Smart Card & Identity News • Smart Card & Identity News • Smart Card & Identity News • Smart Card News • Smart Card & Identity News • Smart Card & Identity News • Smart Card & Identity News • Smart Card News & Identity • Smart Card & Identity News • Smart Card News • Smart Card & Identity News • Smart Card & Identity News • Smart Card & Ide... News • Smart Card & Identity News • Smart Card & Identity News • Smart Card & Ide... News • Smart Card & Identity News • Smart Card & Identity News • Smart Card & Ide... News • Smart Card & Identity News • Smart Card & Identity News • Smart Card & Ide... News • Smart Card & Identity News • Smart Card & Identity News • Smart Card & Ide... News • Smart Card & Identity News • Smart
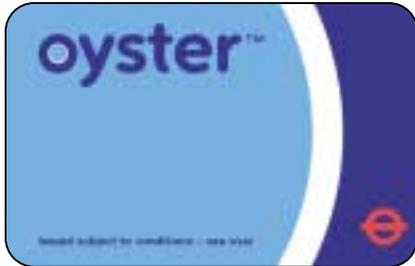
August 2007

Volume 16 • Number 08

Smart Card & Identity News

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

04 • More Outlets for Oyster in London

08 • Gemalto Reports 2nd Quarter Results

08 • Oberthur Card Systems Q2 2007 Sales

06 • MasterCard PayPass Pilot for Italy

This Month's Lead Story

New World Leader in e-Payment

Ingenico and Sagem Securité have recently entered into exclusive negotiations with the aim of combining their electronic payment solutions activities to create a global leader in the industry.

The proposed transaction concerns the payment terminals businesses of Sagem Securité, principally Sagem Monetel and Sagem Denmark and their respective subsidiaries.
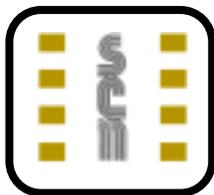
It would involve the issuance of new Ingenico shares to Sagem Securité which would become an important shareholder in Ingenico. As of today, these shares would represent 25% of the shares outstanding following the transaction's completion.

The companies have signed a non-binding Memorandum of Understanding and will now enter a period of exclusive negotiations and due diligence. Within the context of these negotiations, the project will be submitted to the employee representative bodies of the companies involved in the transaction for their opinion. Completion of the transaction, expected by year end, would be subject to Ingenico shareholder approval and approval by the relevant competition authorities. Ingenico will provide an update on the progress of the transaction when it releases its first-half results on 20 September 2007.

The combination of these two businesses would create a group with the best product mix, unique technological expertise, the most extensive sales network and leading market positions, and which would benefit from the Ingenico, Sagem and Monetel brands. Sagem Securité and Ingenico would further benefit from the potential for technological cooperation, particularly in the areas of biometric applications for payment solutions for Ingenico and the development of secure identification terminals for Sagem Securité.

Our Comments

There are more tales again of problems on the inter-net particularly phishing attacks where we are duped into revealing our account information to a bogus web-site. The thing that puzzles me is how does the aver-age person know? These attacks are sometimes very sophisticated and the content of the fraudulent email so convincing.

What hope can there be when the advances of technology are brought to bear against us less technical consumers? I can't help but wonder why the technology can't be applied to my advantage and it really comes down to the account manager, bank or whatever. They have a duty of care to iden-tify my authenticity when making instructions that change the state of my account, always down of course it never seems to go up. A basic biomet-rics test if you like. So how does a user name and password compare? Not very well because the hacker can play the games we have discussed and many more since the data is totally transferable. This is where 2-Factor authentication such as chip and PIN comes in as discussed in this month's issue by Jonathan Tuliani.

Although I am sobered by discussions that suggest we spot a missing mobile phone in 20 minutes and our credit card in 20 hours. Maybe its coming to a bank near you but it seems to me that they have a duty to ensure that I am on the other end of the instruction regardless of how I communicate with them and please not by the 20 minute discussion of asking me a host of impossible questions that the hacker can probably answer better than me. Can I use my Smart Card please?

Patsy

Contents

Regular Features

Industry Articles

Smart Card & Identity News

Sagem Securité intends to remain involved over the long term in the terminal payment sector through its security business and through its role as a shareholder in Ingenico. Sagem Securité would commit, in particular, to the customary standstill and lock-up provisions regarding its stake in Ingenico.

Sagem Securité's electronic payment terminals businesses had a compound annual growth rate of 28.3% from 2003 to 2006, significantly above the industry average. Sales for these activities in the first half 2007 were in excess of 83 million euros.

In 2006, sales were 120 million euros with an EBIT margin of 9.7%. Of the total sales, 50% were generated in Western Europe, 9% in Asia Pacific, 18% in the Americas and 23% in the Eastern Europe, the Middle East and Africa region. Jean-Paul Jainsky, Chief Executive Officer of Sagem Securité, commented: "The alliance with Ingenico would provide our activities with an even brighter future, creating a true leader in the field of secure transaction and payment solutions for many years to come."

Ingenico has recently published its sales for the first half of 2007 (unaudited) as 260.1 million euros, up 5.4% year on year at constant exchange rates, and has previously indicated that the operating margin for this period would show an improvement on the 7.3% EBIT margin for the second half of 2006.

Ingenico had sales of 506 million euros (526 million euros pro forma including the consolidation of Moneyline) in 2006 with an operating profit of 33.1 million euros and an EBIT margin of 6.5%. Philippe Lazare, Ingenico Chief Executive Officer, commented: "Bringing together the activities of Ingenico and Sagem Securité would enable the new group to better grasp opportunities, in both the payment terminals and services areas, as the sector undergoes significant technological and regulatory changes."

Events Diary

September 2007

13 - 15	SmartCards Expo 2007 - *New Delhi, India - www.indobase.com/events/details/smart-cards-expo.php*
17 - 20	Smart University - *Sophia Antipolis, France - www.smart-university.net*
18 - 19	RFID Europe 2007 - *Cambridge, UK - www.idtechex.com/rfideurope*
18 - 19	Geamalto One Forum - S*ophia Antipolis, French Riviera - www.strategiestm.com/conferences/gemaltoone/07*
19	Innovation in Public Services - *London, UK - www.ips2007.co.uk*
19 - 20	Training on Biometrics - Smart University - S*ophia Antipolis, French Riviera - www.e-smart.eu*
19 - 21	e-Smart 2007 - *Sophia Antipolis, French Riviera - www.e-smart.eu*
19 - 21	Cardex & IT Security 2007 - *Moscow, Russia - http://ite-expo.ru/en/conferences/cardex*
19 - 21	World e-ID - *Sophia Antipolis, French Riviera - www.worlde-id.eu*
24 - 27	ASIS International 2007 - *Nevada, USA - www.asisonline.org/seminar*
October 2007	
9 - 11	Smart Card Alliance Annual Conference 2007 - Smart Cards: The Future of Digital Transactions - *Marriott Long Wharf, Boston, USA*
24 - 25	Prepaid Cards Summit 2007 - *The Brewery, London - www.prepaidcardssummit.com*

Smart Cards

More Outlets for Oyster in London

Transport for London is to step up its efforts to persuade passengers to forego paper tickets in favour of Smart Cards by announcing plans to nearly double the number of places in London where Oysters can be bought or topped up. Oyster machines will be issued to up to 1,900 additional newsagents and other shops across London during the next 12 months. The Smart Cards are currently available at all Tube stations and more than 2,200 shops. This is the latest in a series of high profile campaigns to increase Oyster use and is expected to be followed by the withdrawal of paper tickets on London buses and the Underground. Fewer than 3% of single Tube and bus tickets are now bought with cash in London with nearly three-quarters of fares being paid for by Oyster.

6m Wasted on Unused Card System

A new Smart Card system to be adapted by Reykjavík City and Reykjavík Buses (Straetó bs.) in Iceland, to pay for bus fares, trips to the swimming pool and other services, may not be used after all. Developing the system has cost about ISK 0.5 billion (6.0 million euros). Reykjavík City Council had agreed in 2002 to adopt the cards and Straetó bought Smart Card readers. But the company that was in charge of developing the Smart Cards, went bankrupt. "Straetó is not supposed to be responsible for developing or operating such equipment," managing director of Straetó Reynir Jónsson told Fréttabladid. "If we can't reach an agreement with private parties who see business opportunities in this, we'll discard the system."

