Smart Card News • Smart C

December 2006

Volume 15 • Number 12

Smart Card News

Smart Cards, SIM, Biometrics, NFC and RFID

www.smartcard.co.uk

14 • Smart Health Care - The Next Generation

04 • French Merchants Roll Out V PAY

04 • Sony Doubles Capacity of FeliCa Chip

06 • All-On-One Card for PwC

This Month's Lead Story

NXP and Sony Drive Contactless IC Market

In This Issue

Regular Features

World News In Brief

Featured Articles

www.smartcard.co.uk

Dear Subscribers,

Before you know it we have reached the end of 2006 and a difficult year for many in the industry. As we reported last month the major card companies such as Gemalto, G & D, Oberthur and Sagem Orga are struggling to preserve any sort of margin on their card products. Many are known to be making a loss on every card they sell. The semiconductor manufacturers are being equally squeezed in the value chain, not to the point of making a loss but certainly to the point at which they dream of higher margin products.

The Squeaker this month reports on more gossip in the industry and finds it equally difficult to see how the situation is going to improve in the short term. Its not that we are seeing less cards only that we have reached the bottom of the commodity barrel. By contrast it was refreshing to talk to the drivers of terminal supplier Verifone at their Xmas bash at Madame Tussauds. Back from the ashes and positively thriving it was just a different culture being higher up the value chain and nicely cushioned between the card companies and the system integrators.

If you had to put your finger on it this has probably been the year of the contactless Smart Card. Promoted heavily by Mastercard, Visa and American Express, payments using contactless Smart Cards have arrived and show every sign of taking an even more significant place in the payments market. The attraction of course is not the contactless technology per se but the wave and pay simplicity without signing the docket or entering a PIN. I do wonder if any thing has happened to the security of this payments process and David Everett is starting a new series of technology briefing articles to try and answer these questions.

Being Christmas many of us are probably using the internet as a better way of doing the shopping. I never thought I would say it but there is something rather attractive about shopping on your PC, magically it arrives (usually) soon after and its cheaper than visiting your local shops and even the not so local. So how much of a risk am I taking? Read the articles starting in this months newsletter. Happy Christmas to all our readers and best wishes for a successful new year,

Patsy.

NXP and Sony Drive Contactless IC Market

NXP Semiconductors, formerly Philips Semiconductors, and Sony Corporation have signed a memorandum of understanding (MOU) to establish by mid-year 2007 a joint venture (JV) that will drive global adoption of contactless Smart Card applications in mobile phones. The anticipated JV will plan, develop, produce and market a secure chip that will include both MIFARE and FeliCa operating systems and applications, as well as other contactless card operating systems and applications.

In Tokyo, Sony issued a press statement confirming the joint venture and saying the new company, which will be established in 2007, will focus on developing secure IC chips for use in contactless applications. By combining this secure chip with an NFC chip a universal contactless IC platform can be created for mobile phones. As a result, mobile device manufacturers and service providers around the world will be able to design products and services which are compatible with the different contactless IC protocols and operating systems that are already deployed in different countries. Therefore consumers will be able to enjoy multiple applications such as payment and transport ticketing from various service providers on one device.

Marc de Jong, Executive Vice President and General Manager, NXP Semiconductors said: "This joint venture signals the evolution of interoperable mobile services, regardless of technology platform or geography. Combining MIFARE and FeliCa contactless technologies in a single chip opens a vast array of opportunities for consumers using the technologies, as well as for developers creating new applications for global markets. Soon service providers will be able to roll out great new services to end users on a global scale, ensuring a broad range of offerings to keep customers happy wherever they are."

Mr. Hiromasa Otsuka, Corporate Executive and SVP, Sony Corporation commented: "With FeliCa, Sony has established a contactless IC business model whereby mobile phone wallet services are deployed in multi-application, multi-handset and multi-carrier modes. The new JV will introduce customers around the world to a new lifestyle where simply touching a terminal with a mobile phone gives access to a wide range of services. And it will contribute to Sony's vision of a network consumer electronics entertainment world."

NFC is a combination of contactless identification and interconnection technology that enables wireless short-range communication between mobile devices, consumer electronics, PCs and smart objects. NFC has proven popular in trials around the world. Its interoperability with MIFARE, FeliCa and ISO14443 infrastructures promises to make mobile phones become wallets and transport tickets.

MIFARE is the most widely installed contactless Smart Card technology in the world with about 1.2 billion Smart Card chips and more than seven million reader modules sold. Current shipments of FeliCa ICs stand at 170 million units and of these 30 million are mobile FeliCa chips for use in mobile phones in Japan. Sony is creating a unique business model for the use of contactless IC for mobile phones.

NXP and Sony will individually offer chips and applications based on their respective technology platforms MIFARE and FeliCa, while both companies will continue to develop NFC technologies jointly.

The joint venture has received the support of the GSM association, which is the apex body for the world's major mobile operators. It said 14 operators worldwide will support one common NFC format on the mobile phones they distribute for their networks.

Smart Cards

SEPA A Key Priority

Visa Europe has welcomed the European Central Bank's report, 'The Eurosystem's View of a "SEPA for Cards". The ECB report states that "the Eurosystem expects at least one European card scheme to emerge in the coming years". It adds that this scheme "would be a key factor in enhancing diversity and competition in the market." It also considers that "shareholder-driven solutions" could lead to "excessive price increases" and concludes that "The existence of at least one more European bank-owned scheme would lessen the risk of price increases." Peter Ayliffe, President and CEO of Visa Europe, said: "While we have yet to fully review the report, we agree with the ECB that European governance of payment systems should be one of the key priorities going forward. Visa Europe strongly supports the creation of SEPA and a truly internal market for payments: SEPA will spur competition to the benefit of consumers. At the same time, we recognise the need and desire of European banks to control such a fundamental part of their business."

German Health Card Pilot

Pilot trials for the rollout of the new electronic health card in Germany are to start this year with up to 10,000 new-generation Smart Cards. Sagem Orga is equipping test regions with Smart Cards and card terminals based on the latest gematik specifications and will thus play a crucial role in the future telematics infrastructure of the German healthcare system. Sagem Orga has already passed key tests for approval of the card for one of the pilot regions. The trials involving 10,000 electronic health cards will be followed by tests with larger volumes of up to 100,000 Smart Cards before the whole of Germany is supplied with a total of 80 million health cards.

French Merchants Roll Out V PAY

Visa Europe has reached a milestone with Carte Bleue and French acquirers on the acceptance of its new European SEPA compliant debit card V PAY. French Merchants have begun to display the V PAY decal to welcome V PAY cardholders. Technically, V PAY cards can be accepted at all French merchants with certified EMV terminals. By the end of March 2007, it is expected that in the region of 500,000 merchants will display the V PAY acceptance mark.

Vista to Support Gemalto Smart Cards

To strengthen digital security and help enterprises against continuing threats to corporate data, Gemalto and Microsoft have announced that Windows Vista will support Gemalto .NET devices right out of the box. Enterprises can now easily and cost effectively replace weak user name 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 e-purse services. These steps protect digital identities and data from ever-evolving threats.

Gemalto Acquires Leigh Mardon

Gemalto has entered into an agreement with Leigh Mardon Group Pty Ltd to acquire Leigh Mardon Taiwan, a 100% owned subsidiary of Leigh Mardon Group Pty Ltd. The closing was scheduled to take place on November 30, 2006, upon satisfaction of certain conditions precedent as stated in the agreement. Leigh Mardon is an established supplier of secure transaction products and services with its headquarters in Melbourne, Australia. The company is a market leader in financial cards in Taiwan and Australia.

