News • Smart Card News • Smart Card News • Smart Card News • Smart Card News • Smart Card News
mart Card News • Smart Card News • Smart Card News • Smart Card News • Smart Card News • Smart Ca
ews • Smart Card News • Smart Card News • Smart Card News • Smart Card News • Smart Card News
mart Card News • Smart Card News • Sm   rd News • Smart Card News • Smart Ca
ews • Smart Card News • Smart Card N   rt Card News • Smart Card News • Smart C
mart Card News • Smart Card News • Sm   rd News • Smart Card News • Smart C

Smart Card News

Smart Cards, SIM, Biometrics and RFID

www.smartcard.co.uk

03 • Edinburgh to Become a Smart City

05 • LEGIC All-in-One-Card Solution

06 • Parcxmart Platform Goes Live

05 • Travel Smart Cards for Devon CC

This Month's Lead Story

Edinburgh to Become a Smart City

In This Issue

Regular Features

World News In Brief

Featured Articles

www.smartcard.co.uk

Dear Subscribers,

Spring at last and ID theft is mushrooming. This, we are told, is the crime of the decade with 1 in 4 adults in the UK knowing someone who has or have had their ID stolen. We are told we must preserve our identity security by destroying our bank details, household bills or anything that will help a criminal to take on our identity. How well are the organisations we deal with looking after our personal information? Only this month the Bank of America lost, misplaced or even had stolen, they aren't sure, around 1.2 million government cardholder accounts. Apparently the computer tapes holding the cardholder information were being shipped by air to a backup data centre in December, when the tapes went missing. But don't worry, the bank are monitoring the accounts for any unusual activity, they regret any inconvenience and are concerned about customer privacy information. Let's hope the tapes turn up and Bank of America will not have to worry about 1.2 million stolen ID's.

Egg, the on-line bank has been distributing their PIN codes electronically over the web through an encrypted internet gateway. They claim this has saved them 50p for each PIN posted across this channel and has reduced fraud from mail interception.

London's 2.2 million Oyster cardholders will soon be able to pay for small items using their card just as they do in Hong Kong with the Octopus card. This is being compared to Mondex, the first electronic purse scheme launched in 1993, the Oyster card is a transport ticket card not a bank card and offers the cardholder the ability to make small payments. Mondex was really to early and the cardholder could not see a benefit over cash. The infrastructure was also not in place. This scheme is bound to be a success assuming they can get the security right,, it's just what the commuter wants.

Nokia has launched the first Near Field Communications (NFC) product for payment and ticketing in a NFC shell for their 3220 phone. The consumers payment information is stored in the contactless chip of the shell and all the consumer has to do is tap their phone on a POS device or ticket gate. At last we are seeing the phone as a wallet, something we have been advocating for some time, but for large memory SIM, the debate continues as to whether data should be stored in the handset or the SIM. This month Dr. David Everett explores problems with Chip and PIN on page 16.

22

Edinburgh to Become a Smart City

Edinburgh in Scotland is to become a Smart City by offering its citizens a Smart Card that will allow them access to a range of services provided by many different suppliers throughout the city. This new card is called the One Edinburgh Smart Card and was commissioned by Edinburgh council in partnership with Edinburgh Leisure, Edinburgh Young Scot and Lothian Buses.

The One Edinburgh City Card Project has been delivered by Edinburgh council and British Telecom (BT). The project involves using a Java contactless and dual interface Smart Card, supplied by Trub AG, as a multi application card allowing the One Edinburgh Card to be used for all services within the city. Thus eliminating the need for a multitude of different cards all for different needs. The One Edinburgh Card aims to be used for cashless school meals and vending machines, school registration, reward schemes, leisure activity membership, library membership, concessionary travel, proof of age and to be used on the city's Lothian Buses as GOSmart Tickets.

The project is being piloted in 22 state secondary schools throughout Edinburgh and will initially be used for cashless school dinners. The Project is part of the Council's Smart City programme to change the way they organise and deliver services. A statement by Edinburgh Council said "Our partnership with BT helps us develop Edinburgh as a Smart City. Using new information and communications technology (ICT) we are changing our systems, procedures and service delivery.

This vision includes 'joining up' our own services and working with other agencies and organisations in the city. The project is funded by the Scottish Executive and through the Smart City Partnership between the City of Edinburgh Council and BT.

To make this project work the cardholders' details and photographs will have to be stored in a database and in a world where paranoia is ripe and people feel that big brother is watching, this is one issue the project has had to address. The city council has stated that they will only use this information to provide the services that are requested and for reproduction or replacement of existing cards. For each service that a citizen of Edinburgh decides to use, the organisation/company providing that service will only be able to use the information on the database to deliver their particular service. The Council is restricted and has to abide by the guidelines laid out in the Data Protection Act 1998

BT assigned Trub to deliver the project Smart Cards and services. Trub manufactured 33,000 printed long-life "dual-interface" cards made of PVC including holgrams. The Integrated chip technology is based on the Philips P8RF5016 chip and IBM Jcop30 JavaCard operating system. Trub is supplying around 50,000 dual-interface cards and is guaranteeing them for a 4-year life-time. Trub is also supplying the outsourced process for the graphical card personalisation (photo, text) as well as the electronic card preparation/personalisation. Not only the loading of keys but also the installation of applets and Mifare initialisation is fulfilled in the personalisation process.

Dr.David Everett of the Smart Card Group commented "The Edinburgh choice of technology shows a lot of forward thinking in that they can handle simple transport concessions with the Mifare part of the card, while the java card domain opens up an a hole host of applications with the potential of using public key cryptography". The One Edinburgh City Card Project is still in its pilot stages and the Smart Card technology still has to be tested so it may still be some time before Edinburgh's citizens are able to use the One card for their everyday lives in the city.

In conclusion Edinburgh council stated "After the pilot, we aim to expand what the Smart Card can be used for. This will include a wide range of services not just Council ones. We will be working with different companies and organisations to develop the Smart Card over a period of time time."

Smart Cards

New Standard for PIV Smart Cards

The U.S. Commerce Secretary Carlos M. Gutierrez has announced that a new standard for Smart Card based identification methods has been developed. The Commerce Department National Institute of Standards and Technology (NIST) computer security specialists worked with the Office of Management and Budget (OMB), the Office of Science and Technology Policy, the Departments of Defense, State, Justice and Homeland Security in addition to the private sector to develop the new standard, known as Federal Information Processing Standard (FIPS) 201, Personal Identity Verification (PIV) of Federal Employees and Contractors.

This new PIV Smart Card standard specifies technical and operational requirement for the Personal Identity Verification standard, describing the minimum requirements to meet the directive and describing the process to prove an individual's identity. The standard applies to identification cards issued to all federal government departments and agencies and their employees and contractors requiring access to federal facilities and systems.

Physical Access Council Created

Smart Card government and industry leaders are forming a new Physical Access Council, created by the Smart Card Alliance as organisations worldwide implement new access control systems to improve security and more accurately verify the identity of individuals seeking access to physical facilities. The Physical Access Council is managed by a combined government/industry steering committee. Current steering committee members are: AMAG Technology; Axalto; Integrated Engineering; Northrop Grumman Corporation; MAXIMUS; Philips; SCM Microsystems, and the U.S. Department of Homeland Security.