£1b for UK e-Borders Scheme

The government's electronic borders scheme to control illegal immigration into the UK is set to receive a cash injection in excess of £1 billion. About 29 million people have already been screened in trial schemes, which have included both air and sea passengers. The programme involves the submission of detailed traveller and crew data from airlines and ferry firms to a governmental database in order to track the movements of people on national and global watch lists. The UK prime minister Gordon Brown has announced details of a new counter-terrorism strategy which included the full electronic screening of all passengers travelling to the UK and the further rollout of biometric visas.

Vulnerability in US e-Passport

Lukas Grunwald, a computer security expert has managed to clone and manipulated the content of a RFID passport. In a statement Grunwald said that the new US electronic passport was "fundamentally insecure by design." He went on to say that the vulnerability in the US e-passport could enable a person "to crash the reading machine at an airport or to manipulate it in a nasty way so that forged passport could be accepted," This view by Grunwald is supported by many other technologists who believe the RFID technology in e-passports is not secure and cannot assure privacy.

In response to this Randy Vanderhoof, Executive Director of the Smart Card Alliance said, "I don't know if there is any credibility in this story." However he did point out that Grunwalk was using a German passport with a fingerprint biometric and that the US was not using fingerprint biometric in its e-passport, only a digital image. Paul Procter of Gartner said the vulnerability that Grunwald discovered is, like many exploits of RFID technology, was of "low probability but high impact." He went on to say that the problems with securing information on RFID passports are "real" and "well-known," but for the US government would not act unless they "caught someone cloning it in a nefarious way."

Smart Cards for Oz Govt Transactions

ANZ Bank has struck a deal with the Australian federal government which will see its business customers issued Smart Cards for making secure transactions with government departments. Under an arrangement struck between ANZ and the Department of Industry, Tourism and Resources (DITR), a select number of ANZ business customers will be piloting the use of Smart Cards that will contain an Iden-Trust digital certificate to authorise such government transactions as applying for grants, licences and permits; for signing and submitting government tenders and contracts; or even a transaction as simple as registering a business or company name.

The Smart Card pilot is a part of a wider federal government initiative called the VANguard program, aimed at providing validation and authentication solutions between government and industry in an attempt to streamline communications and cut red-tape. The program was announced with AU$29.6 million of funding in the 2006/07 budget and is expected to be complete within the next two years.

4
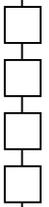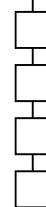
New NFC Tag Specifications

The NFC Forum has published four new tag type technical specifications. By standardising the tag types and formats these new specifications, announced the NFC Forum, is promoting interoperability across the NFC market, enabling low-cost volume production, and clearing a path to a global, cost-effective mass market. The operation specifications for the NFC Forum tag types, numbered 1-4, provide the technical information required to implement the reader/writer and associated control functionality of the NFC device, enabling interactions with the tag.

"It is essential to the adoption and growth of NFC technology that all NFC-enabled devices interoperate seamlessly and deliver a consistent user experience," said Christophe Duverne, Chairman, NFC Forum. Building on existing technology, the Forum's tags are based on the International Organization for Standardization (ISO) 14443 Type A and B standards and Sony's FeliCa. The four tag types are all based on existing contactless products and are available commercially.

Smart Cards Drive Asian EAC Market

Heightened concerns over security along with liberalisation and strong economic growth has been driving the Asia Pacific region toward more high-end electronic access control systems in recent years. The sheer size of the market combined with low penetration levels make for huge market potential and fewer biometrics regulatory issues in Asia Pacific as compared to other markets such as the United States and the United Kingdom are all expected to contribute to the future growth of electronic access control systems (EACS) in the region.

New analysis from Frost & Sullivan into the Electronic Access Control Systems Market in Selected APAC Countries, has revealed that revenues in this market totalled $0.50 billion in 2006, and are likely to reach $1.34 billion in 2013. Among EACS product types, keypads presently account for the highest revenue percent share in the EACS markets of countries examined in this study. However, this is likely to change by 2013, with some countries expected to leapfrog keypads and go to card-based or biometrics-based technologies that provide higher security. "On the other hand access cards, comprising proximity and contactless, are likely to experience increased adoption rates, and their share is expected to increase from 32.6% in 2008 to almost 60% by 2013.

Demand for biometrics is also likely to increase due to technology advancement, increasing concerns over security and the growing urgency to catch up with the western markets." observe Frost & Sullivan Analysts Parul Oswal and Navin Rajendra. Overall, market growth is expected to be driven primarily by cards-based systems and biometric applications. Offering competitive prices to end users is likely to be a key success factor due to increasing competition from lower cost providers, especially those from China and Taiwan.

Smart Cards Help Prevent Poverty

Smart identification cards (ICs) can provide a complete database for nations to not only keep track of the level of poverty but also facilitate in eradicating it. Prima Asia Pacific Consulting Sdn Bhd, a consulting firm has teamed up with Asia Pacific Card & System Sdn Bhd (APCS), who are one of the two largest manufacturers of Smart Cards in Malaysia. According to Prima the Langkawi International Dialogue (LID) 2007 conference will give a good platform for them to persuade developing nations to implement smart IC.

"The implementation of smart IC will complement the human capital agenda in developing nations, because with such a card they will have a stable database to further develop their nations," its Managing Director, Adznir Mokhtar. said "We want to encourage the use of Smart Cards in developing countries so that they can analyse their challenges through the data and come up with solutions to cut the rate of poverty,".

New Member at GlobalPlatform

American Banknote is the latest organisation to join the expanding membership ranks of GlobalPlatform, and the association's fifth new member since January 2007. A global supplier of secure documents, services and systems, American Banknote joins GlobalPlatform to support the development and promotion of the organisation's open Smart Card infrastructure, which it will utilise to enhance the deployment of Smart Card technology throughout the ABnote Group operating companies.

L-1 Acquires Two New Companies

L-1 Identity Solutions Inc has completed its $66 million acquisition of privately held McClendon Corp. McClendon shareholders received $33 million in cash and $33 million in L-1 stock as part of the acquisition. L-1 says McClendon will add about $20 million to its annual revenue.

L-1 Identity Solutions, Inc has also completed the acquisition of privately-held Advanced Concepts, Inc. Advanced Concepts shareholders will receive approximately $72.0 million in cash, subject to a post-closing adjustment, as well as the opportunity to earn up to an additional $6.0 million in consideration if key performance thresholds are attained.

Big Push for EMV Rollout in Australia

Visa and MasterCard are preparing to bankroll multimillion dollar marketing campaigns for the rollout of EMV payment card technology throughout Australia. Bruce Mansfield, Visa's GM for Australia and NZ said Visa and MasterCard were using a variety of lures, including contributions to marketing campaigns to encourage major banks to adopt the technology.

This month Westpac Banking Corporation will introduce EMV technology and the Commonwealth Bank of Australia is also expected to announce an EMV rollout when it releases annual results next month. ANZ has been issuing Smart Cards since 2003 and expects all its terminals will be chip ready by the end of this year. Westpac will begin upgrading its network in the next few months. The Australian Payments Clearing Association is considering an industry-wide adoption plan of EMV technology.

MasterCard PayPass Pilot for Italy

MasterCard Worldwide has announced the first MasterCard PayPass pilot programme in Italy, in partnership with Poste Italiane - business unit Banco Posta. By the end of 2007, Poste Italiane will launch a six to eight month pilot with its new cardholders, who will be offered a prepaid card with MasterCard PayPass technology - the PostePay Evolution MasterCard card.

Marco Siracusano, Marketing Director of Poste Italiane - business unit Banco Posta said: "Our common challenge is to widen the use of contactless technology and to make consumers more aware of the concrete benefits of Tap & Go. MasterCard is an important partner in our joint 'war on cash'. Facilitating the use of electronic cards will contribute to the further growth and development of the Italian economy."

Ingenico Buys Turkish Distributor

Ingenico has agreed to purchase PLANET, the Group's Turkish distributor, for a total consideration of 26 euros million.

PayWave for Spanish Cinemas

Visa Europe and La Caixa have launched the first contactless payment initiative in Spain using Visa's payWave technology. La Caixa have installed specially adapted terminals at Kinepolis cinema halls in Madrid to accept contactless card transactions using Visa payWave cards.

G&D Obtains ISO Certification

Giesecke & Devrient (G&D) has received ISO 9001 certification for its card-based operations in the US. The two facilities, located in Dulles, Virginia and Twinsburg, Ohio, join other G&D facilities with the accreditation and support the company's US businesses for USIM, payment, transit, government and identification cards.

