly as possible.

A sophisticated solution design must consider that during the launch of a new service/application, millions of potential subscribers will download a new applet on their handset at the same time. To reach the highest level of scalability for OTA Post-Issuance Personalisation (PIP), one must search for a company experienced in highly scalable and secure PIP projects. A stand-alone Key Management System allowing connectivity to multiple hardware security modules will, for example, play a crucial role in minimising the time required for cryptographic processes.

With multiple and sometimes competing application providers and services for NFC mobile devices, the need for a neutral platform to enable management, installation, upgrade and deletion of applications over the mobile service provider network is another important issue to consider. Considering such a neutral system will provide a comfortable increase in system flexibility. Implementing "independent" and "neutral" solutions is also crucial when looking at the unpredictable development of business cases, the speed in which technology develops and the price sensitivity of services. Organisations that today choose for independent and "neutral" card/SIM management solutions will be later less dependent on card personalisers, card manufacturers, mobile network operators or hardware device manufacturers. Independent card and application management providers will always try to achieve a maximum level of inter-operability for third-party solutions.
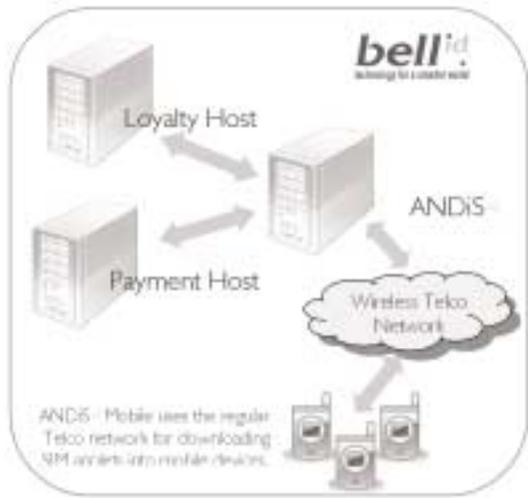
They will make sure their SIM management system works with any of the card manufacturer's SIMs, with any mobile device, any personalisation service, etc. Most importantly, an independent card/SIM and application management solution will certainly make the operating organisation less dependent on the pricing politics of other infrastructure provider. Most trials and pilots so far have demonstrated that the technology available today is ready to be used for scalable roll-outs. We know now that end users appreciate the benefits and convenience of using their own handsets as means of ticketing, cash or loyalty. The technology's availability and the convenience for the end-user seem a good basis to continue and drive ongoing discussions about business cases between network operators, financial institutions and other potential parties.

Events Diary

May 2007

02 - 05	Cardist International Card Technologies Exhibition - *Turkey*
06	Card-Ex - *Egypt - www.epytec.com*
07 - 09	Advanced Identification Systems - *Brussles, Belgium - www.intertechusa/aiseu*
13 - 15	Cards and Payments Middle East - *Dubai - www.worldofcards.biz/2007/cme*
15 - 17	CardTech SecurTech 2007 - *San Francisco, USA - www.ctst.com*
16 - 18	RFID Solutions Expo - *Tokyo, Japan - www.ridex.jp/en/*
22 - 23	Security Document World Conference and Exhibition - *London - www.sciencemediapartners.com*

June 2007

05 - 07	Austalian Smart Card Summit - *Sydney, Australia - www.acevents.com.au/cards2007*
25 - 26	Contactless Cards Conference - *London - www.smi-online.co.uk*
14 - 15	Hi-Tech Financial Crimes & Fraud - *Kuala Lumpur - www.marcusevans.com*

13
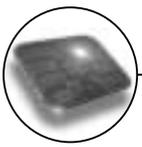
Gemalto Moves Beyond Smart Cards in 2007

By Sally Hudson and Christian A. Christiansen, IDC

Situation Overview - The ability to achieve true digital security across systems, services, geographical boundaries, and wired and wireless transports will result in hitherto unimaginable freedom of movement and capability for countless people worldwide. The technology available today is rapidly transforming the way people go about their everyday lives. This transformation is often referred to as the "digital revolution." The freedom to interact, purchase items, access data and services, or travel anytime or anywhere is now an integral part of what we have and, more important, what we have come to expect. The downside is that both personal and corporate identities are now widely exposed and at greater risk of being compromised, misrepresented, or even stolen. Equally important is users' sense of ease and confidence in adapting to new behaviors when faced with ever-growing numbers of new gadgets, online services, and the digital equivalents of existing habits and things often taken for granted in the physical world.