Chip&SIM

Chip&SIM, a new Chip and PIN solution from Thyron Systems, has now received full accreditation from a total of four UK acquiring banks. To date, Barclays Business, RBoS/Streamline, euroConex (Alliance and Leicester) and now HSBC have all tested and accredited the "Chip&SIM" hardware and software for use in a number of easy to deliver and flexible Chip and PIN scenarios.

At the heart of the "Chip&SIM" solution lies Thyron's PayCell MPT500 payment terminal.

Mobile Suica Service Launched

East Japan Railway has joined forces with NTT DoCoMo and Sony to launch a new mobile Suica Smart Card service in January 2006. The partners will conduct a trial service beginning in March using pilot service-compatible handsets.

The new service will combine JR East's Suica Smart Card functions with DoCoMo i-mode mobile phones enabled by Sony's FeliCa Smart Card platform. IC chips for the service and service applications will be developed by FeliCa Networks, a joint venture established by the three companies. The Mobile Suica service will enable i-mode FeliCa handsets to be used as Suica cards.

A test of the service will begin this month using pilot i-mode FeliCa handsets. The service will allow users to check the fare balance, recharge e-money fares, and buy a commuter pass whenever and wherever from their handsets, as well as enjoying the basic Suica Smart Card functions. JR East plans on service expansion by making the service available for online shopping (by the second half of 2006) and for purchasing Shinkansen bullet train tickets (in fiscal 2007). More than 10 million Suica cards have been issued.

Union Secures EasyCard Deal

A consortium led by Cathay United Bank has announced it has outbid another consortium to secure the right to issue the multi-purpose MRT Easy-Card/credit card for three years. The Smart Card Union -- formed by Cathay United, Chinatrust Commercial Bank, Taishin International Bank and Taipei Fubon Bank -- won the bid by offering NT$412.5 million in royalties, a mere NT$2.5 million more than a bid led by rival Union Bank of Taiwan and Far Eastern International Bank. All four banks in the successful consortium are shareholders of Taipei Smart Card Corp, EasyCard's distributor.

The Smart Card Union expects to issue more than 2 million multi-purpose cards, which combine credit, e-wallet and transport pass features, over the next three years. The banks will share royalties jointly but pay for rebates individually depending on the number of cards issued.
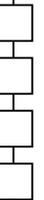
$21.8 Million Contract for Cubic

Cubic Transportation Systems Limited has received a contract valued at approximately US$21.8 million from Swedish transport operator Skanetrafiken for the design, delivery and implementation of the "Resekortet" Smart Card-based fare collection system. The new multi-modal system will connect bus and rail services in Skane, the largest county in southern Sweden.

Travel Smart Cards for Devon CC

Unicard is supporting Devon County Council's trial of smart school travel cards with a fully managed service based on the Unicard web-based card management system. 1200 pupils at four Devon schools and colleges have now been issued with smart cards containing details of their entitlement to travel on public transport.

SCB Access for MULTOS Cards

SCB Solutions and MAOSCO Ltd, the secretariat of the open industry consortium that governs the MULTOS specifications, have announced the availability of a new version of SCB Access for MULTOS cards. SCB Access is a solution for Secure Logon and Single Sign-On applications. A user can access a PC or an application by inserting a Smart Card and a PIN code. With SCB Access, user names and passwords are securely encrypted and stored on a Smart Card. User names and passwords are then submitted automatically to the appropriate applications. Users need to remember only one password to unlock their Smart Card. All the others can be forgotten; no more need for unsafe "stickies" to remember their passwords.

GlobalPlatform Updates SCMS

GlobalPlatform has published a revised version - v4.0 - of its Smart Card Management System (SCMS) Functional Requirements. The new version of the SCMS Functional Requirements, last published in 2002, reflects updates to benefit the entire GlobalPlatform Smart Card infrastructure for cards, devices and systems.

Specifically, it addresses Smart Card Management features required to pre-authorise part of the card management to a third party. This brings it into alignment with the GlobalPlatform Card Specification v2.1.1, which defines card requirements for delegate management.

LEGIC All-in-One-Card Solution

LEGIC Identsystems Ltd has released its latest LEGIC all-in-one-card solution which is a technology platform that allows the user to integrate a wide range of LEGIC all-in-one-card applications, such as access control, time & attendance, parking, cashless payments (e.g. cafeterias, vending machines), IT-access, e-tickets up to high security biometrical applications into a single identification credential.

New Student/Oyster Photocard

Novacroft, working on behalf of Transport for London (TfL), has launched a new scheme integrating TfL's Oyster card and Student Photocard. This will be the first combined Smart Card and photocard to be issued by TfL. Until now, the Student Photocard has been a dumb, plastic identity card that students were required to keep with their ticket when travelling. It is expected that during the initial stages of the scheme, over 100,000 Student/Oyster Photocards will be issued.

Students will be able to store ticket (including discount) information on their Student/Oyster Photocard, using it to travel at a reduced rate on London's public transport network. When the student finishes their studies the card can be used as a normal Oyster card.

SafesITe Integrates MyID

Intercede's MyID smart ID issuance and management software is fully integrated as part of Gemplus's SafesITe Corporate smart identity management system. The smart ID management software allows Gemplus customers to immediately start issuing and managing smart IDs. Intercede has also collaborated with RSA Security Inc. to supply its MyID Smart Card and Identity Management System to a prestigious European aerospace contractor.

Smart Card Ticketing System for NZ

The ERG Group has been selected as the preferred bidder to supply a contactless Smart Card ticketing solution for transport operators in Auckland and Wellington, New Zealand. ERG will be installing their ticketing equipment on 1,100 buses and ferries owned by Stagecoach New Zealand. The system is expected to be available to the public in the second half of 2005 and progressively expand in the first half of 2006.
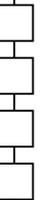
Pub Proof Card Reader

A new 'pub proof' PIN Pad with integrated card reader has been launched in the UK by Secure Retail, specifically to facilitate the roll-out of Chip and PIN in bar environments.

Fully EMV Level 1 compliant, with VISA PCI approval pending, the Sagem unit from Secure Retail has a water proof pin pad with flush fitting keys to facilitate cleaning. The card reader is built into the front of the unit to allow the customer to insert a card easily during a transaction. It includes drainage holes to ensure that any liquids spilt run away easily.

A built-in privacy shield helps reduce the risk of 'shoulder-surfing' for customers PIN numbers during a transaction. The unit is made of robust metal to improve resistance to physical attack. Tampering with the cabinets will disable the devices and make them non-operational. It also has a tamper-switch that will detect if the device is dismantled from the target equipment.

Parcxmart Platform Goes Live

The Parcxmart Smart Card payment platform has gone live in stores in the JapanTown section of San Jose, California. The participating Japantown merchants will now be able to distribute Parcxmart Cards, load value onto these cards using VeriFone Omni 3750 POS terminals, and then accept the cards for in-store purchases. The Parcxmart card can be used for on-street and off-street parking payments in participating cities once Parcxmart-compliant single and multi-space meters are installed.

