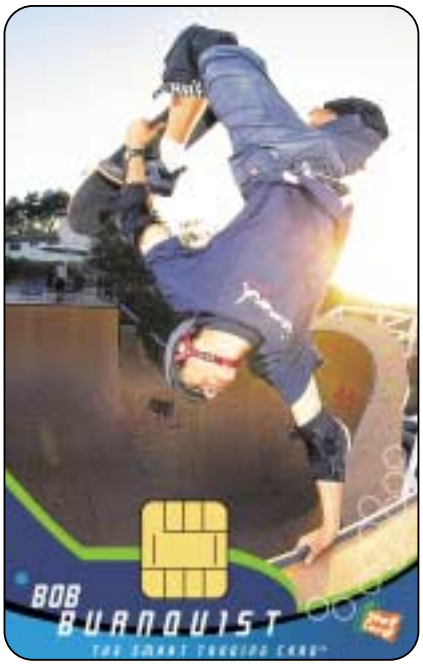
April 2002

Volume 11 • Number 4

Smart Cards Now

www.smartcardgroup.com

66 • *Miotec Hybrid Card*



66 • *Trading Card for Kids*

67 • *San Francisco Pilot Expands*

This Month's Feature Story

70 **SmartCards@India 2002**

Certain images obtained from IMSI's MasterPhotos™ Collection
1895 Francisco Blvd. East, San Rafael, CA 94901-5506, USA

Also In This Issue

Lead Story

63 *SchlumbergerSema Predictions 2002/03*

Special Features

74 *You Or I - Who's Who, How Can We Help, and the URI Project*
75 *C'mon, C'mon, Let's Work Together*
79 *Smart Cards On The Web*

News In Brief

64 *Proton for Central & Eastern Europe*
65 *Infineon Develop Chip Watermark*
66 *Trading Card for Kids*
67 *Transit Ticketing Contracts in Europe*
68 *Mobile Commerce Taking Off*
69 *Biggest Healthcare Project in Asia*

Corporate News • Spotlight

72 *Ingenico Fortronic Growth*
73 *ORGA*

Smart Card Technology

76 *The End of PKI as We Know It?*
76 *Ask the Experts*

Featured Companies

A.T. Kearney, Inc, ActivCard, Alcatel, American Express, APACS, Ascom, Atmel, Caradas, Cubic Corporation, First Data Corp, Fujitsu Invia, Gemplus, Glenburn Technologies, Hypercom, ICMA, Incard, Infineon, Ingenico Fortronic, ITV Digital, KBC Bank & Insurance Group, MasterCard, Metropolitan Transportation Commission, Miotec, Mist, NDS, november AG, Numenor Consulting Ltd, Oberthur Card Systems, ORGA, Paymap, Proton World, SchlumbergerSema, Security Biometrics, St George Bank, ST Microelectronics, StatCard Entertainment, Inc, TECO Electric & Machinery Company, Translink, United Microelectronics Corporation, Verifone, Visa, Visionics, Vodacom Congo, Welcome Real-time, Wirehound, Worldsmart Technology

By market (million units)	2000	2001	Growth actual 2001 versus 2000	2002	Growth forecast 2002 versus 2001	2003	Growth forecast 2003 versus 2002
Payphone	1040	1060	2%	1030	-3%	990	-4%
Mobile communications	450	400	-11%	450	13%	550	22%
Banking	120	145	21%	181	25%	220	0 22%
Others (eGov, IT, Pay TV and Transport)	180	196	9%	263	34%	357	36%
Totals	**1790**	**1801**	**.1%**	**1924**	**7%**	**2117**	**10%**

By region (million units)	2000	2001	Share of total	2002	Share of total	2003	Share of total
Europe, Middle East, Africa	895	883	49%	923	48%	974	46%
Asia Pacific	519	558	31%	597	31%	656	31%
Latin America	340	322	18%	346	18%	402	19%
North America	36	38	2%	58	3%	85	4%
Totals	**1790**	**1801**	**100%**	**1924**	**100%**	**2117**	**100%**

By technology (million units)	2001	2002	Share of total	2003	Share of total	2004	Share of total
Memory cards	1126	1159	64%	1158	60%	1155	55%
Microprocessor cards	664	642	36%	766	40%	962	45%
Multi-application cards ...of which are	155	222	35%	357	47%	530	55%
JavaCards	53	112	51%	200	56%	336	63%

Source: SchlumbergerSema

Smart Cards Now **is published monthly by Smart Card News Ltd PO BOX 1383 Rottingdean Brighton East Sussex BN2 8WX England**
Telephone : + 44 (0) 1273 515651 • Facsimile : + 44 (0) 1273 516518 • General Enquiries : scn@pavilion.co.uk ISSN 0967 196X

Managing Director Patsy Everett ~ patsy.everett@smartcard.co.uk • **News Editor** Jack Smith • **Technical Advisor** Dr David B Everett

Graphic Designer David Lavelle ~ david.lavelle@smartcard.co.uk
Customer Support Amanda Pearce ~ amanda.pearce@smartcard.co.uk

Russian Agent : Alex Grizov Recon Company "Sport Hotel" 5th Floor Leninsky Prosp., 90/2 Moscow 117415 Russia
Telephone : +007 095 131 92 92 • Facsimile : +007 095 131 92 65 • e-mail : recon@ropnet.ru

Editorial Consultants Dr Kenneth Ayer • Peter Hawkes • Simon Reed • Robin Townend

Printed by DAP (Sussex) Ltd. Telephone : +44 (0) 1273 430430

Don't Forget!
Our Website containing daily News On-Line, and information about the full range of SCN services, can be found at the following address: **www.smartcardgroup.com**

SchlumbergerSema Predictions 2002/03

SchlumbergerSema's annual review of Smart Card market trends highlights some significant trends and successes despite the economic slowdown of the last year when 2001 year-on-year growth rates for the entire industry fell from typical +20% levels to +3%.