Peter Hawkes Receives a Degree

Peter Hawkes, one of Smart Card News' editorial consultants, has received an honorary degree from the University at Kent. Peter Hawkes led the team pioneering the application of integrated circuits in telecommunications, initiating several projects on Smart Cards, biometric identification and secure network technology. He helped found the Association for Biometrics, serving as Chair for seven years, and has worked on the development of radio-frequency identification tags and contactless cards.

Biometrics

Brunei Get Biometric Passport

Brunei's Immigration and National Registration department has announced that Bruneians will soon be using biometric passports with the completion of a $7.1 million project by the month's end. The biometric passport project is a joint undertaking between a local company, Information Technology Protective Security Service (ITPSS), and German company Giesecke & Devrient (G&D). The chief executive officer of ITPSS, Shamsul Bahri Hj Kamis, said that the e-passport project is scheduled to be completed this August.

The biometric passport will be embedded with a 72-kilobyte chip, which will contain permanent data on the owner's facial and fingerprint images for identification. Under the contract, ITPSS will deploy and maintain the e-passport system, while G&D signed on for the production, supply and the secure delivery of biometric passport services.

Concerns Fuel Biometric Market

According to a report by Global Industry Analysts, the world Biometrics market is forecast to register a Compound Annaul Growth Rate (CAGR) in excess of 33% between 2000-2010 and cross the US$6.48 billion mark by 2010, with all major regions projected to exhibit growths in excess of 30%. Europe is forecast to emerge as the fastest region for Biometrics, with a CAGR of 35.66% over 2000-2010, while the US, with a share of 37.08% in 2010, will maintain its dominating position. Facial Recognition Technology market will outstrip all other biometric technologies with a CAGR of 53.72% over 2000-2010 and AFIS market, with an estimated share of 33.69% in 2006, will continue to be the largest segment.

India Launches PAN Cards

All the new income tax payers in India will soon begin to get biometric Permanent Account Number (PAN) cards with enhanced security features like fingerprints or retinal scans, aimed at checking duplicate cards and better tax compliance. When asked whether the date of launching biometric PANs could be October, Finance Minister P Chidambaram, at a press conference said "It could be."

Referring to the fate of current PAN card holders, Mr Chidambaram said, "They will be persuaded to switch over to biometric PAN cards in their own interest. Earlier PAN cards will, of course, remain valid." The Finance Ministry had earlier set up an internal group to finalise the norms for introduction of biometric PANs. The ministry is hoping to introduce iris-based biometric PANs to all new applicants once the present data about PAN cards is updated.

New Association for Biometrics

Intellect, the UK trade association for the technology industries, has launched a new working group - the Intellect Association for Biometrics. The group will aim to ensure that both policy makers and the technology industry are fully informed and able to address this biometrics market in a cohesive and consultative way.

It incorporates the former International Association for Biometrics and is Intellect's first specific biometric group. Companies joining the group will benefit from sharing expertise, information and ideas between the biometrics industry and external stakeholders, including the government. Intellect will also strive to encourage growth of the market and promote consumer education on their behalf.

New CRI Power Analysis Training

Cryptography Research, Inc. (CRI) has announced the availability of test equipment and a training program on power analysis attacks for FIPS 140-3 validation laboratories and product vendors. "As governments increasingly rely on devices such as Smart Cards, electronic passports, and mobile communication systems, it is critical that data and keys be protected with effective security and tamper resistance," said Paul Kocher, president and chief scientist at Cryptography Research.

Siemens & Fujitsu Collaborate

Siemens IT Solutions and Services and Fujitsu Limited have collaborated in a bid to expand the market for the PalmSecure palm vein authentication system developed by Fujitsu in combination with Siemens' biometric software "ID Center". Siemens IT Solutions and Services and Fujitsu have combined their technologies to develop a new biometric IT solution for personal recognition using palm vein scanning.

SafeSign for Wing Lung Bank

Thales has announced that Wing Lung Bank, one of the oldest and most established Chinese banks in Hong Kong, has deployed Thales's SafeSign to enable token-based two-factor authentication for its retail e-banking customers. As one of the first local banks in Hong Kong to deploy token-based two-factor authentication, Wing Lung Bank now meets the Hong Kong Monetary Authority directive which states that single-factor authentication for high-risk transactions is no longer adequate in the face of rising online security threats.

ACI Remedies ID Theft for Banks

ACI Worldwide has announced that it has signed 11 deals in the Europe, Middle East and Africa region (EMEA) over the last twelve months, bringing the total number of ACI Proactive Risk Manager customers to more than 120 worldwide. With fraud on the rise, the number of customers using ACI's comprehensive fraud detection solution has grown more than 60% during the past three years, making it one of the company's fastest selling products. The software now monitors more than 1.8 billion transactions every day for banks worldwide, including Alliance & Leicester, National Australia Bank, BNP Paribas, Fortis, CIBC and ING Direct.

7

World News in Brief

BenQ to Launch NFC-Enable Phone

BenQ plans to launch its first near field communication (NFC)-enabled phone, the T80, in the fourth quarter of this year, which would make the company the first Taiwan-based vendor to market a NFC-compliant phone, according to Hank Hung, general manager of BenQ Taiwan. By 2010, over 50% of handsets available in the market will come with NFC function, indicating the growth potential of NFC handsets, said Hung, citing data from ABI Research.

First Data Chooses Cardink

Cryptomathic has announced that First Data International has chosen to integrate Cryptomathic's CardInk EMV data preparation system with its VisionPLUS processing platform, for the issuing of EMV cards in Europe, the Middle East and Africa (EMEA). CardInk performs the data preparation (data generation and crypto key management) for Visa and MasterCard branded EMV cards. First Data will use the CardInk system to assist a large number of banks across the EMEA region to issue up to 50 million EMV cards annually.

Mifare Added to CardFocus

Sabadille Systems has announced the availability of version 9.0 of its CardFocus Photo ID and Visitor Management software to include support for Mifare contactless Smart Card encoding. This gives CardFocus users the power to encode embedded Mifare RFID chips when printing identity cards. The Mifare encoding functionality in CardFocus enables card issuers to define the contents of the card memory and/or to retrieve and store the serial number of the Mifare Classic 1KB cards.

EMV Certifications For T4200

Hypercom Corporation has announced recently that its new Optimum T4200 family of electronic payment terminals has received EMV Level 1 and 2 certifications. The new certifications add to the T4200's other security features, including PCI PED approval for secure PIN entry, and enhance the platform's built-in global capabilities such as integrated Smart Card readers and compliance with the European Union's RoHS requirements for hazardous substances. The Optimum T4200 platform has also gained approval under MasterCard Worldwide's Payment Terminal Security Program, established to ensure that IP and wireless-based transactions meet the highest levels of security.

MicroRead for KTF NFC Project

Inside Contactless has announced that its MicroRead, NFC chip, has been selected to equip all mobile phones and devices involved in KTF's NFC mobile payment project.

Financial Figures

Gemalto Reports 2nd Quarter Results

Gemalto has announced its revenue for the quarter ended June 30, 2007. Total revenue for the second quarter of 2007 was 398 million euros, down by 6% at constant exchange rates (and by 10% at historical exchange rates). The decrease reflects mainly lower revenue in Mobile Communication and Public Telephony.

Oberthur Card Systems Q2 2007 Sales

Oberthur Card Systems have reported second quarter 2007 revenues of 144.2 million euros, 17.4% above the record of Q2 2006 and following a 10% growth in the first quarter. Sales for the semester amounted to 278.1million euros, a 13.7% increase year-on-year. During this quarter, microprocessor card deliveries grew by 57% compared to Q2 2006 to 90 million units, sustained by a strong demand in the two main business segments, Mobile & Payment. Year-to-date, deliveries were up 52% to 111.8 million units, highlighting the expected recovery in 2007.

ActivIdentity's 3rd Quarter Results

ActivIdentity Corporations revenues for the quarter ended June 30, 2007 were $16.3 million, compared to $12.9 million for the quarter ended June 30, 2006 and $14.9 million for the quarter ended March 31, 2007, representing year-over year revenue growth of 26% and a sequential quarterly growth of 9%. Net loss for the quarter ended June 30, 2007 was $2.7 million, compared to a net loss of $5.3 million for the three months ended June 30, 2006. Net loss for the quarter ended March 31, 2007 was $3.4 million.

Aladdin's 2nd Quarter Revenues

Aladdin Knowledge Systems Ltd has reported that their revenues for the second quarter of 2007 were a record $25.5 million, an increase of 22% from the $20.9 million reported for the same period in 2006. Enterprise Security revenues for the second quarter were a record $9.0 million, a 44% increase from the $6.2 million recorded in the same period in 2006.