Datacard Joins Multos Consortium

Datacard has joined the MULTOS Consortium and gains a seat in the Systems Forum and Business Advisory Group of the MULTOS standards body. As a Systems member, Datacard has voting rights over the further development of specifications relating to off-card data preparation and personalisation of MULTOS applications. Datacard will also have automatic rights to implement the recently released MULTOS step/one off-card specifications for key management and data preparation of EMV and other value added applications. MULTOS step/one is the entry level MULTOS platform for financial institutions migrating to EMV.

New ST Range of 32-bit Secure MCUs

STMicroelectronics has delivered its 10 millionth 32-bit Smart Card microcontroller (MCU) from its ST22 family. This is a new range of 32-bit devices based around the proprietary 32-bit SmartJ Java-accelerated Secure RISC core.

Lockheed Manage ID's Roll Out

Verified Identity Pass, Inc. (Verified ID), a company created to provide a nationally-recognised credential for people seeking expedited access through airport security checkpoints, has announced that Lockheed Martin Corporation will become Verified ID's lead systems integrator for the operation of all Verified ID installations, including enrollment, biometrics capture, and access control systems. Verified ID also announced that Lockheed Martin has acquired a minority stake in Verified ID.

Hypercom Orders OTI Reader

Hypercom Corporation has ordered its first commercial quantities of On Track Innovations Ltd's (OTI) contactless reader solutions. OTI's contactless readers will be integrated into Hypercom's Optimum T4100 multi-application and Optimum L4100 signature capture card payment terminals specifically designed to speed the check-out lines at retailers worldwide.

UBL launches 'Visa Chip Credit Card'

United Bank Limited (UBL) has launched its 'Visa Chip Credit Card' which has made them the first bank in Pakistani and South Asia to introduce such high-tech multipurpose cards in the country. The new card will have global acceptability in more than 22 million locations worldwide in 130 countries and in more than 12,000 outlets within Pakistan.

800,000 SIM Cards to Kuwait

Setec has announced they will deliver 800,000 SIM cards to Kuwaiti telecom operator Wataniya Telecom during 2005. The 64K PKI SIM card enables secure transactions using a mobile phone. The deal between Setec and Wataniya Telecom is one of the biggest PKI SIM orders in the world. Wataniya Telecom will upgrade all of its customers' SIM cards with the new Setec-manufactured SIM cards. As a result of this operation Wataniya Telecom's customers will have very powerful SIM cards that utilise the public key infrastructure (PKI).
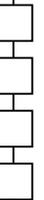
Setec has already delivered the first SIM cards to Kuwait in February and the deliveries will continue through summer 2005.

Smart Cards for Korean Resort

INSIDE Contactless, through its Korean partner, ID Future, has delivered several tens of thousands of PicoPass cards and Accesso readers to YANGJI Resorts for their RFID membership card system. YANGJI Resorts has implemented the RFID system in their ski resort, hotel and golf club to replace the current magnetic card with a contactless smart card for club members. The Smart Card comes with a dual protocol Picopass chip which enables YANGJI Resorts to provide its members with a range of services within the campus such as: access to free lift tickets within the ski resort, secure access to hotel rooms and resort facilities, discounts for purchases within the resort and access to the green and booking the course for Golf Club members.

Biometrics

Datastrip Gets Biometric Terminals

Shera Technology (Kunshan) Co. Ltd., an American run Electronic Manufacturing Service (EMS) provider in China, has announced an agreement to provide manufacturing services to Datastrip Group Inc. for its DSVII family of Biometric Smart Card Terminals. The DSVII-SC terminal is a handheld WindowsCE.NET device specifically designed to provide identity verification by reading contact and contactless chips on identification documents and fingerprints. It supports optional internal wireless communication for data and fingerprint transmission for identity search and verification against a back-end system. Datastrip has recently announced the addition of three new swipe-style models, DSVII-SW, DSVII-PS and DSVII-PA. These new readers add an automatic 600dpi swipe-style scanner.

FGS Secures Biometrics Rights

In its ongoing war against identity theft, FacePrint Global Solutions, Inc. has announced it has secured the exclusive North American licensing rights of a multi-functional Smart Card that, combined with FGS's unique e-DNA technology, will be available to a vast and growing market that includes law enforcement agencies, schools and motor vehicle departments.

Following an assessment of existing technologies, FGS has signed a 20-year, renewable deal with award-winning Smart Card creator Patrick Vassort of Switzerland to widely commercialise the product, known as the Icomsat Smart Card, a contactless card that features fingerprint identity.

FaceKey's New Agreement

FaceKey Corporation has expanded its current distribution agreement with Southwest Biometrics to include an equity based compensation package directly linked to a multi-million dollar revenue target mutually set by both companies. The addendum to the current agreement is exclusive to Southwest Biometrics because of the two companies' working history where they have been engaged in a distribution partnership throughout the progression of FaceKey's biometric products as well as the Company's confidence in Southwest to generate significant revenue through its expanding network of VAR's (Value Added Resellers).

Bioscrypt to Acquire Cognizance

Bioscrypt Inc has entered into an agreement to acquire all of the shares of Cognizance, a privately-held company headquartered in Dublin, California. The transaction is expected to close at the end of March. The initial consideration for this transaction to be paid at closing is US$7 million.

Near Field Communication

NFC Continues to Grow in Size

The Near Field Communication (NFC) Forum, a non-profit industry association promoting NFC technology, has announced that 18 more organisations from around the world have joined the group. The NFC Forum is a global standards development and advocacy group dedicated to advancing near field communication technology, educating the public about its benefits, and furthering its implementation around the world.

MasterCard International, Matsushita Electric Industrial Co., Ltd., Microsoft Corp., Motorola, NEC, Samsung, Texas Instruments and Visa International have become Sponsor Members, receiving seats on the Forum's Board of Directors. As a group, the Sponsor Members will represent the leading players in key industries in all the major regions of the world.
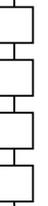
Additional organisations that have joined the NFC Forum in other membership categories include 3ALogics Inc., CETECOM Spain, Gemplus, Giesecke & Devrient, JCB Co. Ltd., Logitech, MeT Ltd., and Smart System Technologies, Inc.

Market in Figures

Axalto 2004 Full-Year Results

Following the 2004 revenue release of January 26, 2005, that reported full-year revenue of USD 960 million, an increase of 25% versus 2003 and a rise of 19% at constant exchange rates, Axalto reports its full-year results for the 2004 financial year ended 31 December 2004:

Axalto achieved a record year in 2004. Annual revenue increased by 25% compared to 2003, to USD 960.4 million. Within the Cards segment, which achieved revenue increase of 23%, all major product lines contributed to the growth, led by the strength of the Mobile Communication and Financial Services product lines and an excellent performance by the Public Sector and other products lines.

Europe, the Middle-East Africa now represents nearly one-fifth of Axalto's total revenue, at USD 187 million. Asia moved up 8% to USD 237 million, representing one-quarter of Axalto's revenue for the year. Axalto also confirmed their position in the Public Sector, Access and other product lines, with a 68% increase in microprocessor card shipments. Gross profit rose 32% compared with 2003, and gross margin improved by nearly 2 points, to 32.8% of sales, compared with 31.0% last year.