The SIM (Subscriber Identity Module) Smart Card market experienced an unanticipated drop in 2001 of around 10%. The main reasons were low levels of handset renewals due to the perceived failure of WAP, the non-arrival of 2.5G technologies, near saturation of handsets in some countries, and the fact that many operators had overstocked on SIMs to meet growth predictions that did not occur.

SchlumbergerSema now expects growth in the wireless Smart Card sector will be a modest 12% this year, rising to 20% in 2003 with the key driver being the arrival of higher bandwidth mobile network infrastructure.

Chip phone cards decline

The company also notes early signs of decline in memory-only chip phone cards which account for well over half of the industry's total card shipments - over a billion units in 2001. However, this only reflects a small portion of the industry's revenue, as phone cards have become a commodity product. The phone card market, which has in recent years grown by around 10% per annum, is now being affected by the increasing penetration of mobile phones, the growing ability to pay for calls via multi-applications cards - such as e-purses and debit applications on financial cards.

Financial market

The financial market is the next largest application sector and grew by 21% in the last year as magnetic stripe bank cards are replaced with Smart Cards. The EMV (Europay/MasterCard/Visa) specification continues to dominate the industry. The case for Smart Cards in the banking industry was originally built on controlling fraud. Today, applications are increasingly focused on winning and retaining customers by offering innovative multi-application cards with multiple services, such as credit, debit, e-purse and cash dispensing facilities; new functions such as loyalty, secure remote access to accounts; and even non-banking applications like healthcare.

Market prospects for public sector ID cards will start to become immense from 2004 onwards, predicts SchlumbergerSema. Although the government-driven card application sector involves large volumes, and is the largest consumer of microprocessor Smart Cards after mobile communications and banking, it is still in its formative years. Several countries are currently tendering for national ID cards, with some projects expected to reach their roll-out stage during the next two years. Numerous other countries are currently starting to consider options in this area, partly as a result of heightened security concerns stemming from the events on September 11.

Contactless card technologies for ticketing and tolling are now spreading out from high-profile mass transit applications in major cities to numerous smaller-scale projects in mid-sized cities and towns.

The pay-TV market for Smart Cards is already substantial. Although it is likely to grow only sporadically in the short term, it is potentially a star in the Smart Card industry's future as cable and satellite set-top box card systems come up for renewal every two to three years.

Newest major application

IT Security is the newest major application for Smart Cards says the review. Although still involving small numbers, Smart Card-enabled IT security is experiencing explosive growth. Smart Cards are providing a user friendly and convenient tool for implementing enterprise-wide security for physical access to premises, as well as logical access to computers and private/public networks.

Looking forward two years, SchlumbergerSema expects Smart Card-enabled PKI (Public Key Infrastructure) technology to play a growing role in the deployment of many 2.5 and 3G networks, the roll-out of national ID card programs, and the implementation of Smart Card-based network access for enterprise IT systems.

The review predicts that by 2003, 50% of Smart Card shipments will support multiple applications and that the open JavaCard standard for multi-application cards - building on its unchallenged leadership in mobile communications - will attain industry-wide domination in the same time frame.

Contact

- **Emmanuelle Saby** Schlumberger Sema
  - ☎ +33 (0)1 46 00 71 04
  - 💻 www.slb.com

Proton for Central & Eastern Europe

Proton World and the KBC Bank & Insurance Group have signed an agreement licensing KBC Bank to implement the Proton Prisma multi-application Smart Card technology in a number of its associated banks in Central and Eastern Europe. As a group, they opted for a single secure chip card platform, i.e. the end-to-end high-security multi-application system, Proton Prisma, developed by Proton World.

In the initial phase, the agreement will involve CSOB Bank in the Czech Republic (with branches in the Slovak Republic), Kereskedelmi es Hitelbank (K&H) in Hungary, and the Poland-based Kredytbank, which also has branches in Lithuania and a subsidiary in Ukraine. The agreement also provides for possible implementations of Proton Prisma technology by other KBC associated companies.

KBC's associated companies will issue the Proton Prisma Smart Cards primarily for use with EMV PLUS, Proton World's credit/debit application..

Herman Agneessens, KBC, said: "By choosing Proton Prisma as the common chip card platform for KBC's international retail banking approach, we will be able to migrate to EMV in a cost efficient way. Not only will the joint purchasing of cards cut costs for KBC in the short term, it may also lead to permanent cost reductions by means of common IT card-related development for all banks in the KBC Group."

UK PIN Trial in Northampton

The Association for Payment Clearing Services (APACS) has selected Northampton for a public trial by banks and retailers of the use of PINs (Personal Identification Numbers) at point of sale in preparation for the national roll-out of PIN verification for all credit and debit card transactions in the UK by 2005.

With plastic card payment fraud in the UK currently costing card issuers more than £1 million a day, it is expected that the chip and PIN verification system will more than halve fraud losses.