The need to strongly secure digital interactions while making them easy to use and trusted is essential to the expansion and use of comprehensive, useful solutions in the digital world. IDC believes the delivery of a secure digital device will offer protection for digital identities, assets, and transactions while preserving and expanding individual freedom by providing personalised, convenient, and trusted devices for digital interactions. Digital security can be simply defined as solutions that protect and enhance digital interactions, based on a combination of secure personal devices, software platforms, and services. An important part of this security technology is classified under the identity and access management (IAM) umbrella. Having evolved from traditional 3As security, IAM has expanded to provide the who, what, where, when, and even why of digital interactions. Forecast data shows that, worldwide, IAM market revenue is expected to grow from $3.4 billion in 2006 to more than $5 billion in 2010, exclusive of services. Companies offering lower-cost, open standards.based, and easy-to-integrate IAM solutions should be poised to do well in the coming years. As contactless payment takes off around the world, many countries, especially those within the US Visa Waiver Program, are migrating to electronic passports, and momentum will be steady.

Greater Digital Security = Greater Freedom - The ability to provide truly secure personal devices for individuals can greatly enhance the freedoms we enjoy in our digital interactions by providing confidence that personal and private data will not be compromised or stolen while keeping the user experience one of ease. Consider that secure personal devices allow us to conduct a variety of what we now regard as common everyday activities. These include: 1) Making online purchases; 2) Receiving and sending personal information from wired or wireless devices; 3) Tracking and managing essential healthcare data online. In the future, we anticipate that secure personal devices will continually refine the way we: *1)* Travel globally in a safe and expedient manner; *2)* Access the office from anywhere, anytime, and from any device; *3)* Control and manage different passwords; *4)* Use mobile devices capable of performing multimedia and payment functions; *5)* Include more biometric information. These capabilities need to continue to evolve to offer even simpler and safer user experiences in the future. In this document, we examine Gemalto's contributions and future plans for securely protecting and enhancing digital interactions.

Company Overview - Gemalto is a $2.2 billion entity focused on providing digital security infrastructure and technologies. It is incorporated in the Netherlands and operates from major business hubs such as Austin; Washington, D.C.; and São Paulo in the Americas as well as Beijing, Singapore, and Tokyo in Asia.

For Europe and emerging markets, it operates from Paris, Moscow, and Dubai. Sales offices are located in close to 100 countries. The company, a result of the merger between Gemplus and Axalto in 2006, employs more than 10,000 people from 65 nationalities. Gemalto has 21 production sites, 32 personalisation centers, 9 research and development (R&D) centers, and 102 sales and marketing offices worldwide. Regional breakdowns (as a percentage of Gemalto pro forma 2005 revenue) are as follows: Europe, the Middle East, and Africa (EMEA), 53%; Americas, 27%; and Asia, 20%.
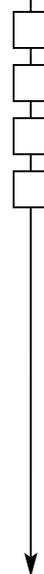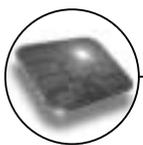
The vendor has expanded beyond its traditional Smart Card roots and is now focused on creating end-to-end solutions for digital security, including the development of software and middleware, design and production of secure personal devices, and various deployment, as well as operated, services. The company dedicates 1,500 employees to research and development; its combined R&D investment was $146 million in 2005. Currently more than 2 billion end users already use a Gemalto product of some kind. Gemalto's key markets are in telecommunications, financial services, enterprise security, Internet content providers, and the public sector and transportation. The company provides a wide range of solutions and services built around its secure personal devices, including strong authentication tokens and badges for network access, EMV and contactless payment cards, and electronic passports and ID documents as well as SIM cards for mobile communications.