SuperCom's Financial Results

SuperCom Ltd has announced its unaudited financial results for the fourth quarter and fiscal year ended December 31, 2004. Revenues for the fourth quarter of 2004 were $3,453,000, an increase of 63% compared to $2,118,000 in the fourth quarter of 2003, and the Company's highest quarterly revenues since the 2nd quarter of 2002.

Net profit for the fourth quarter of 2004 was $451,000 compared to a net loss of $814,000 for the fourth quarter of 2003 and a loss of $663,000 for the third quarter of 2004. Revenues for the fiscal year ended December 31, 2004 were $7,344,000, an increase of 2% compared to $7,244,000 for fiscal 2003. Net loss for 2004 was $1,872,000 compared to a net loss of $1,995,000.

NBS Reports 1st Quarter 2005 Results

NBS Technologies Inc. has announced its unaudited financial results for the first quarter ended December 31, 2004. For the first quarter ended December 31, 2004, the Company recorded a net loss of $2.3 million compared with net income of $1.4 million in the first quarter of fiscal 2004. Revenue for the quarter totalled $16.6 million, a decrease from $24.7 million reported in the first quarter of fiscal 2004.

ERG Achieves $15.9 Million Profit

ERG Group, has reported a net profit after tax of $15.9 million for the six months ended 31 December 2004. This result compares very favourably with the previous corresponding period, which showed a net loss after tax of $43.0 million.

Operating revenue for the period improved by 18% to $116.5 million, with the commencement of the successful delivery of several major contracted projects.

Radio Frequency Identification

RFID Market to Reach $7.26 Billion

A new market research report covering RFID from 2005 to 2015, researched by IDTechEx, reveals some surprising new disruptions. Mimicking the barcodes market, where the market for barcode labels grew then declined, the value of the RFID market will similarly peak before the annual numbers of tags sold peak.

The report reveals that the tagging of about 30 billion pallets and cases for military and retail mandates has slowed in pace due to a range of technical problems at previously little used UHF frequencies. This is however being resolved with 3.1 billion tags being used for pallets and cases in 2006.

Item level tagging (especially by pharmaceuticals) and tagging of baggage, animals, books, tickets and other non retail markets are strongly growing in value - in 2008 6.8 billion tags will be sold for such applications and 15.3 billion tags for pallets/cases, but the former tag value will be higher than that for pallets/cases.
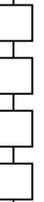
4 Million RFID Labels for Libraries

ASK has been selected by Bibliotheca, a European RFID library system provider, to supply C.label, a RFID smart paper label, to American and European public libraries. ASK labels are based on its core technology of a printed 13.56 Mhz silver ink antenna on paper and direct flip chip embedding process. ASK has supplied specific labels and readers to more than 20 French, Italian and German libraries over the last 4 year.

Tesco to Purchase RFID Readers

ADT Security Services, Inc, has signed a multi-year contract with Tesco UK as its exclusive supplier of Electronic Product Code (EPC) Radio Frequency Identification (RFID) readers and antennae. This contract is the largest publicly announced single order of EPC RFID readers, and it follows the successful completion of an RFID pilot program with Tesco. The first phase of the contract involves the provision of over 4,000 readers and 16,000 antennae by 2005 for the dock door.

Cubit Takes on the Sokymat Name

Sokymat has acquired Cubit Electronics GmbH, and will change its name to Sokymat GmbH. The synergies generated by combining the commercial and technical expertise of both Sokymat and former Cubit will strengthen Sokymat's role within the highly competitive RFID market.

UPM Rafsec New Beijing Office

UPM Rafsec is opening a new sales office in Beijing, China, to strategically position itself at the core of the world's promising embryonic RFID market. Also Hong Liu joined the new UPM Rafsec office in Beijing as the Business Development Manager for China. He will report to Edward Lu, UPM Rafsec Business Development Director for Asia.

NEC Launchs RFID@NEC

NEC Solutions Asia Pacific Pte Ltd (NECSAP)has launched its RFID solutions called "RFID@NEC in Southeast Asia. The launch of RFID@NEC is in sync with Singapore's aspiration of being the leading regional logistics hub as envisioned by the Infocomm Development Authority of Singapore.

New VP for Gemplus's Keynectis

Gemplus has announced the nomination of Jacques Seneca, Executive Vice President, Research and Development and the Identity and Security Business Unit, Gemplus, to the board of Keynectis. Keynectis is developing services for applications such as digital identification using Smart Card e-passports and electronic national ID applications.

New Managing Director at HID

HID has announced that David Sullivan has been appointed to managing director of the Europe, Middle East and Africa (EMEA) region for HID Corporation Ltd effective March 1, 2005. He succeeds Spencer Hall who is retiring from the company in June of this year.

New VP/GM at Checkpoint

Checkpoint Systems, Inc., a provider of radio frequency-based product identification and shrink management solutions, has announced that Saleem Miyan has joined the company as Vice President and General Manager - Global RFID and Emerging Technologies, a new position. Mr. Miyan is based in Checkpoint's London office. Mr. Miyan will manage Checkpoint's global RFID efforts, overseeing the company's sales, marketing and product development teams in North America and Europe.

A New Board for Ingenico

The Ingenico Board of Directors have made the following appointments: Philippe Lazare, Director and permanent representative of the company Tayninh.; David Znaty, Non-Executive Director. ; Amedeo d'Angelo and Barry Thomson.

Rotation of Lead Director at Fargo

Fargo Electronics, Inc. has announced that Dr. Edward Bersoff has been appointed by the Board of Directors as the Lead Director for 2005/2006 in accordance with Fargo's Board of Director Guidelines.
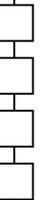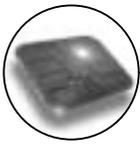
Secure End-to-end Transaction Methodology for the Citizen - Part 2

By Peter Tomlinson, Independant Consultant, Iosis

Peter Tomlinson

Last month's article outlined the concept of Secure End-to-end Transaction Methodology (SETM), which embraces secure messaging across the internet in conjunction with secure tokens (usually Smart Cards) and secure terminal technology. End-to-end methodology enables direct, encrypted communication between a Smart Card and a remote server, without any information appearing in the clear at an intermediate node such as a terminal. At the same time, the ubiquitous PC can still be used for the main part of the dialogue between the user and the remote service provider's server, because confidential information required to complete a transaction never appears in the clear in the PC.

Within SETM one type of such information, namely a cryptographic certificate, is no longer stored in the PC: it is generated only in a secure server and stored only in the secure token (smart card) held by the user. To implement SETM, a secure secondary device (a sub-terminal) is added as a peripheral to the PC. That device contains the card reader, display and keypad (and perhaps a biometric sensor, such as a fingerprint input device, and perhaps also a receipt printer). The sub-terminal acts as a router, ensuring that the card can communicate with both the user (card holder) and the server without risk of interference from the PC.