Oberthur Smart Visa Order

Oberthur Card Systems is to provide more than 40,000 multi-application Visa cards to St George Bank and Worldsmart Technology (WST) for the first Australian live cashless payment scheme and customer loyalty program combined. The scheme was recently launched in Queensland, Australia.

The card, Oberthur's GalactIC Lite, incorporates the Visa Cash DES (e-purse) application with WST loyalty application and St. George Bank Load Restriction application. A secure key management system to protect the applications and their interactions with the loyalty terminals was also developed using Oberthur's Security Access Module (SAM) cards.

Card Management Infrastructure

Oberthur Card Systems and Caradas have developed the first ready-to-install Smart Card management infrastructure designed to improve time to market, reduce system integration costs and the risks associated with large-scale Smart Card deployments. The two companies have formed a strategic alliance to market and deliver to financial services companies and retailers in the Americas.

The packaged system includes Smart Card management software, authentication server software, client software, Smart Card hardware and software, consulting and system integration services, personalisation, fulfilment and project management services. Combined with multi-application Smart Cards, the package is a complete infrastructure for bank card issuers - supporting both Visa and MasterCard issuers.

MasterCard/Welcome Alliance

MasterCard International has signed a global co-marketing agreement with Welcome Real-time which will see it adopt Welcome's XLSmart loyalty solution. XLSmart will enable MasterCard credit or debit cards to store, process and deliver the electronic equivalent of incentives like reward points, coupons, gift certificates and tickets. The XLSmart System is deployable on both the MULTOS and JavaCard platforms.

For more information visit ...

Protonworld
www.protonworld.com
Oberthur
www.oberthurcs.com
Visa
www.visa.com
Caradas
www.caradas.com
MasterCard
www.mastercard.com
Welcome Real-time
www.welcome-rt.com

Infineon Develop Chip Watermark

Infineon Technologies is working with German biotechnology company november AG on a method of providing a coating for the gold contact surface of the module on chip cards to have unique identification features.

Much as the watermark on a banknote, the coating applied by november AG adds another layer of identification information to the security system providing visual verification that the module and therefore the chip beneath originate from a trustworthy source.

Customers will be able to choose to have the "watermark" on the chip modules in different colours or in the form of product and company logos. The first of the new chip card modules are scheduled for the start of 2003.

New Microcontroller from Atmel

Atmel Corporation is shipping the first high-end Smart Card microcontrollers based on its new secure AVR architecture. The new architecture forms the basis of the AT90SC19264RC, which is a high-performance 8-bit secure microcontroller based on the AVR enhanced RISC architecture. Its low power consumption also makes it compliant with mobile phone requirements.

The company says that typical high-volume pricing is expected to be $4.00 for 100K units.

The AT90SC19264RC, which features 192K bytes of ROM and 64K bytes of EEPROM, will be followed by other members of the family offering a set of products ranging from 2K bytes EEPROM up to 128K bytes all being software compatible to each other.

Atmel also introduced its AT05SC1604R Smart Card IC for production and general release. This 4K bytes EEPROM HCO5 microcontroller has 16K bytes of ROM and 1K bytes of RAM and is targeted at banking and government applications.

The device has been certified to EAL4 Augmented level under the Common Criteria or ISO-15408 security standard.

NEC Gains Visa Approval

NEC Corporation has announced that its range of 32-bit RISC microcontrollers for Smart Cards have become the first 32-bit Smart Card ICs to obtain Visa Level 3 Approval. NEC's V-WAY family of microcontrollers was launched in 1999 and established the company as one of the few chip vendors to produce 32-bit RISC microcontrollers for Smart Cards in large volumes.

Wireless Facial Recognition

Visionics Corporation and Wirehound unveiled facial recognition capabilities on Java technology-enabled phones from Motorola at the 2002 JavaOne Developer Conference in San Francisco. The application, developed specifically for a law enforcement agency, uses Visionics' FaceIt ARGUS as the delivery platform for facial recognition capabilities and Wirehound's Birddog software on a Java 2 Platform, Micro Edition (J2ME) technology-enabled mobile phone with a colour display.

The FaceIt ARGUS system automatically finds faces in a field of view and searches them against a mug shot database. Upon finding a match, the Birddog component generates a wireless alert to the phones used by mobile law enforcement officials, who are then able to verify the identity of the subject.

The phones can store multiple images and are alerted when a new image arrives. Non-matched images are automatically discarded from the system.

"By teaming with Wirehound, we are now providing a compelling solution for on-the-spot criminal recognition," said Dr. Joseph J Atick, Chairman and CEO of Visionics.

Online Biometric Signature Verification

Security Biometrics' new Hosted PenFlow Biometrics Signature Authentication Application for small and medium sized businesses is a communication infrastructure that allows any individual to be authenticated via a handwritten signature. PenFlow is targeted at law firms, insurance companies, accountants, car dealers, data base security and access providers, credit unions, on-line mortgage, banking and loan institutions, pharmacies and inventory control.

For more information visit ...

Infineon
www.infineon.com
november AG
www.november.de
Atmel
www.atmel.com
Visionics
www.visionics.com
Wirehound
www.wirehound.com
Security Biometrics
www.sigbio.com

Trading Card for Kids

StatCard Entertainment has announced that its Smart Trading Cards, which allow points and other information to be earned and saved on the cards, are now available at the 698 Toys 'R' Us stores across the US. The initial series, XAction Skate, allows teens and tweens to assume the identity of their favourite professional skateboarder. An exclusive interactive entertainment Web site can be accessed only with the Smart Trading Card, ensuring online safety for young users.