World News in Brief

8

Revenues for the first six months of 2007 were $50.6 million, an increase of 16% from the $43.7 million recorded in the first half of 2006.

AuthenTec's 2nd Quarter Results

AuthenTec's revenue for the second quarter of 2007 reached a record $12.3 million, up 51% from the second quarter of 2006 and 32% sequentially from the first quarter of 2007.

Precise Releases Interim Report

Precise Biometrics Interim Report for January - June 2007 shows the group's net sales amounted to SEK 11.3 million and for the second quarter SEK 5.4 million. The group's income for the interim period amounted to SEK - 18.1 million and for the second quarter SEK -8.8 million. During this period Precise Biometrics won the procurement for the Portuguese national identity card. This is the first ID card order in Europe, which is based on a Precise Match-on-Card solution, and a total of 14 million licenses will be rolled out.

VASCO Reports 2nd Quarter Results

VASCO Data Security International's revenues for the second quarter of 2007 increased 75% to $32.4 million from $18.5 million for the second quarter in 2006 and, for the first six months of 2007, increased 83% to $58.8 million from $32.2 million for the first six months in 2006. Net income for the second quarter of 2007 was $6.9 million, an increase of $3.8 million or 126% from $3.0 million. Net income for the first six months of 2007 was $11.8 million, an increase of $7.6 million or 181% from $4.2 million.

LaserCard's 1st Quarter 2008 Results

LaserCard Corporation's revenues for the first quarter of fiscal 2008 were $7.9 million, compared with $9.2 million in the prior quarter and $10.6 million in the same quarter a year ago. The net loss for the first quarter of fiscal 2008 was $2.4 million, compared with a net loss of $6.9 million. In the same quarter a year ago the net income was $0.2 million.

Cubic's 3rd Quarter Results

Cubic Corporation's sales for the third fiscal quarter were $233.7 million compared to $214.9 million last year, an increase of 9%. Net income increased 87% to $11.2 million from $6.0 million in the same quarter last year. Operating income for the third fiscal quarter was $16.6 million compared to $10.3 million in the third quarter last year.

HID Appoints New System Architect

HID Global has announced that Dr. Scott Guthery has joined the company in the role of System Architect, in charge of leading the formulation and development of secure identity-based products and services. In this newly created position, he will report to Dr. Tam Hulusi, Executive Vice President, HID Global.

SCM Microsystems Names New CEO

SCM Microsystems has appointed Felix Marx as Chief Executive Officer, effective November 1, 2007. Mr. Marx will be based at the Company's headquarters in Ismaning, Germany and will also be Managing Director of the Company's German subsidiary, SCM Microsystems GmbH.

Ingenico Appoints New Group CEO

Ingenico SA has appointed Philippe Lazare as Chief Executive Officer of the Group. He succeeds Amedeo d'Angelo who has overseen the successful turnaround of the Group.

VeriFone Terminates of Executive VP

VeriFone Holdings, Inc has announced that it has terminated the employment of William G. Atkinson, Executive Vice President, effective immediately; based upon information discovered by management that Atkinson had been soliciting VeriFone employees to join a competitor.

Pay By Touch Appoints New CFO

Pay By Touch has announced that Robert M. Sigler joins the company as CFO.

Infineon Terminates CFO Contract

The Supervisory Board of Infineon Technologies have released Rüdiger A. Günther, Chief Financial Officer (CFO) and Labor Director, from his positions. He has been replaced by Peter J. Fischl who was their original CFO before Mr Günther.

New Chairman at SIMalliance

SIMalliance has announced that Michel Canitrot has been elected Chairman of the new elected Board of SIMalliance.

World News in Brief

GlobalPlatform: Enhancing Today's Smart Card Infrastructure to Meet Future Requirements

**By Kevin Gillick, Executive Director, GlobalPlatform**

Kevin Gillick

The Advantages of Open Smart Card Specifications - Eight years of strong industry collaboration within GlobalPlatform's technical committees, have resulted in vast and significant advances for the Smart Card industry. Indeed, member collaboration has made an incontrovertible contribution to the technical evolution and growth of the industry worldwide, thanks to broad market acceptance of GlobalPlatform's interoperable specifications for the entire Smart Card infrastructure, encompassing Smart Cards, Smart Card readers and their associated back-end systems.

Since its early beginnings in 1999, GlobalPlatform has been governed by its membership, which today includes global hardware, chip and technology vendors, payment associations, integrators, telecommunications organisations and international government agencies. This stable membership base has sustained its strong business justification for the development of an open Smart Card infrastructure and has sharpened its focus exclusively on the technical needs and requirements of the industry. In doing so, members also enable the rapid development of GlobalPlatform-based solutions within their own organisations. So what drives this demand for an open, interoperable Smart Card platform and what benefits does such a platform offer? To answer this question, it must first be acknowledged that business models for Smart Card based programs are becoming more complex. In some instances, the model requires the formation of strategic partnerships among cross-sector organisations and, in many more cases requires greater flexibility from the outset to address future program demands relative to scale, post issuance capability and the ability to add further applications.

An interoperable platform, such as that made publicly available by GlobalPlatform, offers a secure yet adaptable Smart Card technology base that can respond to requirements that are unforeseen at the time of initial deployment. This gives issuers the reassurance that the infrastructure they have chosen will be able to adapt and grow as business conditions change - essentially 'future-proofing' the time and money invested in the development of the program. Open Smart Card specifications also allow issuers to take advantage of competitive multi-sourcing opportunities in the market place. Many global vendors offer open solutions and unlike proprietary offerings, solutions developed to GlobalPlatform Specifications are easily transferable, ensuring that issuers no longer need to be 'locked in' to a single-source commercial relationship. With so many benefits, including flexibility, scalability, interoperability, security, multi-sourcing opportunities and long term reassurance against program changes, an open platform is the obvious choice for issuers wanting to secure the longevity of their Smart Card program and investment.

GlobalPlatform: A Membership Forum Addressing Industry Needs - GlobalPlatform was established by key players within the Smart Card industry to bring together organisations and end-users with an interest in creating a global interoperable infrastructure for single and multi-application Smart Cards. GlobalPlatform's role was then - and remains to this day - to develop, maintain and promote common specifications for Smart Cards, devices and systems through member collaboration, ensuring that the demands and requirements of the wider industry are accurately and fairly reflected. Acceptance of the organisation's technical specifications has grown consistently and significantly. As of December 2006 the organisation estimated that there were in excess of 110 million non-telecommunication GlobalPlatform Smart Cards in circulation worldwide and an additional 1.2 billion GSM cards utilising GlobalPlatform for Over-The-Air (OTA) application downloads. Forty known Smart Card programs, spanning the financial, ID/security, government, healthcare and mobile telecommunications markets, were deployed across Europe, Asia, Australia and the Americas, utilising a combination of GlobalPlatform card, device and systems technology.
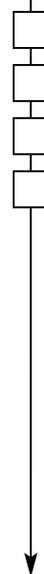
By the end of 2007, it is estimated that the volume of non telecommunication GlobalPlatform cards will rise to 150 million and, in addition to the increasing number of GSM cards utilising GlobalPlatform technology for OTA application downloads, 25 million GSM cards will apply the entire GlobalPlatform card framework for SIM applications. The number of GlobalPlatform Smart Card programs is also expected to increase by over 50% in the coming year.

Role and Priorities - In line with the organisation's role, GlobalPlatform is equally responsible for promoting its specifications as for developing and maintaining them. Educating on the benefits of open standards, sharing best practices and showcasing the many 'real-world' implementations remains a high priority for GlobalPlatform. Another key focus is to maintain GlobalPlatform's position at the forefront of the Smart Card sector, through innovation on a technical level. In recent months, this has been demonstrated through a number of milestone events:

❐ In March 2007, GlobalPlatform's card technology received world-wide validation when it was included in ISO/IEC 7816-13 international standard: commands for application management in a multi-application environment. As a result of this, GlobalPlatform has already started work towards incorporating the new ISO/IEC 7816-13 international standard into the GlobalPlatform Card Specification v2.2 and will be the first standards body to be fully compliant to the specification by the end of 2007. This will enable the organisation to provide card issuers with a simple migration path from the existing GlobalPlatform Specifications to the new ISO standard.