Sony Doubles Capacity of FeliCa Chip

Sony Australia has developed a new generation of its FeliCa branded contactless IC Smart Card chip, more than doubling its memory capacity. Developed jointly with Fujitsu Ltd, the memory of the new chip has increased from four to nine kilobytes. This augmented capacity makes the new chip a perfect fit for handling multiple applications on the same smart card. With improved processing speeds of 424kbps accompanying its increased memory capacity, the new Sony FeliCa Smart Card makes multi-application management, such as Identification, e-ticketing, e-wallets and access control a truly viable option for a wide range of organisations.

Guatemalan Banks Go Contactless

CPI Card Group and INSIDE Contactless have been selected by Visa Latin America to provide cards with contactless technology for three major banks in Guatemala. As part of the Visa Smart Breakthrough program, CPI Card Group has issued over five million contactless cards in the US with several major issuers in the US market. The contactless cards, manufactured by CPI and powered by MicroPass from INSIDE Contactless, will be issued at Banco Uno, Banco Custcatlan and Bi-Credit.

4
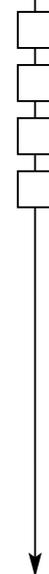
Cubic Awarded $11.58m Contract

The Washington Metropolitan Area Transit Authority has awarded an US$11.58 million contract modification to Cubic Transportation Systems, Inc to implement software and technology upgrades that will unite Washington Metropolitan Area rail, park-and-ride and regional bus systems through common Smart Card media and a centralised transaction processing and reporting back-office system. The system enhancements include new contactless card readers at all Metro subway and parking facilities, which will expand the already successful SmarTrip regional Smart Card system. The upgrades will increase efficiencies and open new commercial opportunities that could save the agency millions of dollars in annual operating costs.

1 Million SIM cards for Mobinil

Sagem Orga has received a landmark order from Mobinil, a mobile operator in Egypt, for 1 million SIM cards. For Sagem Orga this is an important success in the booming Egyptian mobile telecommunications market. Last year, according to industry analyst BIS Shrapner, Egypt has experienced a growth of 84%.

ARM Powered Unattended Reader

Hypercom Corporation has released an ARM powered EMV/PCI approved unattended bankcard reader module for use in the self-service kiosk market. The Optimum H2210 is a manual hybrid card reader accepting both magnetic stripe and Smart Cards and offering key size, integration and flexibility advantages over competitive units, according to the company. It features a 32-bit ARM 7 processor operating at 66Mhz and 4MB flash memory for fast transaction speeds, with program execution contained within the 8MB SDRAM.

Contactless for NYC Subway

VeriFone Holdings is providing an integrated payment solutions being used in the contactless subway trial underway in New York. VeriFone's solution includes the VeriFone Secura system with contactless smart card capabilities, together with management software. The pilot began this summer and involves 80 systems installed at various Metro stations. The pilot is open to any of the 50,000 Citibank contactless customers with a Citi credit and Citibank Debit payment tag, or Citi credit or Citibank Debit MasterCard card with the PayPass logo.

Contactless Solution at Dubai Airport

Dubai International Airport has selected Eastnets and Zebra Card Printer Solutions to provide a card management and issuing solution using contactless Smart Cards for the airport. The cards will be used on new electronic gates (eGates) in the airport, designed to reduce delays and enable registered passengers automated entry or exit through the airport. The solution uses Zebra printers with Mifare cards with 100,000 cardholders enrolled to date. Over 25 Zebra Card Printers are now being used at the airport to produce the contactless Smart Cards needed to accelerate immigration procedures and enable passengers to merely swipe their cards and have a three second fingerprint scan and then they are free to move quickly through the airport.

Vegetable Based Plastic IC Card

Sony has revealed the world's first IC Smart Card made out of vegetable-based plastic, and capable of contactless communication. This particular card can run applications like the Edy pre-paid e-money service, or work as ID access cards for companies. Besides the announcement of the product, Sony also mentioned they will be issuing about 2000 cards with Edy applications to some of their employees. IC cards have been around for a while, but eco-friendly vegetable-based cards with such capabilities are indeed something new. Although there is no real functional difference between these cards and the 100% plastic ones, Sony is trying to show their greener side to the world. Unless costs are competitive this technology is most likely bound to stay on the ground unfortunately.

US Government Selects Gemalto

The highest-ranking agency within the US Executive Branch of Government has chosen Gemalto to provide card management services, including two-factor authentication technology, in compliance with the Homeland Security Presidential Directive 12 (HSPD-12). 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 (CAC) supplied by Gemalto. Under this contract, the comprehensive solution includes deployment and use of personalised smart ID credentials for secure access to information systems and federal buildings.

In addition, Gemalto provides technical advice and integration and delivery services. Intercede is providing the card management system within Gemalto's SafesITe Government solution.

New Smart Card Factory in Slovakia

Giesecke & Devrient is opening a new card production facility located in the city of Nitra in the Slovak Republic. The plant, which took a year to build and covers nearly 20,000 square meters (215,000 sq. ft.), is one of the largest factories in the world for producing Smart Cards for the fields of mobile communications, electronic payment, health care, identification, and IT security. Its production capacity currently runs at more than 250 million card bodies per year, including chip embedding, with enormous potential for the future. All in all, the company has invested roughly 20 million euros in the facility, which employs a staff of nearly 250.

All-On-One-Card for PwC

PricewaterhouseCoopers (PwC) plan to use a contactless all-on-one-card solution at their new Swiss offices using LEGIC technology. One of the challenges facing the new system was to provide a cleverly devised access system, to provide optimum security yet which at the same time was to be as easy to use as possible. PwC had even more requirements the new system has to fulfil: Employees ID cards were also to be used to make e-payments, book flexible workstations, and operate the "Follow&Secure" system, an innovative office automation concept. But with LEGIC's contactless all-in-one-card technology it was a simple matter to bring all these requirements together.

Sagem Orga Passes Test for eGK

Sagem Orga has passed the function test of the operating organisation Gematik for its electronic health card (eGK). Passing this test is the prerequisite for shipping cards to the pilot regions, which is expected to start before the end of 2006. The primary focus of the testing process was on acceptance of the software functions of the operating and application systems of the Smart Card. Gematik examined the software in comprehensive basic and application tests in its new test laboratory and confirmed that the functions of Sagem Orga's product are in compliance with the specifications developed by Gematik. The electronic health card of Sagem Orga is based on version 3.0 of the high-security operating system MICARDO.

Your London Citizen Card Scheme

Accourt, an independent London based consultancy, has been working with London Connects the London-wide agency supporting local, regional and central government in the delivery of the e-government agenda to create a vision for a new pan-London citizen card scheme. The proposed "Your London" card scheme aims to provide a single card for all citizens that will support many aspects of day to day life - travelling, learning, working or recreation throughout London.

The planned card could allow access to local authority services including leisure centres, libraries, educational facilities and transport. Loyalty and discount reward facilities may also be added, in particular in conjunction with smaller retailers in local communities. It is planned to start the rollout of the "Your London" card in 2008 following the trials of a number of small scale schemes in some London Boroughs.

SIM-Centric Solutions For NFC

Oberthur Card Systems reinforces its partnership with Inside Contactless by launching a SIM-centric solution for NFC contactless transaction. Oberthur Card Systems decided to focus only on architectures that allow mobile operators to keep control over the contactless application; Inside Contactless was selected as the ideal partner for the project.