StatCard has animated skateboarding's top 10 athletes allowing cardholders the chance to compete as their favourite athlete in single or multi-player skate games, enter online skate tournaments, and earn rankings. Each trading card offers unique playing features; cardholders can also collect 30 XAction Skate Booster Cards that add new dimensions to the online experience.

Miotec Hybrid Card

Miotec and Fujitsu Invia are to supply Finland's Turku Vocational Institute with an information security solution that includes a Miotec hybrid card combining fingerprint biometrics, PKI and RFID technologies. Biometrics allows logging-on to information systems without passwords, PKI enables encryption of e-mail and RFID technology is used for access control.

New Members for ICMA

The International Card Manufacturers Association (ICMA) has added five new companies: Principal Members (Card Manufacturers) - IntelCav Cartoes (Brazil), Mahavir Decorative Products (India) and Sokymat (Switzerland). Associate Members (Suppliers) - Indigo USA and MagTek (USA).

MIST Opens Asia-Pacific Office

MIST's NBS Smart Card Issuance group is expanding its sales and service operations in the Asia-Pacific region and opening an office in Tachikawa City, Tokyo, Japan.

New JavaCard Technology

Gemplus has announced that it has developed the JavaCard Remote Method Invocation (JCRMI) - a technology designed to speed the design and adoption of multiple application Smart Cards - in association with the JavaCard Forum.

JCRMI provides a model to manage the relationships of Java applications interacting between different machines and aims to free developers from having to manage low-level exchanges by reducing major design, programming and testing difficulties.

Campus Card Project in Canada

QI Systems has completed a US $170,000 campus-wide Smart Card automation system for the University of Northern British Columbia.

The change from a magnetic stripe-based card system involved installing QI's Smart Card payment terminals for the Unattended Point Of Sale (UPOS) machines, including name brand vending, laundry, copier and parking equipment. In addition, QI developed, designed and installed direct cash-to-card value reload stations, which are PC based, capable of cash-to-card, accounts-to-card and credit-to-card with online communication capability. They are also designed to accept bills and coins, print receipts, dispense cards, have a built in alarm, and can reload values to a variety of proprietary and open card schemes.

Smart Card systems integrator Touch Technology International provided the operating system for the project with the installation of its transaction processing, settlement and reporting software.

VeriFone Ships 10mth System

VeriFone has announced the shipment of its 10 millionth payment system and claims market leadership.

Douglas Bergeron, CEO, said: "VeriFone is proud to once again lead this industry as a profitable independent company focused on the needs of merchants and acquirers everywhere. No other company comes close to reaching 10 million shipments."

For more information visit ...

StatCard Entertainment, Inc
www.statcard.com
Miotec
www.miotec.fi
Fujitsu Invia
www.invia.fujitsu.com
ICMA
www.icma.com
Mist
www.mistwireless.com
Gemplus
www.gemplus.com
Verifone
www.verifone.com

Transit Ticketing Contracts in Europe

Further signs that electronic ticketing systems in public transport are gaining momentum came last month with announcements of schemes in Germany, The Netherlands and France.

The Rhein Main Verkehrsverbund (RMV) and Hanau Strassenbahn (HSB) have launched a pilot for an advanced electronic ticketing system as the prototype for a comprehensive electronic ticketing system for the entire RMV region. The system is being provided by T-Systems, a subsidiary of Deutsche Telecom, and Cubic Transportation Systems, Ltd (CTSL), the UK subsidiary of Cubic Corporation.

The new ticketing system has been installed on more than 60 buses operated by Hanauer Strassenbahn AG (HSB) in Hanau, about 20 km from Frankfurt, and uses microprocessor, dual interface (contact/contactless) Smart Cards and check-in/check-out bus validators that process tickets on both entry and exit. Check-in/check-out allows the application of distance-based fares (such as zones) without driver intervention.

The system also includes the use of the Cubic TriReader (supporting a variety of card technologies and applications), a transaction management computer and software, hand-held inspection units and a wireless communication network that transmits data from the buses to the depot computer systems.

Also in Europe, Cubic has teamed with EDS on a Euro2.2 million contract from the Rotterdam Electronic Tram (RET) to install The Netherlands' first "gated" public transit fare collection system.

Cubic will provide an access control system for six new stations of the Benelux Line in Rotterdam, the most recent extension of the Rotterdam metro network, which begins operation this year. The system consists of gates and a central computing sub-system.

The new system has a series of gates that allow the traveller access to the station with tram, bus card or season ticket. Data is loaded to and collected from the gates by the computer sub-system. The design of the access system also allows RET to connect to a national electronic ticketing system.

French transport agency RATP and Ascom have launched the first ever contactless and disposable ticket on the Orlyval transport network in Paris. The network uses Ascom's contactless cards for season pass holders but the project has been extended to include occasional users who can now buy a 'disposable' contactless ticket. The ticket will also be valid for use on the national RATP and SNCF networks.

It is planned to extend the scheme to the whole Paris region.

San Francisco Pilot Expands

San Francisco's Metropolitan Transportation Commission (MTC) and a half-dozen Bay Area transit operators are expanding their six-month pilot program for the TransLink regional fare payment system with plans to issue between 2,000 and 3,000 additional TransLink Smart Cards to program volunteers over the next few weeks.

The first batch of contactless Smart Cards was mailed to some 4,300 program volunteers in late January for the pilot program on selected routes and at certain stations of six of the region's largest transit agencies.