Key Vertical Markets for Gemalto

❑ **Telecommunications** - The world leader in SIM card supply, Gemalto provided some 680 million SIM cards in 2005 to more than 400 mobile operators worldwide. The vendor's SIM, RUIM, and USIM cards are designed to run the gamut from enabling basic GSM applications on up to full multimedia and convergent offers for advanced operators. Gemalto is focused on developing complete offers that help operators drive average revenue per user (ARPU), increase customer loyalty, and differentiate their brand. Examples of these solutions relate to contactless mobile payment, mobile TV, multimedia content and service management, and convergence. The vendor also supplies large volumes of prepaid cards for public telephony.

❑ **Financial services and retail** - Gemalto is one of the leading providers globally in EMV chip card migration. It offers several products and services in this area, including innovative contactless payment devices, outstanding card designs, payment terminals, and readers. The comprehensive product portfolio includes software platforms as well as highly secured data management, card personalisation, and deployment services. The company offers a portfolio of solutions that comprises payment system gap analysis and online card design customisation and creates fully integrated and customised card management solutions as needed.

❑ **Enterprise** - Customers in this space include Shell, Chevron, Pfizer, Boeing, and Microsoft. The strong authentication technology solutions provide access control to buildings, email, IT networks, corporate databases, employee services, benefit schemes, secure project databases, and confidentiality on the road, plus other applications and services. Solutions are available in multiple forms, such as corporate badges, USB keys, and one-time password (OTP) tokens compliant with the OATH framework and other standards. Gemalto also provides B2B authentication and digital signatures as well as all components for end-to-end security solutions, including readers and client middleware.

❑ **Internet content providers** - Gemalto provides secure Internet and network transaction solutions for service and content providers, online retailers, and those that deliver online services to the general public, including financial institutions, enterprises, and governments. The client base cuts across many sectors, including government departments, banks, online merchants, and major enterprises. In this area, Gemalto offers a range of authentication solutions, applications and software, managed services, and delivery, plus a wide choice of products, including authentication tokens, OTP on mobile devices, EMVgenerated OTP and associated readers, and other devices.

❑ **Public sector and transport** - With the 2005 acquisition of Setec, a leading provider of electronic passports and ID solutions, Gemalto has one of today's largest reference track records in major epassport and eID card projects, including in France, Denmark, the Czech Republic, Russia, Portugal, Singapore, and the United States; some of the world's biggest ehealth programs; and numerous driving license, vehicle registration, and tachograph projects. The company has extensive technological partnerships, plus a comprehensive road map of operating systems as well as card bodies, security features, and personalisation software. Gemalto today is well positioned to provide turnkey solutions to governments for secure document and enrollment services, with success stories of state-of-the-art electronic ID programs in countries such as Belgium, Finland, and Oman. Gemalto is also a leading provider of contactless tickets and associated systems for mass-transit operators in some of the world's major cities.

Vendor Profile

15
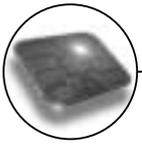
Gemalto and Authentication - The increasing need for combined physical and logical access security across industries has been an area of increasing focus and technology development over the past 12 months. This demand is driven by the need for physical security access to buildings and secure areas as well as the need to meet compliance regulatory requirements and prevent ID fraud.

Recently, the highest-ranking agency within the executive branch of the US Government selected Gemalto to provide card management services, including twof actor authentication technology, in compliance with the Homeland Security Presidential Directive 12 (HSPD-12). Under the terms of the contract, the solution includes deployment and use of personalised smart ID credentials for secure access to information systems and federal buildings. In addition, Gemalto will provide technical advice and integration and delivery services. Intercede, a worldwide technology leader in the field of Smart Card management solutions, is providing the card management system within Gemalto's SafesITe Government solution. Gemalto has long been a major provider of strong authentication devices to the US Government. More than 12 million microprocessor-based smart cards are in use today by several agencies, including the Department of Defense, which has deployed 11 million Common Access Cards (CACs) supplied by the vendor.