Smart Card Rollout for Canadian Bank

The Royal Bank of Canada has selected ACI's Smart Chip Manager to provide the foundation for its planned migration to chip technology for debit and credit cards. RBC chose Smart Chip Manager as its foundation for initial chip card issuance for market trials, beginning with internal trials in late 2007 and as a future platform for launching innovative payment card products using chip technology. ACI will work with RBC to migrate to chip technology gradually and support its existing and future business goals for chip cards.

T2100 Deployed at Bangkok Airport

Hypercom Corporation has announced that the new Thailand Suvarnabhumi International Airport in Bangkok has selected Hypercom's Optimum T2100 payment terminal as the preferred choice for card payment solutions. More than 1,000 units are being deployed in the airport's retail outlets and duty free shops.

6

The adoption adds to the 20,000 T2100 units that have been installed by retailers in Thailand since its introduction in October 2005. The terminals at the airport were offered to retailers by the country's two major banks: Siam Commercial Bank (SCB) and TMB Bank (TMB). The airport opened in September.

Fargo Joins GlobalPlatform

Fargo Electronics has joined the membership of international standards body, GlobalPlatform, in a move, that demonstrates the company's commitment to the development and marketing of interoperable standards across the entire Smart Card infrastructure. Fargo Electronics joins GlobalPlatform as a Participating Member and will add its voice to the work of the GlobalPlatform Systems Committee. The Systems Committee designs infrastructures for single and multi-application Smart Card programs and develops associated requirements, specifications and guidelines. A current work priority of the committee is to finalise the GlobalPlatform Systems Compliance Program, the first phase of which was launched in November 2006.

FIPS 201 Certification for ICLASS

HID Global's iCLASS model access control readers have been approved by US General Services Administration (GSA) as Transparent Contactless Readers for their FIPS 201 Approved Products List. The certifications now enable HID Global to provide government agencies and other organisations with a trusted source for FIPS 201 certified contactless Smart Card readers. In addition to these readers, HID Global has also received approval on the iCLASS OEM 150 module to assist manufacturers in embedding HID's FIPS 201 approved products into their own.

New Biometric Solutions for Norway

Motorola Inc has recieved a contract with Norway's Ministry of Foreign Affairs (UD) and the National Police Computing and Material Service (PDMT) to provide for the collection and verification of biometric data for Norwegian passports, visas and other travel documents. Biometric data provides the capability to identify people through unique physical attributes such as fingerprints, the iris, or face characteristics. Motorola will supply approximately 700 fixed enrolment stations for use in Norway and a further 100 portable versions for use in Norwegian embassies and other enrolment centres around the globe.

Finger print capture will be capable of supporting 1000 pixels per inch (PPI) images, as well as the more common 500 PPI.

Biometric Payments for Citibank

Pay By Touch has announced that Citibank Singapore has rolled out Pay By Touch's biometric payment services to its Citibank Clear Platinum cardholders. With immediate effect, cardholders are invited to enrol in the biometric credit card service, and pay for goods and services with the touch of a finger.

Europay, MasterCard & Visa

VISA Java EMV Cards in Hong Kong

Gemalto has announced that it has delivered the first Visa Java EMV cards to DBS Bank (Hong Kong) Limited, an Asia banking specialist and one of the leading card issuers in Hong Kong. This project marks a significant milestone for Smart Card development in Hong Kong's banking industry. In order to meet the latest Visa's security requirements, DBS Bank chose to partner with Gemalto in implementing its ComPass Visa card program. The Visa EMV (Europay, MasterCard, Visa) cards comply with EMV requirements and will help DBS Bank to bring greater peace of mind for cardholders, with additional protection against fraud.

Gemalto's Visa EMV card is highly secure and has an open platform operating system that enables post issuance application downloads and loyalty functions. Additionally, the card provides a unique attraction for users by featuring a translucent card body, which is particularly nice-looking. With these Visa Java EMV cards issued by DBS Bank currently in circulation, this migration to the EMV standards will kick off the largest exercise of its kind in Hong Kong market.

MasterCard Push New Smart Card

MasterCard has rolled out a global dual-interface (contact and contactless) Smart Card for the Asia Pacific, Middle Eastern and African (APEMA) markets named the MasterCard PayPass M/Chip 4 Combi Card. The "latest generation" of MasterCard EMV payment applications uses both contact and contactless chip payment solutions on a MULTOS (multiple operating system) 32K dual-interface platform provided by Keycorp.

World News in Brief

7

Bell ID Signs Contract with CUETS

Bell ID has announced that it has signed a contract for the provision of a full EMV migration solution with CUETS. The ANDiS4EMV solution provided to CUETS combines the management of card, key and application life-cycles with EMV script processing used for the generation, management and delivery of scripts to update cards dynamically post issuance, and for secure management of offline payment risk. The ANDiS solution, which will facilitate the issuance of millions of EMV-compliant MULTOS StepOne cards, furthermore provides a comprehensive key management system, data preparation functionality and a platform for post-issuance personalisation.

UAE's 1st Retail EMV System

S1 Corporation, a provider of customer interaction software solutions for financial and payments services, has announced that the National Bank of Dubai (NBD) in association with Dubai Duty Free (DDF) has implemented the first EMV-compliant, integrated EFTPOS solution in the UAE using S1's Postilion technology. The implementation of this solution at DDF, based at Dubai International Airport and the third largest airport retailer in the world, is the first EMV EFTPOS implementation in the UAE and the Gulf Region.

Contactless EMV Reader

ViVOtech has launched the ARM based ViVOpay 4500 EMV contactless reader for the European, Middle Eastern, Asian, Canadian, and Latin American markets. Built on ViVOtech's ViVOpay 4000, the ViVOpay 4500 features ARM processor-based hardware with large application memory to support multiple branded EMV and magnetic stripe contactless applications in addition to retailer loyalty, prepaid and NFC mobile phone payment programs.

Radio Frequency Indentification

Oyster Card Recieves RFID Award

Officials at Cubic Transportation Systems Ltd have said the Oyster Smart Card transport ticketing system developed for London by principle partners Cubic and EDS has won a 2006 RFID Breakthrough Award. The award was presented to TranSys, the consortium that Cubic and EDS founded to deliver, maintain and operate the PRESTIGE (the name of the project)/Oyster card system.

Smart Label Factory for China

The Muehlbauer technology group has announced the order of a complete RFID Smart Label production line ("Smart Label Factory") from China recently, Muehlbauer enhanced its RFID-portfolio with the new converting line and is now able to offer complete solutions for the production of RFID Smart Labels from one source, in addition to the turnkey solutions in the business areas of Smart Cards and ePassports.This strategy already yields results. Within a short time, four customers ordered the new production equipment.

Semtech RFID Ltd., a wholly owned subsidiary of Sino-Tech International Holdings Ltd., as one of the four customers with the manufacturing base in Dongguan, Guangdong, China, is now the first company to order a turnkey Smart Label production line for the Chinese market from Muehlbauer: A flip chip line for the production of inlays and a converting line for the fabrication of self-adhesive labels or RFID tickets. Semtech RFID Ltd. will be the first company in China to produce inlays, as well as finished Smart Labels, on Muehlbauer equipment.

RFID Inlays for Pilot Project in China

UPM Raflatac is taking part in the largest retail RFID pilot project in China. The company has been selected by retail METRO Group to supply its Rafsec G2 ShortDipole RFID inlays for an innovative pilot scheme that will see products tracked along the supply chain from China to Germany. UPM Raflatac will provide its EPC Gen2 UHF tags for the METRO Group's pioneering project "Advanced Logistics Asia". in Germany. The inlays, converted into four-inch by six-inch labels by RFID Systems and Supplies Limited (RSS), will be tested at package level using different product categories. The RFID tagged packages will be monitored as they are shipped from the consolidation centre in China to METRO operations in Germany.