"The whole point of the pilot program is to gather information so we can fine-tune TransLink and make it work on every transit system in the Bay Area," explained TransLink Project Manager Russell Driver of MTC. "We quickly decided that we wanted to open the system up to a lot more users than we originally thought."

Currently, the TransLink card can be used at 18 rail stations, on 31 bus lines, three ferry routes, and on two light-rail lines. Once the pilot program is expanded to include San Francisco's Muni Metro System this month, pilot program volunteers will be able to use TransLink on a total of six light-rail lines in San Francisco and Santa Clara County.

MTC has contracted with Motorola and ERG to implement and operate the TransLink fare collection system.

For more information visit ...

Cubic Corporation
www.cubic.com
Ascom
www.ascom.com
Translink
www.translink.org
Metropolitan Transportation Commission
www.mtc.ca.gov

Mobile Commerce Taking Off

Two recent studies indicate that mobile commerce is set to take off within the next few years. According to marketing consultancy Frost & Sullivan, mobile commerce could generate £25 billion in mobile payments by 2006.

The study considers mobile expenditure for a number of key user payment scenarios including automated point-of-sale payments (vending machines, parking meters and ticket machines); attended point-of-sale payments (shop counters, taxis); mobile-accessed Internet payments (merchant WAPsites); mobile assisted Internet payments (fixed Internet sites using phone instead of credit card), and peer-to-peer payments between individuals.

Results forecast mobile-accessed Internet and peer-to-peer payments will make up the bulk of payments, accounting for 39% and 34% of spending respectively in 2006.

Ben Donnelly, research analyst at Frost & Sullivan, said that it is more a question of how and when, rather than if, mobile payments will gain mass market acceptance.

"Analogies can be drawn with the introduction of credit cards 50 years ago, currently the principle alternative to cash. They were perceived as a niche product and unnecessary luxury for many years until global technology standards made them viable for the mass market," he said.

The report emphasises a number of benefits that will drive consumer and merchant adoption of mobile payments. Mobile users will be able to free up their time by making purchases walking down the street, paying bills while waiting for a train, or paying back a debt to a friend immediately after a meal. When purchasing goods online, consumers will not have to divulge their credit card details over the Internet, but instead supply their mobile number.

Forty-four per cent of mobile phone users globally say they would like to use their mobile phones for small cash transactions such as bus, taxi or train fares or items from vending machines, but only two per cent have done so, according to new research from AT Kearney and Judge Institute, part of Cambridge University's Business School.

The Mobinet study reveals intent to use m-cash is highest in Japan at 50%, 46% in Europe, 43% in the rest of Asia and 38% in the US. However, only two per cent of mobile phone users worldwide report any experience of m-cash, as the technology to perform such transactions is still in its infancy. Paul Collins, AT Kearney principal and leader of the study, warned: "Consumer tastes in the mobile arena are fragile, so it is imperative that the community of mobile phone makers, carriers, content providers and financial services companies rally quickly to provide mobile cash capabilities before consumer interest wanes."

SchlumbergerSema Milestone

SchlumbergerSema says that it expects sales of its Simera Java-enabled Subscriber Identity Module (SIM) Smart Card to surpass ten million units sold in North America in early 2002.

"SchlumbergerSema supplies its Simera Java-based SIM card to nearly every major wireless network operator using SIM cards in North America," said Edward Jacobsen, the company's Vice President of Mobile Communication Solutions in North America.

Incard Mokard SIMs to Brazil

Incard is to supply 32K Mokard SIM Smart Cards based on Java language to Tim Brasil, one of the operators launching the GSM service in Brazil.

ORGA SIM cards for MobilCom

ORGA Kartensysteme is supplying SIM Smart Cards to MobilCom AG in Germany. The shipments to MobilCom are part of a master agreement that both parties signed at CeBIT 2002.

Alcatel Wins African GSM Contract

Vodacom Congo has contracted with Alcatel to build a GSM network in the Democratic Republic of Congo in a five-year deal estimated to be worth Euro 145 million. The deal will build upon Vodacom Congo's existing GSM infrastructure and also utilise Alcatel's GPRS/EDGE and UMTS-ready services.

For more information visit ...

A.T. Kearney, Inc
www.atkearney.com
SchlumbergerSema
www.slb.com
ORGA
www.orga.com
Incard
www.incard.it
Alcatel
www.alcatel.com
Vodacom Congo
www.vodacom.net

Biggest Healthcare Project in Asia

Taiwan to Issue 22 million Smart Cards

Taiwan's National Healthcare Chip Card project starts in July and 22 million Taiwanese residents will be provided with a Smart Card by the end of 2003. The card will replace existing paper health card systems and store cardholder information such as medical records, treatment and visit records and administrative data.

It is the first major project of its kind to be rolled out in Asia. TECO Electric & Machinery Company, Taiwan, is the sole supplier of the Smart Cards for the project and will use microcontroller chips from Infineon Technologies featuring 32K bytes of EEPROM. The chips, from Infineon's 66Plus family will be produced by United Microelectronics Corporation, a certified Infineon Manufacturing partner in Taiwan.

The 66Plus controller ICs are manufactured using 0.22 micron process technology and combine security controller architecture with a high-performance memory configuration for optimised power consumption.

"We are pleased to be working with TECO to roll-out Taiwan's National Healthcare Smart Card, which is also the first major project of its kind to be rolled out in Asia," said Loh Kin Wah, President and Managing Director, Infineon Technologies Asia Pacific.