In Europe a secure on-line transaction method was first described some 6 years ago by the French banking community, and became the input material to a process that eventually produced two CEN/ISSS Workshop Agreements on the FINREAD set of specifications (found at www.finread.com). The most recent news is that ISO/IEC JTC1 SC17 has begun to develop an ISO/IEC standard based on the FINREAD work. Current ideas for SETM, however, add further security, derived from the OSCIE GIF modelling exercise that came out of the e-Europe Smart Cards programme. The intent in France was to use secure transaction methods for authorisation of on-line payment transactions (but for internal reasons within the global banking community they have not implemented it). For a secure bank debit transaction, once the user has agreed the transaction value (not classed as a secure item), the process is:1) The payment server sends the transaction authorisation request direct to the Smart Card in an end-to-end secure message - the request contains transaction value, name of payee, transaction reference; 2) The Smart Card sends the authorisation request only to the sub-terminal's display, together with a request for authorisation; 3) The user types the PIN number and Enter, which is sent only to the Smart Card in a secure message; 4) The Smart Card sends the transaction authorisation message direct to the server, again using a secure message

Thus the PIN never appears in the clear in the PC, and the same goes for the card number and associated security information. Optionally the sub-terminal may include a printer, on which a transaction confirmation can be printed once a completion message (again a secure message, but this time sent to the secure terminal) is received from the server. A little note about cost: in 1999 the French demonstrated a very low cost terminal, looking just like a pocket calculator with the addition of a Smart Card slot and a thin cable to the PC. Today, for the same cost, we should be able to source a small secure terminal with a sizeable graphics display and USB interface. Manufacturing cost should be under £10. In an unattended citizen service environment, particularly in the public sector, the primary secure transaction is identification and authentication. When the user is in an unattended environment, for example on-line from home or office, only the information available from the token (the card), plus anything collected securely via the secure sub-terminal (e.g. PIN or biometric), can be relied upon - this is eID and eAuthentication. Thus, once an SETM environment has been set up as a secure transport mechanism, the user's ID information and a related certificate will be sent by secure message directly from the smart card to the server (and ID data can be displayed on the secure sub-terminal for confirmation by the card holder). Note that sometimes the service providers use the term verification for this process, but authentication is the correct term when a secure transaction is to follow.

Technology
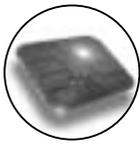
Authentication of the card holder is just part of creating a secure (authenticated) state that is required to persist throughout a user session in order to avoid the real user being replaced by another or being spoofed by software. There is, however, more that we can and must do, in order to prevent spoofing, cloning, and other interference. How can we be sure that spoofing is not occurring in the terminal? Indeed, how can we be sure that the terminal contains the necessary router configuration and is not a fraud that allows the PC to take over all communication with the card? Here is the recent contribution to the SETM concept: the key to security is not just an end user (card holder) certificate, but a certificate chain together with one or more PKIs, as well as the secure end-to-end messaging. Certificates attest to the authenticity of the card platform (silicon and OS), the on-card application, and the secure sub-terminal - and all must be checked on-line to the relevant PKIs before the transaction can be allowed to go ahead.

A basic indicator of the creation of a persistent authenticated state is the issue of a session certificate created by an authentication server. This can be checked by other servers - and each time that it is checked a basic function is to ensure that the card has not been removed from the terminal. As a further check, the user may be asked (via the Smart Card) to re-enter the PIN or provide the biometric again. Of course migrating to this method needs: 1) new development of software; 2) deployment of PKIs associated with databases of personal information about customers and citizens, and 3) a supply chain secured by certificates and PKIs (securing of the sub-terminals at the manufacturing stages, securing of card platforms and on-card applications). The SETM method needs a whole system view, not a component level view.. It also needs a realisation by public sector promoters of schemes (that will issue, indeed are issuing large numbers of Smart Cards into the hands of citizens) that security is not something to be added on later - instead it must pervade all design work. While the private sector may take a view that the cost of fraud prevention can be balanced against the fraud levels experienced if preventative measures are not taken, the public sector should not be allowed that luxury. And what about the big systems integrators in the supply chain? No bid at the moment, even though most of the building blocks have already been proved - but then the public sector is generally not an informed customer.

The North West Adopts Transport Smart Cards

New developments in the North West of England are giving a clear indication of the future of ticketing for Local Authorities, transport operators and customers. A "smart" way to access public services in Bolton, UK, has been introduced on a pilot basis in the north of the Borough. The Bolton "123 Card" enables people to use some of the borough's libraries, leisure centres and to travel on the 225 bus route between Bolton and Blackburn with just the one card. The card can also be used at similar facilities in Blackburn and Darwen. Up to three thousand volunteers are being recruited in the north of Bolton and south of Blackburn to trail the card. Introduced last November the card was officially launched in February 2005. Bolton, along with Blackburn and Darwen Council, is at the forefront of the drive by local authorities in introducing Smart Cards in their areas.

Their pilot is the first in the country to offer an interoperable card across a local authority/regional transport authority boundary with a transport provider. This is one of the first schemes to put an ITSO shell (application) onto a card alongside Local Authority applications. The Smart Card enables bus users to place a sum of money on to the card to be used to pay for bus fares. The card also electronically identifies if the customer is entitled to any travel concession and the ticket machine on the bus offers the correct ticket type, again improving the speed at which customers can board buses and speeding up the journey.

Bolton is not the only area in North West of England to be claiming a first, Cheshire County Council has become the first authority to receive Smart Card certification from ITSO following testing at Integri. The "Cheshire TravelCard" test samples were produced from pre-approved Mifare 4k cards, supplied by Magnadata, and were loaded with the ITSO shell and IPE2 by Cheshire on equipment supplied by ESP Systex. There are a large number of Local Authorities using Smart Cards for concessionary Travel in the UK but Cheshire County Council's scheme is so far the only multi-operator Travel Card offering passengers the choice of stored value cards or period passes. "This is an important step forward for ITSO" said Peter Soddart, Head of Marketing for ITSO, "and is an exciting addition to all that is happening in Smart Cards in the North West."

European Commission Paves Way for RFID Technologies

By Ewout Keuleers, Legal Advisor for the European IST SmartCities Project


Ewout Keuleers

The Data Protection expert group of the European Commission, the so-called Group 29, recently released a working document on RFID technology and privacy issues. Group 29 confirms that the use of low-cost Radio Frequency Identification technology (RFID) has substantial advantages in not only a number of sectors and industries, but also for individuals and public services, governments included. In addition to the more standard applications in the transport, distribution or retail sector, Group 29 underlines that RFID chips embedded in goods could also increase consumer safety.

It is clear that the wide spread implementation of RFID chips in consumer goods, such as razor blades, cars, identity cards, cell phones, etc., also triggers certain underlying privacy issues. Indeed, the ability to surreptitiously collect a variety of data all related to the same person; track individuals as they walk in public places (airports, train stations, stores); enhance profiles through the monitoring of consumer behaviour in stores; read the details of clothes and accessories worn and medicines carried by customers are all examples of uses of RFID technology that give rise to privacy concerns. For this reason, Group 29 urges manufacturers and deployers of RFID technology to design and implement technology that is in line with the legal EU privacy framework. This framework consists mainly out of two European directives. In the first place, the data protection Directive 95/46 sets out the general principles for the processing of personal data, notably the rights of the consumer-data subject. Secondly, this general regime is contemplated by a sector specific directive. Directive 2002/58 on electronic communications and privacy deals with particular issues such as the use of hidden identifiers, e.g., RFID tags, and location data.