IDC believes that the next wave of identity and access management technology is focusing on providing an individual with a single form factor that consolidates multiple authentication requirements into a unified merge identity. Today this is usually a Smart Card or token, and this form factor captures and stores the user's credentials and identifies them across different and diverse access methods into a single, common, and secure digital identity for each individual. This process can then be applied to either physical or logical access methods linked to a corporate back-end system. Many organisations are working toward this common goal to ensure secure, safe access and to facilitate compliance regulations. It will ultimately serve to streamline business processes as well. Beyond the IAM space, Gemalto is also running a number of pilots with innovative technology applications. For example, in conjunction with MasterCard, the French banking group Crédit Mutuel-CIC, and a French mobile network operator, Gemalto is testing contactless payment using handsets that comply with Near Field Communication (NFC) technology. The vendor maintains that the trial is the first of an NFC-based payment application that fully supports the international EMV standard. The application is stored on a Gemalto SIM card in the phones, which is also a first for an NFC payment trial.

Company Strategy - The Gemalto vision of digital security is to make personal digital interactions secure and easy for billions of individuals in an increasingly connected society. The company defines its mission as the delivery of secure personal devices, software, and services, through innovation and collaboration, enabling its clients to offer trusted and convenient digital services to billions of individuals. Today, close to 3 billion microprocessor-based Smart Cards already securely identify individuals and provide them with access to services on networks, addressing the way individuals conduct their daily life. These individuals want and expect more freedom to communicate, travel, or buy anytime and anywhere in a secured way.

Protection of these digital identities, assets, and transactions is vital to individuals as well as to governments and business. The role of the microprocessor card is to function as a trusted, convenient, and really portable computing platform with its own secure operating system and applications. IDC believes that these secure personal devices are a highly suitable form factor for personal identification and related privileges when connected to network-based systems. In pursuing its vision of digital security, Gemalto looks to expand its business beyond just that of conventional Smart Cards. The merger between Gemplus and Axalto led the way in an industry consolidation calling for wider transformation. This puts Gemalto in an advantageous position to benefit from merger synergies and a larger resource pool. The company is increasingly emphasizing end-to-end solutions with a focus on new software development and operated services. This focus spans all of its market segments, and the plan is to map its value more comprehensively with customer needs. One of the key assets, and a significant differentiator, is Gemalto's large global footprint . especially its close relationships with mobile operators and financial service providers worldwide.

Partnerships Are Key - Given the breadth and complexity of the many markets and applications that it serves, Gemalto has also demonstrated that it recognises the importance of partnership networks and strategic alliances. This understanding is particularly crucial in new business developments where bringing complementary know-how from even potential competitors can be critical to achieving success for the customer-specific solution.

16
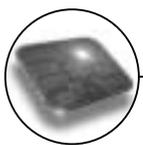
Partnering and collaboration have also proved beneficial to stimulating industrywide innovation breakthrough in many technical markets.In telecommunications, Gemalto emphasizes its Wireless Partner Network, which offers a broad range of mobile applications such as location-based services and call management.

For the public sector, the company recognises the importance of collaborations on a project and local level, collaborating with national printers and systems integrators to offer complete turnkey solutions. Gemalto's commitment to strong partnerships was further demonstrated by its recent agreement with Microsoft. Both companies have announced that Microsoft's Windows Vista operating system will support Gemalto .NET devices right out of the box. This capability will allow enterprises to easily and cost-effectively replace weak username and password-based security with Gemalto Smart Cards and tokens as well as deploy additional digital security applications such as document signature, physical access control, and employee epurse services. Support for Gemalto .NET technology is built directly into Windows Vista, allowing organisations to deploy and use secure personal devices without the requirement for additional software or middleware. The combination of the .NET model and the Smart Card means that the card performs well as a peer computing device; maintains consistent, strong security with applications both on- and off-card; and leads the way to better integrated Smart Card technology.

An important note: The Gemalto .NET Smart Card has been chosen as Microsoft's own worldwide corporate badge for logical and physical access.,In this IAM space, Gemalto also recently partnered with Citrix Systems Inc. and IGEL to deliver highly secure, convenient, and fast access to shared thin-client workstations. Gemalto collaborated with the two companies to create a new thin-client solution that operates in Citrix Systems environments. Employees use Smart Card badges to securely log on and begin or resume work at any IGEL device in seconds. The companies plan to target healthcare and manufacturing organisations.