Infineon is one of two suppliers of microcontrollers for the project which involves a total of 24 million chip cards, including replacement and spare cards.

Hitachi is supplying its AE-4 16-bit microcontroller Smart Cards based on JavaCard 2.1for the project. Hitachi develops and manufactures microcontroller chips at TECO.

Satoru Ito, President and Chief Executive Officer of Semiconductor & Integrated Circuits, Hitachi said: "We are delighted to be selected with our Smart Card controllers in such a high profile project. We see AE-4 smart card controllers as the leading JavaCard platform for high security applications. As such, the AE-4 is a perfect fit for Taiwan National Healthcare IC Card, where security, JavaCard suitability, function integration, safety of supply are forming a valuable offer to our customer."

"Hitachi is one of our consortium members for the contract to supply the National Healthcare IC Cards to the National Health Insurance Bureau under the cabinet-level Department of Health," said Theodore M.H. Huang, Chairman of TECO. "We were impressed by Hitachi's excellent security capabilities and world-leading technology for its smart card controllers and are very proud to have Hitachi as our strategic partner for the National Healthcare IC Card project."

Also involved in the project is Giesecke & Devrient which is supplying the operating system. Ingo Zankel, G&D Senior Vice President, said: "G&D's JavaCard operating system and its applications will be a corner stone in the overall solution. I believe JavaCard on high performance and secure chips will be increasingly important to a wide range of Smart Card applications."

Chips for ATM and Credit Cards in Malaysia

Banking institutions in Malaysia are expected to begin a transition from magnetic stripe ATM and credit cards to chip cards in the second quarter of this year, according to the New Straits Times (Malaysia).

The newspaper reports Deputy Finance Minister Datuk Shafie Mohd Saleh as saying that the process would cost RM150 million for 40,000 merchants to use chip cards.

The move to Smart Cards is aimed at cutting card fraud and particularly unauthorised withdrawals from ATMs.

First Data Corp Acquire Paymap

First Data Corp has announced it is to acquire Paymap, a San Francisco-based financial services company offering proprietary electronic payment services to financial institutions. Financial terms of the deal were not disclosed.

Paymap will become part of First Data's Western Union Financial Services subsidiary, although the company will continue to operate under the Paymap name and under the direction of its current management.

For more information visit ...

Hitachi
www.hitachi.com
Giesecke & Devrient
www.gdm.de
TECO Electric & Machinery Company
www.teco.com.tw
Infinion
www.infinion.com
First Data Corp
www.firstdata.com
Paymap
www.paymap.com

SmartCards@India 2002

by Gourab Foswami, Glenburn Technologies

Speakers' Panel, Session Four

The SmartCard@India conference, part of the larger telecom show the 10th Convergence India 2002, in New Delhi last month provided a valuable insight into Smart Card progress and trends in India by key speakers from government and the private sector.

Rajeeva Ratna Shah, IT Secretary to the Government of India, revealed that the Government has set up a consortium of government ministries of Railways, Transport, Postal Department, Home Affairs and Defence as well as commercial bodies and Smart Card vendors to devise a techno-legal framework for Smart Card usage. As examples, he cited the huge Smart-enabling potential of the country's various rural welfare programs and district postal services.

Jalaj Srivastava, Secretary IT, Government of Goa spoke on the Government's Smart Card implementation programs in the State such as providing election identity cards on a no-cost to user basis with further plans of integrating ration cards and PAN cards. As a further measure, a hook-up of the 385 villages presently connected with telephones with Smart Card based systems in the offing.

Smart Card implementation in the transportation sector in Madhya Pradesh, one of the biggest states in India, was covered by *Rakesh Srivastava*, CEO, MAP-IT. He told delegates of the combined systems of driving licence issuance and vehicle registration in the same Smart Card and the immediate operational improvements observed on implementation.

Krishnamurthy Subramanian, IT Adviser to CAG, Government of India as well as Chairman, Standards Committee, Bureau of Indian Standards, spoke on the various standards which the IT department is proposing to adopt for all future Smart Card-based applications. While the latest release of the BS-7799-2- (April, 2002) will form the general basis in any Government level applications, the ultimate architecture will be based on the Uniform Global Standards based on the Global Platform Consortiums recommendations.

India, he added, would be particularly keen on conforming to TCSEC standards while retaining best-of-breed technologies currently available such as the latest implementation of the EMV standards. This will guide the ultimate journey towards the interoperable, open platform based solutions that will be at once "future-proof" as well as "backwards compatible".

It may be concluded that while there were quite a few encouraging signals from the government representatives, an actual framework of conducting whole-scale projects within India is yet to be in place as many gray areas still exist. The sincerity and speed that will be demonstrated by the Government in addressing these issues will largely be responsible in determining the scale of Smart Card-isation of both urban and rural India in the years to come. Fortunately, there is tangible movement in the area.

Overseas companies like ORGA, Infineon, Philips Semiconductors, iSmart International, ACG AG, DataStrip, etc., also voiced their aspirations for the Indian market and discussed implementing multi-platform, multi-application solutions with Smart enabled services. The main issues highlighted were those of security, authenticity of transactions as well as improvement in the overall service perspectives with the high-end customer section in mind. However, the enormous possibilities in the unorganised sector was also widely discussed.