1. Application of general data protection directive 95/46: Directive 95/46 on the processing of personal data is only relevant to the extent that the RFID generated information is personal data. Group 29 acknowledges that this is not always the case. In some cases, tag information is not combined with other identifying material, for example someone's photograph or name and address, or with a recurring reference number. However, one must be careful to come to this conclusion. Directive 95/46 defines "personal data" and "processing" in a very broad manner. Processing is basically "any operation or set of operations which is performed upon personal data", such as the collection, recording, organisation, storage, retrieval, consultation, use, disclosure by transmission, dissemination or destruction. According to article 2 (a) 'personal data' shall mean "any information relating to an identified or identifiable natural person." This also means that a person can be identified indirectly by reference to an identification number such as the one of the RFID tag. Moreover and to determine whether a person is identifiable or not, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person.

In contrast, the principles of protection do not apply to data rendered anonymous in such a way that the data subject is no longer identifiable. In contrast to the notion of personal data, the one of "anonymous data" should bestrictly interpreted and one must be aware that it may be very difficult to achieve true anonymous data. The Federal German Data protection Act, for instance, states that anonymous data shall only be information concerning personal or material circumstances that no longer or only with disproportionate amount of time, expense and labour , can be attributed to an identified or identifiable individual. It is thus sufficient that any person can make a link between the 'anonymous RFID tag' and a person, even indirectly, to render the Directive applicable. Eventually, one may not forget that RFID tags are designed to identify goods and/or persons. Similar to the use of internet cookies, or other hidden identifiers, even if the individual consumer is not immediately and directly identified at the item information level, he can be identified at an associative level because of the possibility of identifying him without difficulty via the large mass of information surrounding him or stored about him.
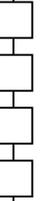
Once the use of RFID, or Electronic Product Codes (ECP), is considered as the processing of personal data the deployers, most likely to be considered as controllers, and RFID manufactures should pay attention to the legal data protection requirements.

2. Implications of the application of the general data protection directive: According to Group 29 it is not feasible to establish how all data protection requirements apply in each RFID scenario. It may be possible to give some general guidelines which data controllers can use and adapt in the light of the circumstances surrounding the data processing. Although it will be for the data controllers, e.g., deployers or distributors, to ensure the overall compliance with these requirements, Group 29 underlines that RFID manufacturers have a direct responsibility in ensuring that privacy compliant technology exists to help data controllers to carry out their obligations under the data protection Directive and to facilitate the exercise of the individual data subject's rights. In this regard, the same EU body already recommended in November 2000 that "the design and selection of data processing technologies, including hardware and software, shall conform to the objective of processing no or as less personal data as possible and shall facilitate the exercise of the data subject's rights". Furthermore, Directive 2002/58 clearly states that it "may be necessary to adopt measures requiring manufacturers of certain types of equipment used for electronic communications services, to construct their product in such a way as to incorporate safeguards to ensure that the personal data and privacy of the user and subscriber are protected".

Besides the general principles on data quality and the justifying legal grounds for data processing, notably the consent of the data subject, one must pay respect to the rights of the individual data subject. In particular and in order to allow the latter to exercise his rights, it is of predominant importance that the individual is informed and made aware of the existence of a RFID processing operation. When a public transport company, for instance, decides to implement a ticketing system based on RFID technology for periodical passes where the name and contact details of the holder of the pass is inserted into the tag. This could allow the organisation to know where an identified individual travels at all times. It is clear that when this is done without providing information to the travellers concerned, their privacy can be seriously threatened.

For this reason, data controllers, e.g., shop owners or manufactures of consumption goods, processing information through RFID technology should provide the data subject at least with their identity, the purposes of the processing, information on the recipients of the data and the existence of a right of access. Furthermore, it can also be recommended that information is given on the means to discard, disable or remove tags from the products, thus preventing them from disclosing further information. Eventually, one must be aware of the eminent risk that third parties shall use RFID tags for other purposes than the initial purpose determined by the data controller or for cross-profiling purposes. This re-routing of the initial purpose shall be easy to achieve when the RFID radio signal broadcasted by the RFID tag is not secured and can be read by third party readers. Directive 95/46/EC states that all data controllers must adopt appropriate technical and organisational measures to protect personal data against unauthorized disclosure or unauthorized access. In this view, the use of Privacy Enhancing Technology (PET), notably encryption algorithms, should be welcomed.

3. Legal regime for RFID based location data: In some cases and provided that sufficient RFID readers are present, the radio signal transmitted by the RFID tag can be used to localise an object, sometimes even a person. The vehicles of a sensitive money or nuclear transport, for instance, can be followed by tracking the tagged vehicles or bank notes. Furthermore, Group 29 refers to use of RFID tags in the pharmaceutical industry to make tracking of medicines easier and to prevent counterfeiting and loss derived from theft during transportation. By the same token, persons can be localised with the same effort as certain products. The sector specific Directive 2002/58 on privacy and electronic communications established a particular regime for the processing of location data, i.e., data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user. Although this regime was conceived for digital mobile public networks, its application to digital RFID communications should be considered. Article 9 of this Directive states that location data can only be processed for the provision of so-called value added services, e.g., the remote surveillance of vehicles, provided that the user or the subscriber have given their consent.

13

Furthermore and even in cases where an informed consent was obtained, users should have a simple means to temporarily deny the processing of location data. Important to note is that for the application of this regime, it is not required that certain data are considered personal data. In the end it must be clear that the wide spread implementation of RFID tags in our society can lead to certain privacy problems. Nevertheless, the debate between all interested parties is still underway and one must understand that RFID technology can be reconciled with the underlying privacy principles. In this view, the industry should take into account that it is in their proper interest to develop privacy-compliant products and that the public roll-out must be accompanied with a privacy compliancy test.

"Making a Difference" with RFID

In a recent Xtalks Webcast, "Making a Difference," with keynote speaker Simon Langford, Wal-Mart's manager of RFID strategy, a group of industry leaders talked about advancing RFID adoption for retailer compliance mandates and leveraging RFID implementation to foster internal process improvements. In his keynote presentation, Simon Langford, head of global RFID strategy for Wal-Mart Stores Inc., acknowledged that bar code technology transformed the way retailers and their suppliers do business, and predicted that RFID will "revolutionise" the industry in much the same way. Langford emphasised that while RFID adoption is a journey that is just beginning, he projects significant benefits for Wal-Mart customers (specifically in the form of zero out-of-stocks), suppliers, and the company itself.