RFID Smart Cards for Fulham FC Fans

London-based premiership football club Fulham has started issuing RFID-enabled Smart Card tickets to fans to cut queues at the turnstiles on match days. This is to try to boost safety at its Craven Cottage grounds. A new RFID Smart Card has been developed for use by the London-based premiership club, containing specific data on football matches that the cardholder has paid for. Each card holds a chip and aerial, and can be updated via telephone.

Some 20,000 of these new Smart Cards have been issued to Fulham members and season-ticket customers. In total, 46 Smart Card readers have been installed on turnstiles at the club's grounds. Fulham's head of IT, Matthew McGrory, describes the new system as faster and safer. "The old system took, at the best of times, ten to 20 seconds per season-ticket holder on the turnstile," he said. "That is now down to four seconds."

On The Move

Oberthur CEO Resigns

The Board of Directors of Oberthur Card Systems has accepted the resignation from office of Pierre Barberis as Chief Executive Officer and Director. After more than four years in office, the essential tasks entrusted to Mr Barberis in 2002 have been completed, and Oberthur Card Systems is now perfectly equipped to face market conditions in 2007. For personal reasons, Mr Barberis now wishes to relocate to South-East Asia, where he will have an occasional consultancy role on the general management of Oberthur Card Systems, his main task being to provide assistance with its development in Asia, an area of major development for the company.

INSIDE Appoints New CSO

INSIDE Contactless has added the latest member to its management team, with the appointment of Bruno Benteo as Chief Security Officer. Bruno's charter is to further develop security features for INSIDE's contactless product line. Mr Benteo comes to INSIDE from THALES, where he was Director of THALES Security Systems Toulouse (France) and also in charge of Business development in Asia, USA and Australia from 1998 to 2006

QI Systems Appoints First CTO

QI Systems Inc has announced that the Company has appointed industry veteran Donny V. Lee to the newly created position of Chief Technology Officer. Effective immediately, Mr. Lee will assume primary responsibilities for strategic planning and implementation for all of QI Systems' design engineering, production and technical development.

CRYPTOCard Appoints New VP

CRYPTOCard has announced that in response to the rapid increase in demand for its two-factor authentication technology in the United States and Canada, it has appointed David Scott as Vice President of North American Sales. Scott will oversee all North American sales, with a particular focus on the continued development of CRYPTOCard's fast-expanding channel network. The arrival of Scott underscores CRYPTOCard's commitment to its channel partners, which are expected to account for 99% of all sales worldwide.

Change of CEO at Octopus

The Board of Octopus Holdings Limited (OHL) has announced that Mr Eric Tai, Chief Executive Officer (CEO), has decided not to renew his contract with the Octopus group when it expired on 18 November 2006. Mr Tai joined Octopus Cards Limited as CEO in November 2001. At the same time, the Board of OHL has announced the appointment of Ms Prudence Chan as the new CEO. Ms Chan has joined the group on 1 November 2006 as CEO - Designate and became CEO on 19 November 2006. Ms Chan's appointment is subject to approval by the Hong Kong Monetary Authority.

New Director at SmartCentric

Continuing the expansion of its operations in the Americas, SmartCentric Technologies has announced the appointment of Carl Painter in the newly created role of Director Technical Services for North America, effective December 1st 2006. His appointment is timely, with the first release of the fully contactless (RFID) version of SmartCity, due for release during the first half 2007.

Sirit Appoints New RFID Engineer

Sirit Inc, a provider of radio frequency identification (RFID) reader technology, has announced the appointment of Bruce Roesner to the position of Chief Technology Officer and Vice President of Engineering, effective immediately. In this role, Mr. Roesner will manage the Company's RFID product and solutions development across all application areas.
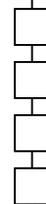
Rumours From the Front Line

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

Olivier Piou, the CEO of Gemalto, has really got his hands full over the coming months. The problem is simple, Gemplus and Axalto before the merger were doing the same business with similar skill and production resources. The major customers - banks and mobile network operators - always like to dual source so the trend will be for the joint company to lose business in these areas. This should advantage Oberthur Card Systems and Giesecke and Devrient, who have recently announced the opening of a new SIM factory in Delhi.

Against this backdrop the card prices are aggressive, SIM prices have halved in the last 18 months and the banks so far have been running with the lowest cost products. So we have fewer cards at a much lower price with an absolute need to reduce production costs by moving factories into more economic environments. When is the blood letting going to start? We have already heard about the closure of the Gemplus Havant factory, rumoured to be March 2007, with the potential for 350 job losses.

Although the letter to employees suggests that posts will be moved to the Axalto plant in nearby Segensworth which currently employs 250 people. Personally I wouldn't want to bank on that! Apart from production we have sales, marketing, admin and R & D, all duplicated between the two original companies. Discussion with well informed sources believe that it is only the labour regulation that are holding things up and I gather that time is fast running out.

Oliver Piou and his cohorts would have you believe that digital identity and enterprise security is the way forward. Not that these aren't growth areas but the danger is that the basic card, token, or document is still a commodity and equally subject to aggressive pricing. As many people keep pointing out to me the ePassport with its 10 year life time is not the bonanza many are searching for. Last week Gemalto were publicising that Microsoft will support their dot net Smart Cards and tokens in Windows Vista.

The press release went on to say that this means you don't need any additional software or middleware - so where is the value added for Gemalto? Nobody I have spoken to believes that the company is currently capable of moving up the value chain to the much touted field of digital security, so is there some acquisition in the offing?

Contactless payments are back in the news again, this time we have a joint trial between Mastercard, Visa and American Express. At a recent APACS meeting the outline details were announced for the initial London roll out. It would appear that the scheme is following Visa's low value contactless approach which uses the EMV Dynamic Data Authentication (DDA) digital signature and allows transactions up to £10 to be conducted at high speed off-line. Over this amount or every so many transactions the customer has to do a standard EMV using the contact with PIN entry just to check back with base.

Over half a million new cards will be issued with over 4000 updated contactless terminals in over 1000 shops in the City of London and Docklands. Now all great stuff, but this is going to happen in September 2007? Not that this is impossible but all the suppliers I have talked to think it's a tad ambitious. But then you could argue, one terminal, one card, and one payment and you're off!

The most interesting bit is the admission or even gospel that this is the cash alternative, so is this the end of the electronic purse?

Squeak squeak

opinion

UHF RFID Applications Meet Unprecedented Opportunity

By Freda Tong, Senior Market Analyst of Vertical Market Research, IDC China

The radio frequency identification (RFID) vertical application market has been estimated by IDC at RMB 1.477 billion in China in 2005, in which ultrahigh frequency (UHF) RFID application accounted for only 10.6% at RMB 156 million. IDC predicts that by 2010, the total market revenue will reach RMB 29.837 billion, with a forecast compound annual growth rate (CAGR) for 2005-2010 of 82.4%.

China's RFID application market has entered the elementary application stage from the introduction phase. RFID applications in this stage involve mainly low frequency (LF) and high frequency (HF) RFID in diverse and mature forms of application. Though of higher commercial value, UHF applications are almost all small-scale closed-loop pilots for a variety of reasons (e.g., domestic standard, technology, and price). Domestic RFID application has extended to industries such as government, logistics (including postal), manufacturing, transport, and communication.