Future Outlook - Within the IAM space, IDC believes the largest increase in Smart Card adoption will be seen in the banking, government, and healthcare markets throughout 2007/2008. Vendors partnered (or merged) to deliver holistic security solutions in 2006, and Smart Card technology is emerging as a preferred delivery/deployment platform, with several industries demanding two-factor and multifactor authentication. The move to Smart Card adoption will not replace OTP tokens, which are still vital for protecting access to mission-critical, sensitive data. The traditional OTP tokens, USB tokens, and Smart Card devices represent diverse form factors for authentication. This allows governments and corporations to select which form factor is best suited for a particular application, industry, or consumer need.

Further, as the Gemalto/Microsoft partnership illustrates, Smart Cards enabled with secure Web services will provide more control for users when they interact with open networks. The Smart Card then becomes an individual personal Web server interacting with the digital world. As contactless payments, epassports, and the overall migration to a more mobile/wireless world progress, Gemalto's ability to invest in R&D and the company's global expertise should benefit its target markets. The creation of Gemalto is certainly positive for the growth and transition of the Smart Card market. Beyond that, the new organisation has the opportunity to be a force for change and innovation via its new vision of digital security. Gemalto provides the industry with a strong player from both international presence and significant, costeffective technology perspectives. IDC believes that the company is well positioned to address a broader segment of the fast-moving digital security market.

Advice to Gemalto - The identity applications and opportunities available for smart cards, especially in the healthcare, government, and financial industries, should provide a wide avenue of growth for Gemalto products. Further, the merger of Gemplus and Axalto has created a large pool of R&D resources and should also serve to provide greater pricing power and faster time-to-market capabilities - both significant factors in a market where cost per user and ease of distribution are critical variables. Gemalto's proclivity for attracting strong partners bodes well, and IDC anticipates that more significant alliances will be announced in the future. The company, though it has substantial resources, needs to guard against trying to promise too much too soon to the industry as it moves forward in 2007. The same caution should be heeded by all vendors in this space. The Smart Card industry is in the midst of major transition. In the next 12-24 months, over-promising and underdelivering could serve to undermine public confidence in universal digital security as a viable 21st century solution.

17

Rumours From the Front Line

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

Plumbing, that's what it's all about, managing the secure flow of data where the Smart Card or token acts as a security endpoint. Some people call this middleware but plumbing has better connotations of getting your hands dirty. The thing is that as we keep on discussing, the Smart Card itself is now very much a commodity so the money is in the plumbing (or even higher up the chain). So which companies should we be looking at? Gemalto subcontracts the Smart Card management system for its products to Intercede and we might argue that this is the core of the Smart Card plumbing scheme. Intercede Group Plc is not a particularly well known company and their last reported figures for 2006 can be seen below ,

£000s	2006	2005	2004
Turnover	2,142	1,806	1,605
Gross Profit	2,027	1,693	1,339
PBIT	(344)	(386)	(661)

Intercede works with a number of market leading OEM, re-seller and technology partners that supply the MyID technology including: Athena Smartcard Solutions, Gemalto, Oberthur Card Systems, RSA Security, SafeNet, Thales, VeriSign and a variety of systems integrators and other security product and service providers. This is a pretty impressive list and one wonders why their sales aren't higher? Intercede has also been spending time in the USA and in particular with HSPD-12, a Presidential Directive which requires all US Federal Government employees and contractors to have a Smart Card based identity card complying with a new standard of Personal Identity Verification (PIV). So far with Gemalto they have got the next phase of the Transportation Worker Identification Credential (TWIC) program.

In parallel with HSPD-12, the TWIC program requires the issuance of a Smart Card containing biometric information to specified maritime workers at ports and vessels regulated by the US Transportation Security Administration and the US Coast Guard. This has a forecast user base of more than 750,000 individuals. The Intercede Board has reported that it expects revenue for the full year to 31 March 2007 to be no less than 20% higher than last year, one might of hoped (expected) more. The Board also reported that the Group has also been cash generative since 30 September 2006. So who else falls into this plumbing trade? Better known names would be ActivIdentity originally called ActivCard, ACI and Bell ID from a card management point of view and Microexpert, nCipher and CryptoMathic in the security area.