Bob Cornick, Zebra Technologies' Vice President and General Manager of RFID, notes: "The momentum of RFID adoption and serious interest in the supply chain is very encouraging, especially when you consider how long it took for other transformative technologies to take hold. As a leading technology-savvy retailer, Wal-Mart is a catalyst." In charting the progress of RFID implementation at Wal-Mart, Langford explained that 104 Wal-Mart Stores, 36 Sam's Clubs and three distribution centers have already been installed with RFID receiving systems. By the middle of January, 57 suppliers had gone live - with Wal-Mart receiving more than 7,000 tagged pallets and 210,000 tagged cases. Langford added that today, more than 100 Wal-Mart suppliers are successfully complying with the RFID mandate and the next 200 suppliers are on target for 2006. Zebra currently works closely with a majority of the companies expected to comply with RFID industry mandates in 2005 and 2006.
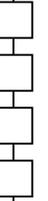
Events Diary

Feature Article • Events Diary

14

Let Your Finger do the Shopping

Patsy Everett, Managing Director, Smart Card News Limited
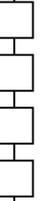
Patsy Everett

Pay By Touch was founded in 2002 and has IBM, Accenture and Discover Financial Services as its business partners. With 24 issued US patents and 12 pending US patents, these give the company exclusive coverage over "tokenless" biometric authentication of financial and loyalty transactions.Pay By Touch is a service that allows customers to pay for purchases using a method of finger scanning at the point-of-sale, eliminating the need to carry cards, cash, loyalty cards or a cheque book. Finger imaging links the individual to an electronic wallet which holds their financial and loyalty programme information.

The initial enrolment process takes about a minute as customers put their finger on a reader, enter a code and swipe the cards they want to use. The Pay By Touch finger scanning technology does not store actual fingerprints; instead it creates a set of geometric points that allow for a secure identity match at the point-of-sale.To access the service you register your credit and debit cards, your bank details and any loyalty cards you use. Enrolment is swift and free. This information is then stored and accessed only by placing your finger on a scanner at the point of sale. Pay By Touch has been running in the US for over 2 years and will very soon be available at the Oxford, Swindon and Gloucester Co-op.

As a biometric, fingerprints are generally seen as non-evasive and are certainly quick to register but one wonders what happens if you have had a weekend of gardening and damaged your fingers, find you have run out of fertiliser and need to purchase a bag using your finger! MasterCard and Visa have reached an agreement to share a common communications protocol for radio frequency-based contactless payments at the point of sale based on the MasterCard PayPass ISO/IEC14443 Implementation Specification and associated testing requirements.

This will ensure that cards and terminals supporting MasterCard and Visa contactless payment applications conform to the same communications protocol and undergo equivalent testing, thus ensuring interoperability across brands. Ensuring interoperability via the use of a common protocol for conducting contactless payments will benefit merchants, consumers and terminal vendors by providing a consistent experience at check-out across both payment brands. With a common protocol in place, merchants will also have the assurance that a single point of sale terminal may support multiple payment brands and will require less time for terminal programming and testing.

MasterCard PayPass is a "contactless" payment program that provides consumers with a simple way to pay. Using MasterCard PayPass, consumers simply "tap" their payment card, or alternative PayPass form factor, on a specially equipped merchant terminal, eliminating the need to swipe a card through a reader or fumble for cash and coins. This solution is ideal for quick payment environments where speed is essential, such as quick service restaurants, petrol stations, supermarkets and cinemas.Visa Wave uses a technology called Radio Frequency (RF) that is also used in a number of mass transit systems, including the "Touch 'n Go" service in Malaysia. Inside the card is a thin copper wire. This is an antenna that sends an RF signal to the terminal, transferring payment information quickly.

Of these two schemes I am concerned about relying on a fingerprint to make my payment. I am worried about how my template is stored and managed in the sytem. Using a biometric in this way dosen't seem that different to entering a password particularly since we now all know that fingerprints are transferable (as shown by Professor Matsumoto of Yokohama University) . Tap and go appeals as its fast, I've got used to using my phone so I carry it at all times and its fast but even then isn't this also single factor (1-F) authentication? Is there some contradiction with the need for Chip and PIN (2-F authentication), or am I missing something?

Technology
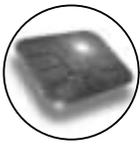
Has Chip & PIN been Chipped?

By Dr.David Everett, Chief Executive Officer, Smart Card Group Ltd

David Everet

Over the last couple of weeks the media has been having a go at Chip and PIN. It all started when APACS, the UK's Payments Association, released the fraud figures for 2004 on March 8th 2005. Apparently UK card fraud losses were up 20% to £504.8m in 2004. For reasons not entirely clear some of the broadsheet newspapers (e.g. The Times) put these losses down as a failure of the Chip and PIN initiative. It takes little analysis to see that on the contrary it is the emergence of Chip and PIN that is holding back the escalation of growth in card fraud. The fraudster knows that he is going to have to look elsewhere for his ill-gotten gains.

Card Not Present (CNP) is the major growth area for fraud (up 24% to £150.8m) and this of course includes the sleazy side of MOTO (Mail Order, Telephone Order) trading, the hackers guide to the galaxy. The Internet, which now carries 10% of all credit card spending also falls into this category.

Identity Theft is another major growth area, which is up 22% to £36.9m. Although you might argue this is a small proportion (just 7%) of the total fraud losses it is the growth rate that matters. This is probably the most frightening area in the whole financial fraud scenario. The technical security controls such as Chip and PIN are going to drive the criminal fraternity into these less protected areas and even worse, there are no simple solutions. Talk to anybody who has experienced Identity Theft and you will start to appreciate that this is going to be the big security problem for the next ten years or more. An electronic Identity Card issued on the basis of some effective registration process would be a good start but it's looking a bit doubtful in the UK right now with an election looming and little support among the cabinet ministers.

It is clear at this stage that chip and PIN do not address these two major fraud areas. Whether it works or not there will be no change in these growth rates by the introduction of such technology.

So where is the role of Chip and PIN? Counterfeit cards are the obvious area where in 2004 the fraud figure went up 17% to £129.7m and this of course is magnetic stripe cards. There are no reported cases of counterfeit chips.

There was also a rise in Lost and Stolen Cards which was up 2% to £114.4m in 2004. However together these two fraud elements account for nearly 50% of the total card fraud losses.

What the media failed to explain was that Chip and PIN is a migration process from magnetic stripe cards. Magnetic stripe cards are still accepted in many situations and this is likely to carry on for some time yet. No card issuer wants to loose his genuine customers so he has to accept the problems that always arise with any such migration path. The point here is that the growth is checked and it will just take a little time to see the impact, which surely nobody seriously doubts.

On Tuesday 15th March the London (TV) Program decided to raise the ante a bit more. The program discussed existing card frauds such as skimming and false ATMs (with a skimming front placed over a real machine). Just to make it more exciting they even had film of the police arresting suspicious people with a card copying kit in the boot of their card.
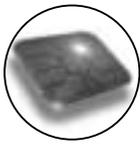
Several experts (Professor Ross Anderson and Mike Bond from Cambridge University) and an industry insider (?) made the case about the insecurity of the PIN on the grounds that bogus terminals are bound to appear. In that sense they are probably right but it misses the point that you are playing with two-factor authentication where both the Card (chip) and PIN are required for the authentication process.

It is unlikely that Smart Cards will ever be counterfeited in the way it is possible to duplicate magnetic stripe cards. Although various attacks have been made on Smart Cards in the laboratory the modern chip has long since moved out of the scope of any back bedroom attack even by industry experts who tend to turn their attention to chips at least one generation away from the current products.