The main application fields of UHF RFID include supply chain (including manufacturing, retail, transport, and logistics), personnel/bill management, asset management, and vehicle management. Through analysis of cases where RFID is applied, IDC finds the current domestic application of RFID features the following characteristics:

1. Government-driven projects are developed more smoothly than enterprise-driven projects.
2. Many applications are small-scale closed-loop pilot applications.
3. RFID tags are used more for logistics equipment and vehicles than for individual commodities.

Currently, LF and HF dominate China RFID market in terms of frequency. This is because the entry barriers for LF/HF RFID technology are low, and many businesses are active in this market where the application cost is also low. Moreover, China's second-generation ID card project and smart traffic card project have facilitated the application of LF and HF RFID in more areas. Nevertheless, product homogeneity is high on the market.

Application of UHF RFID has taken off thanks to promotion from multinationals like Wal-Mart. Though R&D for the UHF chip is weak, the Chinese government attaches great emphasis to UHF standard development and chip R&D, and has made clear progress. Closed-loop UHF applications have delivered satisfying results with endorsement from the government and some businesses. Once the standards are released, China's UHF market will take off and domestic UHF chipmakers will also grow with the continued promotion by the government.

Based on analysis of Chinese RFID applications and market, IDC believes the key to successful implementation is largely planning. Before a project, the benefits of RFID over barcodes or other technologies must be considered. During project planning, the business logic should be analyzed in detail, the commercial processes designed logically, and the business plan formulated in accordance with the features of RFID. It is also crucial for RFID vendors and systems integrators (SIs) to cultivate the market.

They should not only train target customers in relation to RFID technology, but also increase investments in pilot projects to showcase the benefits of RFID by providing hands-on experience to users. The success of these trial projects in UHF application will strongly promote market growth of UHF applications.

www.idc.com

RFID Exotica

By Dr Peter Harrop,Chairman, IDTechEx Ltd

IDTechEx

Dr Peter Harrop

At IDTechEx, when we teach Radio Frequency Identification RFID, we talk of it being a ubiquitous enabling technology like the wheel or paper. Some people consider that to be rather far fetched. After all, wheels extend from prayer wheels, steering wheels and wheels of fortune to aircraft wheels and microscopic wheels in Micro Electro Mechanical Systems MEMS. They are everywhere, as is paper because that appears as anything from art to toilet paper, packaging, books and origami.

However, RFID is now used from Bulgaria to Namibia, from Azerbaijan to Vietnam and Antarctica. It is a life to death experience because it is on containers of sperm and new born babies but it also marks burial plots; the Federal Emergency Management Agency in the USA puts RFID on corpses. Somewhere in between, RFID traces anodes in copper smelters and controls paedophiles. There are well over 10,000 RFID projects out there and there are over 1000 suppliers that have now landed substantial orders for the specialist RFID hardware and services involved. Yet things have barely started. For examples, 50,000 libraries should be tagging everything for many benefits but only 500 (1%) have done so as yet. The IDTechEx RFID Knowledgebase has captured over 2400 cases of RFID in action involving over 2500 organisations in 85 countries. That includes all the examples we have mentioned above. We are now adding cases at twice the rate of one year ago as RFID truly permeates the whole planet.

RFID is monitoring the post in Algeria and Bosnia-Herzegovina and it being used in the Philippines in the form of Stored Value Cards SVCs to replace cash and reduce queues. Road tolling is a use in Slovakia. For proof of ownership it is on reindeer in Lapland. In precious wild plants in New Zealand, it has led to arrests under conservation orders. RFID tags on prepared sushi meals in Japan permit the staff to automate payment and stock-taking but in Antarctica it has enabled research on the behaviour of penguins.

In Thailand, they like to put RFID on chickens for disease control and they use it in cock fighting. In South Africa, RFID tracks ore but in Turkey they encounter it as a loyalty card. In Canada, they have been tracking food trolleys in their aircraft but Italy has RFID on intelligent mooring buoys in marinas giving personalised promotional messages when you tie up. Australia tags boats for theft prevention. The Australians tag race-horses by law but the Canadians tag fish for conservation. In the UK RFID has been used to research the behaviour of insects including butterflies and IDTechEx has several studies of the tagging of elk but not in China, where pandas are the centre of attention.

RFID is the basis of an automated tour of a museum in Korea and it prevents theft in art galleries in France - an improvement on the crude performance of the traditional anti-theft tag in shops and libraries, which is not RFID. From casino chips in the USA to a multifunctional bank card in Azerbaijan, national identification cards in Estonia, China and Oman, weapons permits in Honduras, laptop theft prevention in Brazil and police evidence bags in the UK, one can only wonder what comes next. There is access control in Mexico, student tracking in India and Japan (for safety and attendance control), passports in Slovenia but they have all been done.

RFID is about Government spending: RFID companies that believe that RFID is all about civil supply chains are more likely to lose money, sometimes spectacularly so. Those that investigate where the money is really being spent and where the competition is lighter are generally prospering, from Lockheed Martin sitting on the world's largest RFID order of $425 million for the US Military and a group of Chinese companies rolling out the $6 billion China National ID Card scheme and other companies salivating about the planned UK national ID card scheme which promises to burn many times that sum giving cards to 15% of the number of people involved in China.

opinion

12

Governments have placed the big orders for RFID so far, including tagging post boxes in Saudi Arabia - a world first - and the massive Hong Kong Octopus card scheme for almost all transport and now for general shopping and equivalent schemes to Octopus across China. Sometimes it is local government that has the big chequebook as with mass transit card schemes, something that enabled ERG of Australia to be a US$137 million RFID business with installed equipment from Gothenburg to Beijing responsible for five billion transactions yearly. RFID is even used by the French navy on nuclear submarines and implanted into government employees in Mexico.

RFID is about security: Most of the government backed RFID is about security but what made a Swedish company largest in RFID today? It was secure access, with Assa Abloy enjoying something in the region of $300 million in sales from its ten carefully chosen RFID acquisitions in or near this sector.

RFID is about error prevention: Those thinking of RFID for replacing barcodes and at least civil supply chains are boxing themselves into a corner. The biggest RFID application in Healthcare is the 40 million tags delivered for error prevention on AstraZeneca anaesthetic Diprivan used in operating theatres. The many drug trials that have RFID-enabled, compliance-monitoring blisterpacks this year are concerned with error prevention. The TREAD Act in the US is expected to drive RFID into every car tyre for error prevention. The largest milk cooperative in the world, Fonterra of New Zealand, has ordered over 500,000 tags for milk samples and preventing mistakes with pipe connections and, in a way, the tagging of over ten million test tubes used for blood samples and drug development (potential several billion yearly) is associated with automated recordkeeping because humans make errors.

Indeed, the tagging of mothers and new born babies in German, US and other hospitals is concerned with preventing mother baby mismatches which have reached 20,000 yearly in the US alone. That is just the reported ones. Beyond error prevention, there is anti-counterfeiting of drugs, designer goods and cigarettes and more that is being progressed ahead of conventional track and trace. It has potential of 150 billion yearly just for those three types of product. Is that really a niche market?

The bottom line: The bottom line is that RFID is being used for security, safety, error prevention, anti-counterfeiting, cost reduction, increasing sales, entertainment, crime prevention, customer convenience and art and there is more to come. It is rather as if we had just invented the wheel...or paper.