❐ In May 2007, the GlobalPlatform Card Specification v2.2 received recognition as a finalist in the Innovation category of the Card Technology Breakthrough Awards. The specification was acknowledged as one of the biggest advances in Smart Card technology in 2006, thanks to its success in extending the relevance and capabilities of GlobalPlatform's Card Specification to the government eID / ePassport and the mobile telecommunications sectors. GlobalPlatform accomplished this by addressing key functionality and security requests received from these industries, including Public Key Infrastructure (PKI) functionality and Over the Air (OTA) Card Content Management capabilities.

❐ Finally, GlobalPlatform successfully implemented its plan to collaborate with the Java Card Forum and Sun Microsystems on the upcoming release of GlobalPlatform Card Specification v3.0, expected in 1Q 08. This collaboration will ensure the specification is designed to support the Next Generation Java Cardplatform when released by Sun Microsystems next year.

GlobalPlatform's output is based on the work efforts of three dedicated technical committees populated and driven by the membership - the Card Committee, Device Committee and Systems Committee. Additionally GlobalPlatform has launched a Government Task Force, a Mobile Task Force and plans are underway for the creation of a third task force to focus on Systems Integration issues. The purpose of these strategic 'task force' groups is to focus on the direct link between GlobalPlatform Specifications and specific industry and application requirements with a bias towards large scale deployments, as prioritised by the GlobalPlatform membership. The current task forces accurately reflect two of GlobalPlatform's key technical priorities:

❐ **Mobile** - To address increasing industry convergence, particularly between the mobile and financial sectors, from the perspective of platform security and functionality.

❐ **Government** - To address the rapidly growing demand for Smart Card based public sector ID programs, and accommodate the specific security demands of this sector.

Creating an Open Platform for Mobile - GlobalPlatform has a rich history of successful collaboration with partner associations in the mobile telecommunications sector. The organisation has worked with the European Telecommunications Standards Institute (ETSI) since 1999 to standardise OTA application download and management of Smart Card applications. It has also engaged the Open Mobile Terminal Platform (OMTP) in efforts to standardise mobile device application provisioning and security. GlobalPlatform is also in the process of establishing a formal liaison with the Open Mobile Alliance (OMA) and the Near Field Communication (NFC) Forum. Through close collaborations with these groups and feedback obtained from GlobalPlatform's members operating within the mobile sector, they became aware of the mobile industry's requirement for standardised SIM solutions to ensure the mobile handset reaches its true potential as a universal multi-functional device.
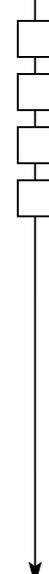
GlobalPlatform launched its Mobile Task Force in 2007 to actively contribute to the development of mobile telecommunications standards from an objective, cross-industry perspective. With the participation of 23 member companies, the task force's key aim is to educate the mobile sector on the benefits and added value of GlobalPlatform's interoperable technology, while expanding GlobalPlatform Card, Device and Systems Specifications to address specific requirements highlighted by the industry. GlobalPlatform has already begun work to align aspects of its Card and Device Specifications with current technology developments in the sector. Only recently, a White Paper titled 'GlobalPlatform's GPD/STIP Solution for Mobile Security' was published. This paper outlines the relevance of GlobalPlatform's device technology - the GPD/STIP Specifications and the Device Application Security Management (DASM) Specifications - to the global mobile telecoms sector. The key points can be summarised as follows:

❐ A GPD/STIP platform on a mobile phone handset offers interoperability, flexibility, reactivity and high security - a combination of requirements exclusively catered for by the GPD/STIP environment, yet essential for the successful deployment of multiple applications from different service providers, and with a varying degree of security rights. The mobile industry's key security concern is to have a proven means of securing, on a single handset, applications from different providers. GPD/STIP technology offers an open software platform to address this concern and, as such, could expedite the growth of this mobile 'multi-application' environment in a highly secure and standardised manner.

❐ The Device Application Security Management Specification, published by GlobalPlatform in July 2007, facilitates dynamic pre and post issuance application download to mobile terminals equipped with a GPD/STIP environment. This introduction of a standardised way to remotely download 'value added' secure services to mobile terminals will help service providers quickly, easily and securely introduce new and differentiated services to the market. From a card perspective, in the third quarter of 2007, GlobalPlatform is expected to announce an amendment to its Card Specification v2.2, which will enable application providers to confidentially and independently manage applications while using a third party's infrastructure. This will significantly benefit application providers that offer end user services exclusive of a mobile infrastructure, and will also enable mobile operators to establish a neutral infrastructure allowing approved application providers to manage their applets Over-The-Air (OTA) on an end-user's SIM.

Creating an Open Platform for Government e-ID - In 2006, GlobalPlatform established a Government task Force in response to the high rate of smart card adoption in government e-ID initiatives, and recognition that many of these implementations were based on GlobalPlatform technology. The aim of this group is to develop, document and deploy solutions to assist governments seeking to source open and interoperable components - on a non-discriminatory basis - from technology suppliers and integrators.

GlobalPlatform's Government Task Force is currently developing a White Paper titled ″The Value Proposition of GlobalPlatform for Government eID Initiatives', which is targeted to be published in late 2007. Further White Papers addressing very specific topics, including how the GlobalPlatform Specifications apply to unique government applications, such as the Personal Identity Verification (PIV) Card in the United States, are planned for the future. Their technical committees have also embraced the challenge to support government. One such example of their work is the latest release of the Messaging Specification, delivered by the Systems Committee, which extends the support of GlobalPlatform technology to government requirements for high-volume ID card issuance through internal or external service bureaus. GlobalPlatform expects to undertake more technical, educational and liaison activities in the government e-ID space in the future. As communities such as the Global Collaboration Forum and the Next Generation IC Card System Study Group (NICSS) come together to discuss Government eID, GlobalPlatform will be ready to ensure its contributions are aligned with regional requirements.

Plans for the Future - In addition to continuing the development and maintenance of GlobalPlatform's core specifications within the technical committees during the next year, GlobalPlatform will sharpen its focus on extending the capabilities of current specifications and developing new specifications to address specific industry and application needs. This important work will be completed by the members themselves, within the technical committees and the organisation's task force framework. GlobalPlatform's success is based on its 'member driven' approach to the technical development of Smart Card infrastructure. Its strategy for the forthcoming year is to further engage its members to drive the organisation deeper into markets and applications where demand for its open technology is high and on an accelerated growth curve.

12

Two-Factor Authentication: Short-Term Fix or Long-Term Solution?

By Jonathan Tuliani, UK Technical Director, Cryptomathic

Internet fraud is increasing. There are many factors that have contributed to the appeal of this crime, in particular, the variety and high value of transactions that are now completed online. In addition to the sizeable rewards, online fraudsters have another motivation: the global migration towards Chip and PIN payments. The adoption of EMV technology has significantly increased the protection delivered during point-of-sale transactions, driving financial crime towards the internet, and other card-not-present situations such as telephone purchases.

Jonathan Tuliani

The financial community is proactive in developing and implementing advanced measures to reduce unauthorised access to data, but with the chance to steal substantial sums, fraudsters have a clear incentive, and are continually evolving their techniques to infiltrate payment transaction systems and access secure funds.

Technology Vulnerabilities - Today's most damaging financial crimes are referred to as 'man-in-the-middle' and 'man-in-the-browser' attacks. These typically arise through the infestation of the customer's PC with a virus or 'Trojan', due to an operating system or browser vulnerability. Many of today's malicious spam emails aim to exploit such vulnerabilities and thus initiate an attack. The sophisticated nature of these threats means that a fraudster can intercept the communication connecting a customer and their bank, whilst remaining undetected by either party. They can then obtain authentication credentials such as user names and passwords, and even modify customer transactions in transit or initiate transactions of their own.

Banking Responsibilities - Traditionally the financial community was wary of authentication technology, believing that if the threats associated with internet banking were highlighted, and internet transactions became more complicated, it would discourage online activity. However, stringent security measures today are welcomed by internet users. Banks that offer sophisticated online protection are seen to add to the customer experience, offering peace of mind, and interestingly for banks, a new marketing and branding opportunity. Over recent years many security measures have been implemented, but today the financial community acknowledges that customers must be authenticated based on what they have (something which is hard to steal or counterfeit) and what they know (such as a password or pass phrase), together known as two-factor authentication (2FA). This benchmark has led to a significant and stable increase in the acceptance and deployment of 2FA methods globally.