Much was made of a hacking attack whereby the contents of the magnetic stripe from a chip card could be copied onto a white (magnetic stripe) card. The data on this card could be modified to change the flag that indicates whether or not there is a chip on the card so that the ATM machine wouldn't go looking for a chip. But it was also pointed out on the program, why go to that bother, you can always hit the chip with a hammer. In some terminals at the current time that would instigate a fall back to the magnetic stripe. These are all just problems with a user friendly migration strategy, the French had the same problem when they first issued Smart Cards.

In this case the hackers were smart enough to discover that a ball point pen was more than enough to break the chip and its easy enough to keep that in your pocket rather than the boot of the car. Eventually of course the fall back to magnetic stripe ceased and their card fraud came plummeting down.

So is the chip and PIN strategy inherently flawed? Well certainly not based on other countries such as France with 15 years experience under their belt.

GIGAntICTM SIMs

The debate over SIM memory versus phone memory continues in the mobile arena. Oberthur is manufacturing a new USIM card, a 128 Mbytes Flash card named GIGAntIC. The dual chip device has been developed by the Data Trust Division of M-Systems using their MegaSIMTM technology.

The chip uses an ARM-7 RISC 32 bit core (SC100 version) with the software development provided by Oberthur Card Systems. The chip has a public key co-processor module (M-Sytems bought out Fortress) and also has USB and MMC interfaces.

Ira Cohen, Vice President of Business Development at M-Systems, is confident about the take up by the Network Operators and cites the joint release of the GIGAntIC with Orange as the start of more to come.

So when is a SIM not a SIM. Oberthur seem to be keeping their options open here because you could probably follow the Secure MMC route or the USIM route. Which approach needs the 128 Mbyte of memory? Well that's where the debate starts and next month we are going to look at large memory SIMs, Secure MMC, and SD cards and the respective roles of the Network Operators and the phone manufaturers.

Kids in Care Get Top IT Security

By The Who Cares? Trust"

Banks, government bodies, insurance and pharmaceutical companies are the type of organisations who traditionally deploy best of breed, top IT security products to diminish the chances of breaches in security. So, it's a welcome change when you hear of young people being put to the top of the pile when it comes to being offered the best in IT security. CareZone, a website which aims to improve the lives of children in care, has tackled the importance of security and developed a website which offers children in care the opportunity to communicate online with those in a similar situation, social workers, doctors and other care professionals in a very secure, online environment. This new scheme for childrean was initally covered on its official launch by Smart Card News in February 2004. CareZone is now a year old and has been a huge success.

CareZone was set up by "The Who Cares? Trust", a charity dedicated to delivering services to children in care. They employed award wining design agency, Lightmaker, to build a site that would offer these children an exclusive zone in which to communicate with other children in care as well as other professionals. Lightmaker have an extensive amount of experience in producing highly innovative websites, and their work on the CareZone project employed the use of in-house technology, TMT 2005, which allows concurrent users on a website to share real-time, interactive experiences.

The site delivers exciting information in an imaginative and innovative way with site features including pages of advice, the opportunity to offer feedback, online support from counsellors and doctors and a secure place to communicate with care-workers and other professionals, from whichever care home the child happens to be.Within the site there is an engaging 3D chatroom where the kids can talk about problems such as bullying, being parted from siblings or the problems associated with frequently being moved from care home to care home. For children who are parted from their siblings it also provides a safe communication network where they know their emails won't be read by anyone else. Games, noticeboards and help with homework are just some of the other areas which are included on the site.

One of the key successes of the site has been the digital vault provided by Cyber-Ark, which gives the children a safe haven in which to store information. Children use the Vault to write their diaries, providing a safe place to record their thoughts and feelings. A sure winner, compared to the traditional physical diary, which most kids don't trust due to the risk of their diary being found and read by their peers or care staff.

The Digital Vault is normally used by banks or large institutions to store administrative passwords, however the CareZone site employs this technology as a "digital safe" for the children to store their birth certificates, photographs, education records, or personal education plans. All information they know they can't delete or have to share with others.

Whilst using the site, the kids have really got to grips with the digital safe, so much so, that it is now being used by the local authorities as a means of getting legal paperwork done, questionnaires and personal educational plans completed. Local authorities can email notification to the children that they have posted a document or information in their own, personal and private safe. The children then read the document, take any necessary action and return it into the safe. According to the local authorities this has saved time and money as paperwork can be sent out centrally and completed very quickly and securely.

18

In order for the CareZone site to be a success, "The Who Cares? Trust", together with Lightmaker had to ensure that the children's anonymity was protected at all times and that they would be assured of a high level of security, protection and privacy whilst using the site. Initially 9 local authorities subscribed to the site when it was first launched and this has quickly grown to 35 local authorities with 1,200 children online. It has become so popular that Lightmaker together with "The Who Cares? Trust" has approached Canadian and Dutch local authorities to develop the site for their children in care. As with all sensitive electronic data or information that has to be used remotely, there needed to be a secure method of access and a means of protecting and managing identities of all users - adult or child - at the initial point of logging on. Lightmaker and "The Who Cares Trust" worked with Diagonal Security, a leading provider of integrated, information security solutions, to find a user authentication solution that suited their requirements.

The chosen technology from RSA Security, RSA SecurID, means that the access method to the site mirrors that of a top bank or financial institution. All 1,200 children have an RSA token, and use this, together with a user name and pin number, to access the site. Lightmaker and The Who Cares? Trust chose the two factor authentication from RSA because of the ease of use, reliability and high levels of security.

Tokens can be posted from a central point, which has proved to be convenient, inexpensive and quick. The straightforward administration behind the allocation of the tokens, together with ongoing technical support provided by Diagonal Security, has strengthened "The Who Cares Trust" efforts to promote the programme to the local authorities. The local authorities have welcomed the RSA tokens as they can be reassigned very quickly if people lose them or no longer require them.

Security for the site doesn't stop at entry point, once the children are in, they must answer further questions in order to email, access the messageboard and chatrooms as well as all other features of CareZone. The security is even more secure around the Vault, as once again, to access the very "safe haven" the children must enter another password to get into their own, personal Vault.

Bryan Sayle, a director at Lightmaker, who has been involved at every stage of the CareZone development, says "Although it seems that we have created a site like a Fort Knox, with really strong access and encryption, to the users it is very simple and easy to use. At no point have we had any complaints from the children saying how difficult it is to access the site. They all naturally respect the security, look after their tokens and get on with it. It's their world and we want them to feel confident and safe with it." Jan Roszkowski - Director Carezone says "The site has been a great success with the children and the professionals in the care industry. There are 60,000 children currently in care in the UK and 480,000 adults supporting these children and so there is a real demand for a site specifically targeted at this group. We hope in time that many more children in care in the UK will have access to the site."

Everyone involved are looking forward to the future of Care-Zone and the opportunities it offers children in care. This development is leading the way in internet security and providing children in care with a much needed environment in which to communicate, learn and store information online.

www.thewhocarestrust.org.uk