Events Diary

January 2007

17-19	OMNICARD 2007 - *Berlin, Germany - www.omnicard.de*
21-23	Intersec Middle East, *Dubai, UAE - www.intersecexpo.com*
22-23	Global Payments Strategies 2007 - *Monte Carlo, Monaco - www.nacha.org/conferences/Global2007*
29 - 30	Global RFID ROI Summit - *London, UK - www.rfid-roi.com*
31 - 01	Security Printing & Alternative Solutions - *Warsaw, Poland - www.security-printing.com*

Febuary 2007

05-09	RSA Conference 2007 - *San Francisco - www.rsaconference.com/2007/US/*
06	The Credit Card Awards 2007 - *The Grosvenor House Hotel, London - www.thecreditcardawards.com*
12-15	3GSM World Congress - *Barcelona, Spain - http://3gsmworldcongress.com*
21-22	RFID Smart Labels USA 2007 -*Boston, USA - www.smartlabelsusa.com*

Smart Health Care - The Next Generation

By Jason Smith, Staff Reporter, Smart Card News Ltd

In 1998 France introduced Smart Card technology into their health care system. French citizens where issued with a Sesam Vitale smart health card with the aim of moving away from a paper-based healthcare benefits payment system to a system based on electronic transactions. When the program was initiated, the French government was the second largest healthcare spender in the world, but citizens were frustrated with the delays encountered in obtaining reimbursement.

Jason Smith

Reducing administrative costs was the key driver for the project. The government needed to change its approach and develop a more efficient and cost-effective system. The new card also enabled the electronic transfer of medical records and prescriptions to healthcare agencies responsible for reimbursement. The Vitale project was controversial from the start, and for the first few years after its introduction doctors resisted using it, fearing they would lose revenue and control.

Today the Sesame Vitale program has become one of the most successful healthcare Smart Card projects worldwide. The Sesam Vitale Smart Card-based infrastructure now incorporates many components, including around 60 million Smart Cards, telecoms network and a message service, 223,000 health care professionals, 230 health software applications, 210,000 card readers, 25 servers handling the flows and 23,000 terminals for card updating, this enables insurers nationwide to access personal information and expedite claims as quickly as possible.

Overall diagram of the SESAM-Vitale system

"The Sesam Vitale health card has become an important part of the French healthcare system. Health professionals and users have the added convenience of being able to conduct transactions quickly and easily with just the one card while knowing the process is secure.", said Jacques de Varax, general manager, Groupement d'Intérêt Economique Sesam-Vitale. "Health insurers can process more claims, faster with a high level of security." However the first generation cards held no photographic identification and stored only a limited amount of data. Due to this GIE Sesam Vitale, the state-controlled social security organisation (CNAM) which manages the Sesame Vitale program, has decided to introduce a second generation version of the Sesam Vitale health card.

The new version, Sesam Vitale 2, will include a photograph and a much greater capacity to store information such as complementary health insurance details. In addition, with the increased storage capacity, administrative processes can also be performed faster. GIE Sesam-Vitale says a new card is necessary because optional insurance plans are joining the Sesam-Vitale system, and the current version of the card is not upgradeable to accommodate all these changes.

The new cards will also have an electronic prescription function. The insured will present his or her Vitale 2 card to the pharmacist, whose computer will read the prescription off of the chip. They will have 32 kilobytes of memory and a crypto-processor Smart Card chip, which is more sophisticated than the 3K memory chip on the current card.

14

The Smart Card chip will store such data as the name of the insured, the health insurance scheme covering the cardholder, and names of his or her beneficiaries. It will also store a digital image of the cardholder, and the same photo will be printed on the surface of the card. This new Smart Card chip technology will be supplied by NXP Semiconductors (formerly a division of Phillips).

"The new Sesam-Vitale health card is a good example of how Smart Card technology can enhance people's lives while maintaining their right to privacy," said Christophe Duverne, senior vice president and general manager for Identification, NXP Semiconductors.

GIE Sesam-Vitale has also picked two French Smart Card companies as the suppliers for the manufacture and personalisation of the second generation of healthcare cards. Gemalto and Oberthur Card Systems will both supply the initial batch of cards issued in November 2006. Gemalto has said they received two-year contracts for at least 16 million cards. Oberthur said it received a multi-year contract, but did not specify how many cards were called for. But work on Vitale 2 has not been without controversy, in part because of reported security problems with the Vitale 1 card. In 2005, two individuals demonstrated they could copy the non-encrypted data on the Vitale 1 card and load it onto another card, according to news reports. A fake card could be used to illegally receive health care services.

The significance of such a breach could be even greater in a Vitale 2 card, because the card contains more data, such as the person's photo, which could then be used to make a fake card. However GIE Sesam-Vitale says that the Vitale 2 card could thwart such an attack because the data will be encrypted.

Cash Replacement Scheduled for 2007

By Sandra Alzetta, Senior Vice President Consumer Market Development, Visa Europe

Visa UK can confirmed plans for the first nationwide roll out of contactless payment cards across the UK, starting in London, by the end of next year. The decision, supported by all Visa UK member banks, will enable card holders to "wave and pay" for low value every day items, such as their morning coffee and newspapers, by simply waving a new secure contactless card over a card reader in participating shops.

Visa Contactless is a fast and convenient extension to the chip and PIN cards already in use in the UK. It extends the trusted chip technology to enable a new way to pay that is faster, more convenient and more secure than cash. Transactions completed in less than a second create time savings for consumers and retailers, significantly reducing queue times at checkouts.

With over 75% of all cash payments being less than £10, the introduction of contactless payments will play a major role in encouraging the use of cards over cash for low value transactions. In addition, the decision to go live in less than a year supports our vision for a cashless Olympic Games in London in 2012. Contactless payments are particularly suited to retail environments such as fast food outlets, coffee shops, newsagents, off licences, bars, pubs, parking facilities and vending machines, all of which tend to have a high cash turnover and where rapid checkout times are desirable.

Research undertaken by Visa in the UK has indicated that consumers are very likely to appreciate the convenience and speed that it offers as an alternative to cash. As a next stage, Visa UK and many of its member banks are working closely with retailers to enlist their support in advance of the contactless roll out. Further details of the precise launch plans are expected to be available by March 2007.

15

Mobile Authentication - The Future of Online Banking Security?

THALES

By Dragoljub Nesic, Head of Professional Services, Thales e-Security

The mandatory introduction of Chip and PIN in the UK is already paying dividends in the payments industry. There has been a significant reduction in retail transactions fraud. However, as statistics from APACS reveal below, fraudsters are not deterred and are instead focussing their efforts on different payments channels. Whilst Chip and PIN provides the much-needed second authenticating factor for in-store transactions, cardholder-not-present (CNP) payments are still highly vulnerable, with fraud losses costing £95.3 million in the first six months of 2006 in the UK alone.

UK PLASTIC CARD AND ONLINE BANKING FRAUD LOSSES

Type of fraud	Jan to Jun-04	Jan to Jun-06	+/-% (04/06)
Online, phone and mail order fraud (CNP) fraud	£70.2m	£95.3m	35.70%
Counterfeit	£66.1m	£53.0m	-19.80%
Lost/stolen	£80.5m	£38.1m	-40.30%
Mail non-receipt	£38.5m	£9.8m	-73.10%
Card ID theft	£19.2m	£15.0m	-21.80%
Total	£252.6m	£209.3m	
Contained within this total:			
Fraud abroad	£46.0m	£48.5m	5.40%
Retailer (face-to-face)	£112.8m	£42.1m	-62.70%
Cash machine fraud	£36.9m	£39.6m	7.30%
	Jan to Jun-04	Jan to Jun-06	+/-% (04/06)
Online banking fraud	£4m	£22.5m	462.50%
Phishing incidents	126	5,059	3915.10%

Source: APACS 30.11.06

Fraud is one of the main drivers for stronger authentication and with CNP fraud levels on the rise, it will not be long before increased security measures for online transactions are implemented in the UK. Banks are also seeking to protect their brand equity and safeguard customers' identities. The demand for this is apparent from a Visa report, which cites that 30% of British consumers are wary of online shopping due to security concerns, highlighting an emerging group of consumers who are trend aware, technology scared (TATS). Banks are currently piloting technology to further secure CNP transactions. One scheme that banks are considering, that is being encouraged from APACS, is to provide each customer with a smart card reader.