Hans Adlkofer, Vice President, Infineon Technologies and the head of chip card business group, indicated the enormous potential of Smart Card penetration in India as a projected percentage of the total Asian market with an estimated compounded annual growth rate of 39% by the year-end. As an indicative figure of actual usage, the estimated demand for the Indian Market for such cards could reach 105.1 million in 2008 from a present level of 8.17 million.

He highlighted the importance of secure and confidential data transactions and emphasised the need of migrating to standardised, interoperable open platforms with secure, multi-applications in the card and a very quick time-to-market cycle.

ORGA's *Jonathan Elcombe* discussed the various drivers of the Smart Card industry with their targets and responsibilities. The roles each component shall play will largely determine the market awareness and usage of Smart Cards, he said.

Robin Roy, Executive Vice President of Vysya Bank, gave the banking perspective to the Smart-enablement of urban India. Specifically Vysya bank, currently in the process of net-enabling, is also seriously contemplating a move towards Smart Cards for the areas where networked connectivity is presently not available. He also listed the possible benefits of such a venture and encouraged support from the overall banking sector in India.

Jagbir Singh and *Vikas Shah* of Bharti Telenet and Tata TeleServices spoke generally on the respective Smart Card implementation programs of their existing systems. While Singh emphasised the need to co-brand such applications with interested MNCs (Mobile Network Companies) to bring the price levels down while maintaining the standards, Shah talked about their successful program of Smart payphones in Andhra Pradesh in collaboration with Schlumberger, France.

Vivek Sagar, Director - Advanced Payment Systems (South Asia) MasterCard International spoke about the evolution of payment systems and the EMV standards and MasterCard's contributions to the development of EMV.

SchlumbergerSema's *Subraneel Bose* gave an overview of the security aspects that go into a Smart Card and the trend of shifting to a Public Key Infrastructure in the e-transactions in an open networked environment . No mention, however, was made on the areas where Schlumberger is planning to penetrate in India, even when approached with a question to that effect. Some tight secrecy observed there!

Daniel Lim Fang Liang of Infineon International championed the cause of contactless Smart Card readers which, he said, required less maintenance with increased reliability.

Shirish Rege of Datacard was still more forthright with his presentation on his product "affina" - a multi-application, multi-platform enabled card life cycle management system with an intelligent back-end data management system. This Platform Management Architecture, he claimed, is the culmination of the best brains of the NatWest Development team (platform7 group) that had worked towards the pioneering applications in the field of electronic purse and embedded systems of the 90s. The product he claims can be customised for any requirement in the Indian market.

Eric Vandeermeersch of ACG provided an overview on the various identification technologies in use in Germany along with their other areas of operation including readers and RFIDs for complete access control systems solutions.

iSmart International's India based CEO, *George White* finished off the event with a note of anguish over the lack of penetration in the payments segment which is his thrust area in India. The figure of total card based (all types) amounted to only 0.6% of the total retail spending. This suffers abysmally in comparison to a figure of 39% in the US and 28% in the UK. While India is lagging a clear 3-5 years behind the leaders, he is still confident of bridging this gap once the latest EMV standards (Visa's EMV Version 4) are out and in place. This would facilitate the global, interoperable transaction cards (both debit and credit) even as India migrates to a fully-fledged Smart Card-based system like the UK and France.

With improving living standards in the urban sector, customers have also become more demanding. To meet their expectations as well as to be ahead of the competition, banks also need to be more innovative and with a personal touch, like the popular supermarket chains of UK which have become the largest issuers of personalised Smart Cards, he added. This could be achieved by various loyalty schemes, e-coupons, gift certificates etc. He concluded by identifying e-purse and e-cash systems as the opportune market and stressed the need for identifying a common security standard for the same.

Udai Singh Pathania of Venture Infotek Global, listed his company's various Smart Card initiatives in the field of e-payment, including the successful petro-cards of BPCL, and the ICICI Bank/MAHE Campus Cards with both identification and payment systems built in.

Rajeeva Ratna, Secretary IT, Government of India
Guest of Honour, Smart Card Tech 2002

Summing up the Indian market, *Sanjay Dharwadkar* of iSmart International, identified driving licence, vehicle registration, ration cards, health cards, community ID cards, state ID cards and dairy co-operative schemes as the possible concentration areas with varying degrees of urgency of implementation. He predicted that by the end of this year, India will be well on the way to rapidly expanding its Smart Card base.

Ingenico Fortronic Growth

Ingenico Fortronic, the Fife, Scotland-based electronic payment solutions company, reports a 11.1% rise in annual revenues to £27 million for the year ending 31 December 2001, up from £24.3 million last year. Strong sales for Ingenico Fortronic's Smart Card transaction terminals and new mobile payment and pre-payment technology boosted the company's growth.

Recent deals including a landmark Smart Card terminal supply contract with Barclays, worth £40 million over five years; a terminal licensing agreement with National Australia Group and the signing of a distributor agreement for Ingenico's pre-payment systems in the Republic of Ireland, have made Ingenico Fortronic one of the fastest growing companies in the French-owned Ingenico Group. The Group posted record sales growth of £240 million in 2001, up from £158 million in 2000.

Website

www.ingenicofortronic.com

EC Approves Infineon Cash

Infineon is to receive a Euro 180 million (US $158 million) aid package from the German government to build a Euro 1.1 billion (US$960 million) microchip plant in Dresden following European Commission approval of the hand-out. The package will be one of Europe's biggest state hand-outs but the EC concluded that the aid did not breach anti-competitive guidelines.