ActivIdentity is an exciting company with latest reported figures below;

$1000s	2006	2005
Revenue	53,375	42,156
Cost of revenue	19,820	19,166
Gross profit	33,555	22,990
Net Profit/loss	(22,472)	(47,926)

Clearly having to work hard but they are well established and deep in the plumbing. ACI is probably at the top end of the chain best known for its inroads in banking with Base24. Its last reported year end figures for 2005 showed total revenue of $313 million with a net profit of $43.2 million. So what can we predict? That there will be consolidation to wrap up these smaller companies, the question is who will move first, the traditional card companies such as Gemalto and Oberthur or the bigger middleware (compared with integrators such as Fujitsu and EDS) companies such as ACI?

Squeak, squeak

18

Topping Up Your Contactless Smart Card On-Board Any Public Transport Vehicle

By Arcontia AB and Vialis Public Transport B.V.

The on-board Add Value Machine (AVM) is an innovative system that allows passengers to conveniently re-load their travel cards on-board any public transport vehicle. Its instant and user-friendly accessibility reduces time otherwise needed to re-load travel cards elsewhere. The trend within new Automatic Fare Collection systems (AFC) is to utilise the use of contactless Smart Cards; either valid as monthly passes or pre-paid travel cards. Within this movement of new technology, it is all about simplifying travelling, making it as convenient and secure as possible.

This it includes the way in which value can be added to the travel card, focusing specifically on passenger operated self service terminals. The on-board Add Value Machine (AVM) is a new way to offer passengers instant opportunity and convenience, to load or re-load their electronic travel card on-board the vehicle in which they are on. On board vehicles today, one is most likely find on-board validators, either at the entrance or at the exit(s) of the vehicle, and thus travellers can flash their contactless travel card in front of the validator to gain access to the ride. The problem, however, arises when there is a need to reload the purse or renew a new month to the travel card. Today, travellers are generally advised to make this transaction in advance at fixed locations in the city. In some cases, this service has been offered by the drivers on-board. Yet, neither of these solutions is of any convenience to the travellers. Not only have many public transport operators begun prohibiting bus drivers to offer this service to travellers, but it can also be observed that bus drivers no longer carry or handle cash due to the risk of robbery.

An on-board AVM is a self-operated terminal, which can for example mounted on-board a bus. When a passenger flashes the travel card in front of the validator and discovers that the travel card needs to be refilled, he or she simply inserts both their credit/debit card and travel card into the AVM. When the PIN code is entered and confirmed, the passenger can easily access their bank account. Unlike an ATM withdrawal, the passenger does not receive any cash; instead he or she transfers a specific amount from his or her bank account to their travel card.

For those travellers who are well out in advance, as well as being frequent users of the web, can via their internet bank transfer a desired amount onto their travel card. This implies that travellers can prior to their trip inform the AFC that he or she wishes to refill their travel card next time they use the AVM. Subsequently, next time the passenger boards i.e. a bus, he or she simply inserts the travel card into the AVM, whereupon the transfer is conducted. The Netherlands is one country that is particularly active with its public transport system and where the first examples of on-board AVM's will be seen in the near future. The five largest Dutch public transport companies have together established Trans Link Systems (TLS) to implement a single payment system for public transport. Together, these five companies constitute 80% of the nation's public transport. TLS has also joined partnership with the carriers and are engaged in certifying that the OV-chipkaart (Dutch travel card) is made available to all people using public transport in the Netherlands. Additionally, the OV-chipkaart can for example be used on-board buses and metros.

Due to the Netherlands' new and well-structured ticketing system in combination with TLS, it can be argued that the country is indeed prepared for a nationwide e-ticketing system, and hence the benefits of on-board AVMs will give passengers more comfort when using public transportation. The new Smart Card payment systems will also improve and simplify passengers' travel experience, as they will no longer have to queue or spend time looking for locations where they can load or reload their e-tickets. Finally, it can be concluded that all passengers, regardless of whether they are casual travellers or commuters, or travelling by train, metro, tram or bus, will benefit greatly from the use of the system, in addition to re-using the automatic Fare Collection Systems easily.