Solutions are also being considered based on the mobile phone as a key tool in providing stronger online authentication. SIM cards are the largest application of Smart Card technology in the world so there is value in harnessing their growing processing power to perform other tasks such as identity authentication. Features that make it an attractive option for banks include its ubiquitous use and penetration in the market, convenient handling and, perhaps most importantly, zero distribution costs. A mobile phone lends itself to multiple authentication methods. Firstly, one-off security details can be delivered to the user via SMS. SMS password confirmation serves as dual-channel identity authentication, making the transaction stronger but not as secure as Chip and PIN. The need for reliable network coverage to enable timely receipt and processing of the SMS password is a possible limitation of this authentication method.

A secondary use is to equip handsets with software that turns them into cryptographic devices. Two-factor authentication is achieved by pushing an application onto customers' mobiles. The handset acts as a PIN-activated challenge-response device, providing a code to authenticate the online transaction. The advantage of this method is that there is no requirement for network coverage at the time of authentication - this is only needed during application provisioning.

Furthermore, although most handsets support Java applications, which, in theory, are platform independent, increased diversity of handsets may require extensive testing in order to assure correct operation on any one. Finally, Radio Frequency Identification Technology (RFID) installed on mobile phones can create a contactless payment device whereby users simply pass the handset in front of a scanner to make a payment. A recent study by Ipsos Insight and Peppercoin in the US found that more than 67 million Americans used a credit or debit card for a purchase of less than $5 in a 30-day period. These findings show the preference for electronic payments and highlight the demand for a rapid payment technology which contactless devices provide.voice and identify transactions made under duress. Although far off, innovations such as these would not only cut the rate of fraud and save banks millions of pounds, but they would also improve customer confidence in online transactions.

Most notably, as the sophistication and capacity of handsets rises, so do the possibilities of strong authentication. VoIP (Voice imprint Recognition) active callback with biometric is one security method that could provide stronger authentication in the near future. Other options involve biometric fingerprint readers on the handsets, or the provision of a Trusted Platform Module (TPM) on the handsets, allowing an increased level of confidence in the security of the platforms. A TPM is a specialised chip that can be installed in a personal computer, or in this case, a mobile phone, for hardware authentication. It authenticates the mobile rather than the user and so it reduces the risk that data on the phone will be compromised by physical theft or by an external hacker. Future modifications could also enable this technology to detect distress in the voice and identify transactions made under duress. Although far off, innovations such as these would not only cut the rate of fraud and save banks millions of pounds, but they would also improve customer confidence in online transactions.

It is likely that UK banks will eventually offer both Smart Card readers and mobile authentication, providing customers with the freedom to choose an option that suits them best whilst removing the risk posed by weaker authentication. Application-based mobile authentication will incur a greater investment from banks, therefore more lucrative clients could be the only group to benefit in the initial investment phase. The banking industry could witness collaboration with mobile providers to supply customers with compatible handsets.

Further a field, both the Far East and Eastern Europe are already incorporating mobile authentication into online transaction security. There are several push and pull factors that have encouraged the growth of this particular security measure in these parts of the world. Banks are faced with a high level of local cyber crime, such as phishing attacks, forcing them to implement stronger authentication. Mobile communication via SMS is highly popular in these regions and is therefore considered an extremely viable addition to securing online transactions. Such regions have also been faced with rapid technology infrastructure development within a short space of time, allowing them to technology leapfrog. They need not pass through the experimental phases of developed countries and are able to effectively skip a generation of IT.

However, even using mobile phones for user authentication does not fully guarantee protection from fraud. Mobile phones will eventually become as vulnerable as PCs due to their growing use as Internet terminals with download functionality, Wi-Fi capabilities and other IT connections. With these technological developments, the number of attacks on mobile phones is expected to increase leaving users open to ID theft from their mobile as well as their PC.

The solution? Mobile phones will need to utilise the cryptographic functionality readily embedded within phone SIM cards or, as mentioned earlier, a TPM or an equivalent. This effectively replicates the level of security provided by Chip & PIN. Compared to Chip & PIN, mobile and SIM card-based authentication requires collaboration between handset manufacturers, mobile operators, banks and SIM card manufactures. Crucially, all of them have to see a clear commercial benefit in driving mobile security solutions forward. Whilst the payments environment continues to migrate towards electronic transactions, banks are no longer at liberty to ignore the losses incurred through card fraud. Mounting pressure from consumers doubtful of online security is also forcing banks to seriously address this threat. Banks must act now to lead the fight against fraud. Whilst mobile authentication is only one of a number of available options, it is an attractive solution to combating fraud.

The SSL/TLS Protocol and MITM Attack

By Dr David Everett, Principal Consultant, Microexpert Ltd

Microexpert®

Dr David Everett

The SSL Version 3 (Secure Socket Layer) protocol (as adopted by the IETF as TLS, Transport Layer Security) is widely used today for securing communications over the internet between a client and host server. When used by a browser to access confidential resources such as bank accounts one often hears about the MITM (Man in the Middle attack) as used in Phishing attacks where one is redirected to a bogus server and the MITM obtains your account number and password. This briefing note explains the problem and shows how it can be resolved by the use of client certificates. The basic SSL protocol is shown in the figure below:
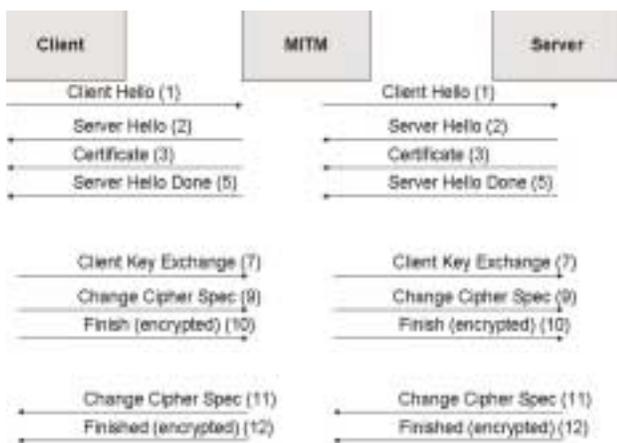

Figure 1 - The Basic Handshake Protocol: In this case the MITM sets up two SSL sessions, one with the client and one with the server. At the end of the handshake (step 12) communications are encrypted but only on a link basis so the MITM can decipher all the messages and obtain the user's name and password. The core element of this protocol is that the client generates a secret key that will be used for encrypting the channel, this is sent to the server in step 7 (but here the MITM) encrypted with the public key provided in the certificate message (step 3), which unfortunately is the key of the MITM.