Earlier this year, the protection provided by 2FA was questioned when press coverage revealed that Dutch bank ABN AMRO's authentication system had been compromised following a man-in-the-middle attack. This particular scam involved criminals sending an email to customers falsely claiming to represent the bank. If recipients opened the email attachment as requested, software was installed without their knowledge. Subsequently, whenever they banked online, their browser was re-directed to a fake website which was an exact replica of ABN AMRO. The attacker was then able to gather the customer's banking details and 2FA security passwords in real time, allowing a fraudulent transaction to take place without the bank or customer's knowledge, and, crucially, before the security passwords expired. The response from the industry was to highlight the vulnerabilities of 2FA and question its long-term viability within the financial community. This was quite an obvious reaction, yet one that demonstrated the market's limited understanding of what 2FA can offer. The reality is that security technology is also evolving to provide all involved in the transaction appropriate protection. In the case of 2FA, this progression is to not only authenticate the parties undertaking the transaction, but also the transaction details themselves.

Secure Security Solutions - The Chip Authentication Program (CAP), designed by MasterCard and sublicensed by VISA, is one such solution which has the ability to validate those involved in the exchange of funds while also authenticating the transaction taking place. The technology has another key benefit: it uses the cryptographic functions already available on an EMV card, allowing customers to re-use the Chip and PIN procedure which has become so familiar.

Industry Insight

13

The success of this approach is based around the introduction of an independent device, separate from the browser and its vulnerabilities. This PC-independence also allows the device to be used on other channels, for example telephone banking and telephone-order sales. Implementers of CAP issue customers with a Personal Card Reader (PCR), with its own keyboard and display, into which their existing EMV compliant debit or credit card is inserted. Similar to an ATM or point-of-sale, the user is asked to input their PIN, optionally followed by transaction details, such as an amount and payee reference number. Once these details are entered correctly, the PCR will generate and display a One-Time Password (OTP). This acts as the customer's electronic signature on the transaction, and must be submitted online to complete the transaction process. It is without doubt that a sophisticated hacker can 'steal' or even modify the OTP en route to the bank, but it is of no use to them-it cannot be used for any purpose other than authorising the transaction which the customer intended. Any attempt to modify the transaction details or use the OTP in a different context will be detected by the bank.

As its name suggests, the generated OTP can only be used once, to prevent so-called 'replay attacks'. The customer must therefore generate a new OTP for each transaction. This is enforced by the CAP Token Validation Service (CTVS), which alongside the PCR, is an equally important element of any CAP deployment. The CTVS's responsibility is to accept OTPs and check that they are valid for the transaction details given and the customer's card used. As such, the CTVS must be designed and implemented to the highest security standards, so that the appropriate controls are maintained on all data passing across its interfaces. It must also meet the high-volume, high availability demands of internet banking and payment processing systems, to ensure that the customer experience is never interrupted. Finally, it must integrate seamlessly into the existing card issuance and management systems-for example, any new card is issued must be accepted for OTP validation.

Short-term Fix or Long-term Solution? - The financial community realises that it is not an option to ignore security threats, particularly in an environment where internet crime is so active. e-Security technology has proven to be essential in achieving fraud reduction, while assisting banks in reassuring online customers that funds are protected. With the Federal Financial Institutions Examination Council (FFIEC) in the USA making enhanced authentication mandatory for all national financial organisations authorising the transfer of money to a third party's account, and the UK payment association APACS endorsing CAP, this technology will continue to be adopted and promoted by the industry.

However, the industry does need to be aware that the solutions implemented today are already under attack. Financial criminals are highly experienced, and new e-security protection measures present a challenge, not a threat, to their operations. Today's 2FA provides an effective defence against all but the most advanced attacks. As these attacks become more commonplace, the option to move from user authentication to transaction authentication offers a long-term defence. By deploying even simple 2FA solutions today, customers gain familiarity with the technology, easing acceptance of the more advanced 2FA solutions that must inevitably follow. To complement this approach, banks need to ensure that their chosen authentication technology offers long-term protection by investing in a scalable, flexible and secure infrastructure. By following industry guidelines, using interoperable solutions and adhering to standards, the industry will be able to follow the necessary technology evolution efficiently and cost-effectively. It will be this advancement from user to transaction authentication that will offer a true long-term defence against online financial crime.

Getting Serious About PCI Compliance

By RSA, The Security Division of EMC

If your organisation takes credit cards or does anything with card data, by now you have probably heard about the Payment Card Industry (PCI) Data Security Standard (DSS), which was originally introduced in 2004. Perhaps you have not paid much attention to PCI or have been slow to implement a compliance program. As of the end of last year, Visa reported that only 15-36% of even their highest-volume merchants were compliant. But that is set to change dramatically in 2007. Visa and MasterCard, the leaders in this effort, have both indicated that they will get more aggressive in enforcing the PCI standard this year. The PCI DSS was developed by the card brands, Visa International, MasterCard Worldwide, American Express, JCB, and Discover. Previously, each had its own program for data security such as the Visa Cardholder Information Security Program (CISP) and the MasterCard Site Data Protection Program (SDP).

The PCI DSS consolidated the individual brand's standards into one international industry standard for securing credit and debit card data. Any organisation that stores, processes or transmits card data is covered by PCI. This means all merchants that accept card payments; banks that manage the merchants and transactions; and service providers that process card data. And all of them have to start getting serious about PCI compliance. PCI applies to merchants that accept credit cards as well as "off-line" signature debit cards which are processed using the same networks as the credit card transactions. All merchants that accept credit and debit card payments are covered by the PCI standard, even when they do not transact business online.

No Silver Bullet for Compliance - To comply with PCI, merchants and service providers need to have a comprehensive security program in place, which includes policies, procedures and technology. No one technology or solution will make an organisation compliant. It requires a commitment to evaluating security controls, determining necessary improvements, implementing changes, and then continuing this cycle by assessing controls annually. But the effort will be well worth it. Non-compliance in the past has not resulted in major consequences for most organisations, even though Visa alone levied almost $5 million in fines in 2006.

Carrot and Stick Approach - These new fines are part of Visa's PCI Compliance Acceleration Program, which not only includes steeper fines but also incentives. Visa's tiered interchange rates-commissions paid for each credit card transaction-will be linked to PCI compliance. Merchants who do not comply with PCI face the prospect of increased rates. According to Visa, the impact will range from $250,000 to more than $20 million per year, depending on the merchant's qualifying volume. These are the kind of dollar values that will make many merchants take notice. Implementing security measures to comply with PCI will likely be much less expensive in the long run than paying higher rates.

Protecting the Payment Card System - Increased enforcement of PCI is motivated by the need to protect the integrity and trust of the whole payment card system. Over the last few years, there has been a flood of data breaches involving credit card data, including some cases in which literally millions of account numbers were compromised. If things continue, it could potentially put the whole system at risk. Consumers might start to feel that using a credit card off-line or online is not safe. The card brands would also like to fend off possible regulatory actions by governments worldwide. For example, because of well-publicised data breaches, the US Congress is considering enacting legislation specifically aimed at the protection of cardholder data. Another big motivator is reducing credit card fraud. Online fraud is approaching $3 billion USD a year in North America alone. Better security will help get this under control.

Benefits of PCI Compliance - For an individual organisation, the benefits of complying with PCI go beyond avoiding fines and increased interchange rates, although these alone are significant. Ultimately the objective of PCI is to protect card information from compromise. Organisations which implement better security measures as per the PCI standard reduce the risk of an actual breach occurring, which safeguards their reputation and customer relationships, and protects them from paying the costs of a breach. Companies with programs in place to protect card data also have the ability to extend these efforts throughout the organisation and protect other sensitive business, employee, partner and customer data. According to a study by the Ponemon Institute, if your organisation has a data breach, you could lose up to 60% of affected customers. Their findings indicated that over 40% of individuals affected by a data breach said that they might discontinue their relationship with the company and another 19% had already discontinued their relationship.

Breaches Are Costly - Costs are another reason why companies need to avoid breaches. The ChoicePoint case provides some hard data about just how costly a breach can be. The impact to their business was huge. Back in 2005, this leading data broker exposed information on about 145,000 Americans and was forced to make a disclosure to all those affected. The end result was a stream of headlines detailing the case, creating a wave of bad publicity for the company. Their direct costs were over $11 million (for communications; credit reports and monitoring; and legal fees). In addition, the sales losses were expected to be about $20 million for the year and their total market capitalisation dropped by $720 million right after the incident.

Trust Can Be an Important Differentiator - Consumers are becoming much more discerning and are selecting companies that will protect their information. A study by Privacy and American Business found that 60% of consumers had decided not to do business with a company because they were not sure how their personal information would be used.

Smart Cards in US Healthcare

By Smart Card Alliance Healthcare Council

The US healthcare market is poised to move from a paper world to an electronic one. In an era of managed care, specialised medicine, thin financial margins, identity fraud, difficult insurance claims, and government demand for secure, portable, and confidential patient information, the competitiveness of healthcare providers may depend on effective use of information technology (IT). However, increased computerisation, reliance on databases, and movement of sensitive patient information require strict controls to safeguard the security and confidentiality of healthcare records.

As the industry advances electronically, data protection is a key concern, fueled in part by legislation such as the Health Insurance Portability and Accountability Act (HIPAA). Current healthcare requires immediate and secure information access without compromised privacy. Smart Card technology represents a unique opportunity to provide healthcare solutions that combine secure information access and management with data mobility and patient privacy. Healthcare administrators are currently major consumers of paper and ink. Keeping patient records, submitting medical claims, making referrals, writing prescriptions, and booking appointments are typically manual processes. The few areas that are automated tend to operate independently of each other. Only a minority of physician practices store patient data electronically. Physicians and other healthcare professionals have a stubborn affinity for using paper-based media to collect and retain patient data.

The use of Smart Cards can reduce healthcare paperwork and protect patient records. The Smart Card can hold encrypted patient information and use a digital signature or a biometric template to reduce ambiguity about the cardholder's identity. The use of Smart Cards can also reduce the incidence of fraud in health benefit claims-a significant issue for the Federal government. And while HIPAA does not call for the use of specific technologies, it is likely that many healthcare enterprises will choose Smart Card based solutions because of their ability to support secure data handling and reduce fraud. Smart Card technology can also improve the healthcare insurance process. Currently, eligibility verification and claims processing are too often characterised by redundant information collection, multiple reimbursement forms and lengthy delays. Paper-based manual processes greatly increase the risk of human error which results in significant avoidable costs to insurers, national health agencies, and healthcare providers. Too often, these processes result in significant delays in referral, treatment, and reimbursement for insured patients.

Smart Cards can provide clean data for eligibility verification and claims processing. They not only can prevent administrative errors and streamline the payment process, they can also prevent medical errors that arise when one practitioner doesn't know what another has been doing. Test results conducted by one practitioner can be available to all practitioners. Before prescribing a drug, a physician can review a patient's recent diagnoses, allergies, and prescription history and be aware of any over-the-counter drugs that could conflict with the proposed course of treatment. In the long run, the data carried by smart health cards not only can prevent illness and save lives, they also can save the healthcare industry billions of dollars. Today, many patients lack control over their health records. Smart Cards are among the few electronic devices that enhance both control and privacy. No one can read what is contained on the Smart Card's microchip or use the card to access computerised records without a personal identification number (PIN) and authoriased hardware and software. Further, Smart Cards interact reliably with a wide range of systems. They can operate over the Internet to verify information in a carrier's database, and they can be read and updated offline at a physician's office, when medical clerks prepare electronic claims for submission to an insurer.

Moreover, the ability of Smart Cards to disaggregate data and encrypt information can protect an individual's right to privacy while still allowing multiple healthcare facilities to share patient information more efficiently. Smart Cards can carry important health information and participate in the health information system's billing and collection functions.

Industry Insight

In recent years, there has been a pronounced effort to establish and refine standards for maintaining and moving healthcare data. With continual advances in Smart Card technology and increased awareness of its practical solutions, the healthcare industry's use of this technology is gathering momentum. The chief stakeholders in the US healthcare system are patients, providers, and payers. Most agree that the key to delivering safe, personalised medicine is communication among all three groups.

1) **Patients** - In today's medical environment, patients are the only ones who do not have access to their own medical data. Today's systems store redundant information in many places. Records are maintained by each physician treating a patient, by every institution serving a patient, and by any insurer who covers the service. However, the patient has virtually no access to the data, no ability to determine what is in the various databases, and no way to change anything that is incorrect. Health cards based on smart chip technology, combined with appropriate medical applications and data, can allow individual patients to maintain and control access to their own medical records. This health card is distinguished from other types of cards by its ability to transport confidential data securely from cardholder to practitioner and by the convenience of providing data immediately. Patient information can be accessed and controlled by the patient, using a card reader connected to the provider's computer or to the consumer's computer at home.

Transaction audit trails tracking both card access and modification can be captured and documented. Security features restrict access to data stored on the card through the use of a password or PIN, making the Smart Card a more secure method of verifying a patient's identity. Today's consumers are demanding improvements in healthcare services. A large number of consumers have multiple insurance policies or plans, suggesting the utility of a single card that is secure and controlled by the patient-a card that can store medical records securely while providing immediate access to providers. More importantly, the card must also be an essential component in the customer interaction between healthcare organisations in a primarily online consumer directed market. Smart chip technology can provide the basis for this essential component.

2) **Healthcare Institutions and Providers** - From the initial registration and admission of a patient through the processing of medical claims and billing, healthcare institutions are increasingly burdened by the cost and complexity of healthcare administration. Smart health cards can provide an institution with positive visual identification of a patient (a photograph) and a direct link to the patient's medical record number, which can be printed or included in a barcode on the face of the card. More detailed demographic and insurance information can be stored on the Smart Card chip, which can make registration more efficient and accurate. The integration of Smart Cards into the registration and admissions process should provide more reliable patient identification and more accurate and efficient links to existing medical records, improving the information gathering process.

For these reasons, the use of Smart Cards can greatly reduce the medical record maintenance costs associated with duplicate or overlaid patient records. (Duplicate patient records result when a new record is created for a patient who already has a record. Emergency medicine often deals with time-critical medical interventions. The rapid availability of medical information during an emergency can save a patient's life. This is another advantage of the smart health card. Smart Cards can store information about medical conditions, allergies, and current medications-information that can be critical to a successful clinical outcome but that is often unavailable in an emergency.

3) *Payers* - The healthcare community, including payers, has been slow to adopt Web/Internet technology, including Smart Card technology. Because of the changing healthcare landscape, however, payers are currently reevaluating their role in healthcare delivery. Smart Cards have a place in a payer's enterprise IT strategy, representing as they do a secure, portable electronic files capable of linking all entities in the healthcare community. Smart health insurance cards can improve data security and confidentiality, restricting access to sensitive healthcare information by storing access rights as keys that are used to authenticate the cardholder and control access. Managing when and where a person's private health information is accessed and making that information more readily available to those who have the need to know it reduces administrative overhead for everyone involved, including the payer. The implementation of a smart health insurance card can automate manual tasks, from eligibility and coverage updates to claims processing, and reduce the time taken by administrative procedures such as verifying patient insurance status and eligibility.

Creating and maintaining electronic medical data sets the stage for making critical information available on demand, for collaborative sharing of information among healthcare practitioners, and for leveraging the Internet to facilitate the exchange of healthcare data among multiple entities and across great distances. The information access and sharing are expected to improve patient care, reduce paperwork, and make systems more efficient. However, it also introduces the need to protect information from unauthorised users. An increasing number of identity systems use Smart Cards as a key component. Smart Cards provide a vital link in the chain of trust. They have a unique ability to verify cardholder identity accurately and to safeguard and offer the cardholder's credentials to a secure, trusted identity system. Smart Cards support such security mechanisms as public key infrastructure (PKI) and biometric templates.

The latter is an increasingly valuable tool for verifying identity, since biometrics is the only technology that can indisputably link a credential or an authentication event to a specific person. PKI and biometric security systems are increasingly applied to verify the identity of individuals in a variety of situations, including in the healthcare industry. Multi-factor authentication methods provide secure physical and logical access to critical information systems. Smart Cards can support all methods or authentication factors, from a physical token (something you have) to a PIN/password/private key (something you know) to a biometric template (something you are). Smart Cards not only can verify identity using any of these authentication methods, these cards can also determine one's access privileges to that information and share it with the trusted system being accessed. That element is essential to maintaining an efficient, secure, and trustworthy electronic healthcare system.

Conclusion - Smart Card technology is critical enabling tool to help resolve some of the issues with which the healthcare community is grappling today. Smart Cards can help reduce the inefficiencies prevalent in healthcare, diminish the number and effect of medical errors attributable to a lack of critical medical information, and empower patients to take a more active role in managing and maintaining their medical records. Smart Cards are not a panacea for all the problems faced by the US healthcare system. However, a Smart Card carrying critical patient medical data does support patient empowerment. The patient's Smart Card protects privacy while ensuring information access and security. It supports the mobility of today's patients, providing a means by which the various specialists who treat the patient can share information.