It is the practical difficulty of the client being able to validate the server certificate that allows this attack to succeed. The MITM may have obtained a certificate for a similar domain name (e.g. A letter o changed for a zero) signed by an acceptable (to the user) CA. Note also that the server doesn't actually at step 12 know whether he is talking to the authentic client. Now look at what happens if we introduce a client certificate as shown below:

Figure 2 - The Client Certificate Handshake Protocol: The difference here is the request for the client certificate in step 4 (which the server can check against its authorised list). The bit that defeats the MITM is step 8 which is a hash of the previous messages signed by the client. Some analysts have commented that you can easily make the client sign a chosen message using a script (e.g. ActiveX). But this would require an unbelievably lax position on the client who would be equally susceptible to an ActiveX control that wipes his hard disk.
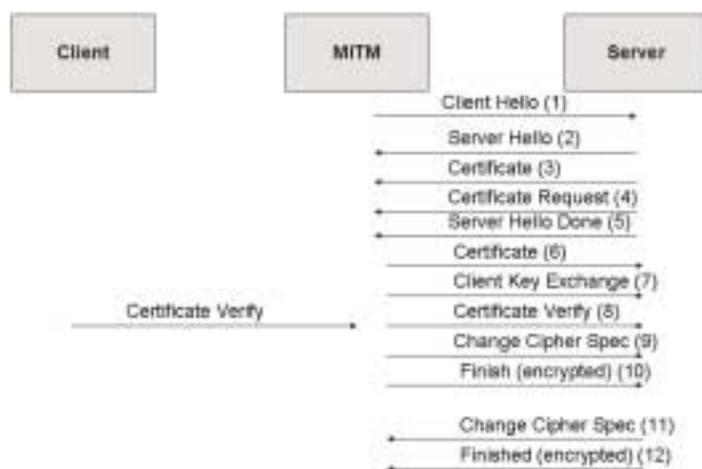
If in doubt the client could always use the Firefox browser which won't implement such controls instead of Internet Explorer. It can be taken for granted that we would recommend the use of a Smart Card for handling the client certificate by which means you can achieve 2-Factor authentication for step 8. You should notice however that although the server has authenticated the client that the client can still be duped because of the difficulty in validating the server certificate. One simple solution to this problem is for the server to send at the end of the handshake a secret picture obtained from the client at the point of registration.

Take a look at Microexpert's demo - **http://ipaqjohn.smartcardgroup.com** - to see this in action.

18

The Dawn of the Digital City

By Jason Smith, Staff Reporter, Smart Card News Ltd

Jason Smith

Imagine what waking up in the future will be like? You wake up to your alarm clock in a sweat after having a bad dream. Your home computer informs you that your pulse rate is abnormally high so you need to relax by maybe doing some yoga. It also suggests a healthy diet plan for the day to help control your blood pressure. You take the computers advice and head to the fridge to get some orange juice but find you have run out. After telling you there is major traffic on your main route to work and showing you an alternative route, your home computer then informs you it has already ordered some more orange juice.

This may sound like an episode of "The Jetsons," but this future is closer then you think thanks to a joint venture between Gale International and POSCO Engineering and Construction Company Limited. They are creating a US$25 billion (19.5 billion euros) digital city in South Korea. New Songdo City will be nestled in the heart of Northeast Asia's economic region, 40 miles south of Seoul and will be built on 1,500-acres of reclaimed land on the Yellow Sea. This piece of land will then be connected to the Incheon International Airport via a bridge.

New Songdo City is seen as the world's largest ever private development project and most ambitious undertaking of its kind. The city has been designed around one thing: the people who will live and work here. The developers say that the people who live there will experience an unparalleled quality of life as technology, resources and innovation will all come together to create an ideal environment.

The aim of the city is to also create a dynamic, premier international business centre, which will be the new "Gateway to Northeast Asia". The new city hopes to encourage major corporations to relocate their regional offices to the area. The attraction and benefit to them, apart from this new development, is the fact that the South Korean Government has designated the area as a free economic zone offering tax breaks and other financial incentives.

The city will comprise of a 100-acre central park, international school, international hospital, an 8-floor ecotarium, a museum and US-style shopping malls amongst its many amenities. An off-shore wind farm will generate power to move sea water through the city's canal system. The convention center will comprise of eight large exhibition halls, meeting and seminar rooms, pre-function space, ballroom/ banquet halls, and food service facilities, and features an impressive vaulting roof.

The design of the center incorporates several sustainable features including natural ventilation and daylighting in the exhibition halls (during exhibit set-up), and a grey water system where sanitary waste is recovered, treated, and recycled for non-potable use. Songdo's architectural centrepiece will be the 65-story Northeast Asia Trade Tower, which will include offices, serviced apartments, and a 6-star hotel.

Gale Industries wants Songdo to become a premier address for the international community to locate their business and to raise a family. "Southeast Asia, Singapore and Hong Kong have that hub function. In northeast Asia, we are creating it here," said Stan Gale, Chairman of Gale International.
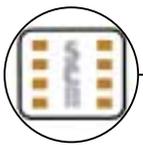
The city will boast the most advanced digital infrastructure imaginable, from blanket wireless Internet coverage and automated recycling to universal Smart Cards that can be used to pay bills, access medical records and open doors. Songdo will merge medical, business, residential and government data systems into a so-called ubiquitous, or "U" city, on a scale never seen before. There are smaller ubiquitous projects, the local term for a digital community, but nothing compares to Songdo.

Homes and offices will all have built-in computers that will collect data from swipe cards and sensors for the "U-life" management centre. It will be run by Songdo U-Life LLC, a joint venture between Songdo's US developer, Gale International, and LG Electronics subsidiary LG CNS, the creator of Songdo's digital backbone. "In America and Japan, some building companies use group control or group management, but in our country it's for a whole city," said Jang Choong-moo, Director of Strategy and New Business at Songdo U-Life.

The city will become the ultimate testing ground for services to track products and people with radio-frequency identification (RFID) chips, which is a technology facing resistance in other countries because of privacy concerns. Kim Kyoung Woo, a spokesman at the Ministry of Information and Communication, said South Koreans generally trust corporations with personal data and that "it's not a big issue" for the public. It is unclear exactly how the information will be protected, but Huh Jeong-wha, IT Director at Songdo U-Life, says residents will have to give permission before their data can be used.

Homes within the city will have a medical station to measure vital health signs like blood pressure and pulse. Traffic reports could be tailored for individuals whose computers could advise them. Schools and other buildings will have Smart Card readers. Parents could find out when their children have arrived at school. Parents can monitor their children using a chip in a mobile device, which will register each child's whereabouts. Researchers are also considering using RFID tagging for garbage disposal and recycling that could also be used to keep an inventory of office supplies, or even what's left in the fridge.

"The resident's Smart-Card based house key can be used to get on the subway, pay a parking meter, see a movie, borrow a free public bicycle and so on. It'll be anonymous, won't be linked to your identity, and if lost you can quickly cancel the card and reset your door locks," said John Kim, Vice President for Strategy at New Songdo City Development. However South Koreans should be wary of this new "Ubiquitous City" according to Liz McIntyre, who co-authored the book Spychips. "Songdo City's anonymous tracking infrastructure could quickly be turned to new purposes, and its people could become virtual prisoners of their own technological creations," said McIntyre.

But with construction well under way, strong interest from multinationals, 2,000 homes already sold for an average of $500,000 a piece and another 63,000 still available, John B. Hynes III, CEO of Gale International sees the future of the city as very optimistic "New Songdo City appears to have secured a place in South Korea's future," he said.

Once completed in 2014, the city's infrastructure will become a test bed for new technologies, and the city itself will exemplify a digital way of life, which is already being dubbed as "U-life". "U-life will soon become its own brand, its own lifestyle," Mr John Kim said.

Merry Christmas and a Happy New Year