Smart Card technology helps reduce the burden of record management, providing timely information sharing and serving as a mobile repository for diagnoses and treatments. A patient Smart Card supports identity verification, provides excellent security, and can speed up patient registration and check-in. Leveraging Smart Card technology can improve efficiency and reduce costs. Smart Cards can provide the US healthcare community with a feasible and expeditious solution to the long-term problem of information access.

League Table of RFID Specifications

By Dr Peter Harrop PhD, Chairman, IDTechEx Ltd

IDTechEx

With about $5 billion being spent on RFID in 2007, of which about $2.24 billion is for tags, what are the favourite specifications? High Frequency (HF) is by far the most popular RFID frequency in money spent and it is even penetrating applications traditionally served by Low Frequency (LF) such as gas cylinders, beer kegs and other metallic objects, rented apparel/ laundry and even pigs in China. Not surprisingly then, it is an HF specification that is in the ascendant.

Dr Peter Harrop

Indeed, most of the leading RFID suppliers offer HF RFID cards and systems, including ERG, Gemalto and Watchdata Technologies of China. Assa Abloy and Allflex are among the leaders primarily because they offer LF tags and systems (secure access cards and cattle ear tags respectively) and NXP, formerly Philips Semiconductors, is in the leading pack thanks to unrivalled success in selling both HF and LF RFID chips though it covers the other frequencies as well. ISO 14443 has its origins in cards but now it is also used for tickets and labels.

18

It involves interrogation at no more than a few centimeters in range. That means that a transaction can not be accidental and the transfer of value or commitment to pay can not be intercepted from a distance. The archetypal use is card access to buses and trains. Recent huge orders for RFID ticketing for Russia, China, Portugal and Norway of around 400 million tickets will also employ ISO 14443. Indeed most of these schemes involve RFID tickets working off pre-existing infrastructure set up for RFID cards. Typically the ticket is used for frequent travellers and the RFID ticket is used for single trips, day trips and the like.
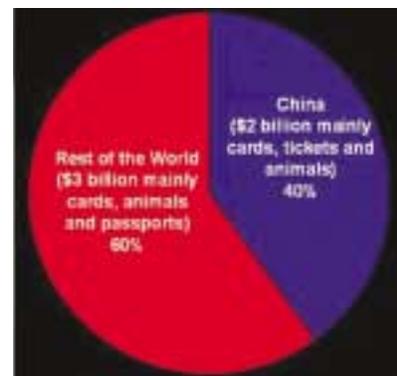
ISO is constantly extending its scope, the latest major success being the third largest global RFID market by value - e-passport tagging where the ICAO requirements are based on ISO 14443. Next comes animal and, to a much smaller extent human tagging employing ISO 11784 and ISO 11785 usually employed in unison. However, although animal tagging is the second largest RFID market by value globally, The spend on these specifications is less that it might be because non ISO proprietary specifications notably at 125 KHz rather than the ISO 134.2 KHz are also widely employed, particularly for pets. The pecking order of RFID specifications by RFID tag expenditure is shown below:

Position	ISO Specification	Frequency	Applications	Global Market Value($m)
1	14443	HF	Card, ticket, access, passport, drug	1200
2	11784/5	LF	Animals	170
3	15693/18000-3	HF	Library, access, conveyance	120
4	18000-6	UHF	Pallet, case, air bag, drug, conveyance, bookstore	120

As we see above, the third most popular specification is ISO 15693 and the later and closely allied ISO 18000-3 specification. Here the range typically employed is around one meter so it is used for "hands free" secure access and supply chains involving cards, badges and labels in the main. Behind that, the relatively new ISO 18000-6, particularly in the form of the so-called Gen2 form is gaining traction in the marketplace. Indeed, it is the basis of the IATA baggage tagging specification fixed in 2005 and it is demanded by many leading retailers and the US Military for pallet and case tagging and it is the basis of tire tagging specifications. It has its roots in supply chain management but it is appearing in asset management such as bookshops and even in secure documents such as visas. There is even a patient wristband to this specification though ISO 14443 is more common here.

As for the future, it is as yet uncertain whether HF or UHF ISO specifications will dominate such things as museum pieces, art works and individual items such as the smallest containers of drugs, where the primary need is anti-counterfeiting by establishing "pedigree". It is also uncertain whether the new active tag specifications within ISO 18000 will gain popularity.

In 2007, there will be three sectors where about $2 billion will be spent on RFID tags. They are cards, where ISO 14443 at HF is entrenched and pallets/ cases where ISO 18000-6 at UHF is entrenched. Battle lines are drawn for the third - item level consumer goods. In the second division will be military and animal RFID, both involving about $1 billion in spend in 2017, military being mainly UHF and animal mainly LF with some HF, that may become dominant if China - the biggest animal market by far - adopts HF more positively, notably to save cost while retaining a reasonable tolerance of proximate water and metal. China is where many of these things will be decided, because, in 2007, it has become the world's largest RFID market as shown in the graph to the right.

China
($2 billion mainly cards, tickets and animals)
40%

Rest of the World
($3 billion mainly cards, animals and passports)
60%

Rumours From the Front Line

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

The newly installed Prime Minister of the UK, Gordon Brown has already started making his mark in the area of security. In his commons statement this month he told Members that the first biometric ID cards will start during 2009. Many thought the project would be dropped or that the biometric database would carry on without the ID card but it now seems clear that the invitations to tender for building and running the planned national identity card will be published in the next few weeks according to the Financial Times. Whatever we might have thought it now seems clear that the project is to go ahead.

For all those suppliers out there this is good news indeed with contracts expected to be worth about £2bn over 10 years. Fairly well published is the fact that only fingerprints will be used, initially at least instead of the more sophisticated iris technology. Rumour has it that there are actually more practical problems with the iris scan than the humble fingerprint readers even though the precision of the iris scan is potentially far superior. Reports from travellers having problems at Heathrow airport which is trialling the iris technology is less than complimentary. James Hall the CEO of the Identity and Passport Service (IPS) has explained that the objective is to keep costs down and the technology relatively simple. Certainly in the US all the concentration seems to be on fingerprints.

The approach now being taken by the IPS is based on the establishment of Framework agreements whereby the IPS can call down programmes of work from the chosen ones that allows a more flexible approach to procurement. Further rumours from inside would suggest that the IPS doesn't really know how the national ID card scheme is going to work and there is still a significant discussion phase with potential vendors to determine the architecture for the future. One has to wonder what PA Consulting the principal consultants on the ID card project have been up to for the last couple of years. It certainly hasn't been hampered by lack of funds, so far the project has spent some £72m and that's before the procurement process starts. Figures from the IPS annual report show that there was spending of £30.9m for the year ending March 2007 up from £27.7m in the previous year. Home Office figures show that PA consulting earned £28.4m from the project in the two years 2004/5 and 2005/6.

So for all the hungry vendors out there what happens next? Well first of all you need to register, the Identity and Passport Service's (IPS) Framework Procurement has been published in the Official Journal of the European Union, inviting potential suppliers to make approaches. Apparently the IPS aims to secure around five preferred suppliers over the next nine months to be followed by a series of mini competitions to determine individual contracts. According to James Hall, "We want to create a team of people who understand our agenda. We're approaching this whole thing in recognition that we're building a set of long-term capabilities."

According to Bill Crothers, Executive Commercial Director for the IPS, suppliers will be required to "design, build, deploy and service" the projects - which will include an overhaul of the Immigration and Asylum Fingerprint System - as well as offer business process and IT outsourcing. The OJEU Notice was published on 11th August as 2007/S 154-192267. The NIS Strategic Supplier Framework is the new name for the National Identity Scheme Framework. The National Identity Scheme ('NIS') is discussed in the Strategic Action Plan published by the Contracting Authority in December 2006(Strategic Action Plan). This notice follows the Prior Information Notice published by the Identity and Passport Service ('IPS') in April 2007 and commences the procurement activity for delivery of the NIS. The NIS will comprise delivery of products and services to a number of public sector organisations and others and will provide a comprehensive and secure way of managing personal identity data.

The Contracting Authority will be conducting this procurement through the Home Office eSourcing portal and it is seeking expressions of interest to be in the form of a response as set out in the PQQ which can be accessed via the eSourcing portal, www.homeoffice.bravosolution.com. Happy hunting to all you vendors out there but do note that the maximum number of vendors is expected to be 6, can you name them? How about, EDS, Fujitsu, BT, IBM and Siemens Business Systems for starters.