The cash injection is Euro 40 million (US $35 million) short of what the government had originally intended.

Gemplus Management Reshuffle

Gemplus parted company with yet another senior member of its team at the end of March when Frederic Spagnou, Chief Operating Officer since May 2000, stepped down. His responsibilities have been allocated to other members of the Gemplus management team.

The company also announced the appointment of Yves Guillaumot as its new Chief Financial Officer following the departure of Steven Gomo which was announced earlier this year. Guillaumot will act as CFO on an interim basis until a permanent successor is appointed.

ActivCard Files Lawsuit

ActivCard has filed a lawsuit in the US District Court, District of Delaware, alleging Vasco Data Systems International's infringement of US Patent No. 5,937,068 entitled "System and Method for User Authentication Employing Dynamic Encryption Variables" which was issued by the US and Trademark Office on August 10, 1999. The complaint also alleges false designation of origin in violation of Lanham Act 43(a) and common law trade dress infringement.

Steven Humphreys, CEO of ActivCard, said: "ActivCard's strategy is to openly license our technology to enable interoperable and standards-based solutions that help to grow the overall market. When users of our intellectual property are unwilling to enter into a licensing agreement, however, it undermines our ability to maintain the best technology standard for the industry, so it really harms all of our customers. In these cases, therefore, we intend to vigorously protect our Intellectual Property."

ITV Digital to Sue NDS

UK TV company ITV Digital is preparing a £100 million lawsuit against News Corporation's UK subsidiary NDS over allegations that the company damaged its business by publishing its Smart Card security code on the Internet.

The struggling digital television firm says more than 100,000 forged Smart Cards ended up in circulation giving free access to its programmes and depriving it of millions of pounds of revenue.

Lawyers for ITV Digital want to join a $1 billion legal action against NDS in the US, launched last month by Canal Plus (SCN, March 2002).

NDS has dismissed the allegation as "outrageous and baseless," and is preparing to counter-sue.

Appointments

Hypercom has promoted Hugo Bolanos to Senior Vice President Sales & Marketing for its operations in Europe, Middle East and Africa.

Semiconductor manufacturer ST Microelectronics has appointed Andrea Cuomo as Corporate Vice President and Advanced System Technology General Manager.

ORGA

Smart Cards Now talks to Graham Carson, Managing Director

Graham Carson

Although the love affair turned distinctly sour last year, all the major Smart Card players have been involved in the burgeoning mobile sector in one sense or another. However, in ORGA's case, the link goes back a lot further. Back in 1987 ORGA invented the first SIM card on the original analogue mobile phone network in Germany. UK MD Graham Carson is the first to admit that the company has never truly exploited its involvement in such a pivotal technological breakthrough.

Despite this missed marketing opportunity ORGA have nonetheless remained a key player in the telecoms world ever since. "Historically, Telecoms has driven the Smart Card industry to where it is today," says Carson. "If you haven't been a player in the mobile industry then you haven't been a player and we've been fortunate in that regard."

Looking at the current fall-out in the telecoms arena Carson pinpoints a number of key factors: "Mobile is semi-cyclical type of business," he says. "You have a huge surge in demand that drops off once saturation has been reached. However you usually see several of these curves happening at once being driven by new technology. People were expecting the first 3G pilots to be implemented last year and that didn't happen. This meant that there was a gap between hitting the GSM saturation point and the start of the 3G rise."

Carson admits that it was unforeseeable that so many of the key SIM markets such as UK, Germany and France would all reach saturation point at the same time, but notes that over-eagerness regarding 3G was also a factor. In retrospect the expectations that were set for 3G were clearly well ahead of the technology and, in many respects, this still remains the case today with 3G technology still not available on the high street.

Looking forward Carson predicts the telecoms market will expand into a situation where financial institutions and billing providers will have to get on board to turn the peripheral 'gimmicks' such as SMS messaging into real business cases. This throws up a whole new set of challenges: "How do you bill for a piece of content that only has a value for a split second?" he says. "That's the challenge because a lot of the billing structure is not equipped to handle this type of flexibility."

Telecoms undoubtedly remains the exciting end of the market for the Smart Card players, but ORGA have been sensible enough to keep focussed on its real core business of banking. Whilst many rivals came crashing down as mobile revenues collapsed last year, ORGA rocked but remained steady. "Those companies that managed to perform well last year were strong within banking. If you look at the card market globally, banking produces the greatest demand - far outstripping GSM/3G. Banking is the one market that has the most stable supply situation." Carson said.

The other key area for ORGA, according to Carson, is ID and authentication although he admits that the sector has an even more problematic project cycle than the mobile model. "You can't just open a factory to implement two million cards then close again," he says. "A lot of ID projects will have to be split between a number of different suppliers to cope with that peek demand. This could only be achieved by the big system integrators like IBM, Unisys or EDS. I don't know a Smart Card vendor who is really equipped to handle it."

The key battleground common across all sectors has remained the quest for open standards with the industry continuing to be dogged by proprietary software. According to Carson, the industry is at last beginning to move toward true open standards in the form of MULTOS and, most notably, Java, but there are still major problems: "There is no point in having something that is open platform if nobody can use it. If I still have to go to the supplier to get my applet I am still locked in to the supplier."

For ORGA, the success of open platform technology is crucial to the company's target of regaining the technology leadership it demonstrated in the days of the first SIM card. "Gemplus has always been the marketing leader but we used to be the technology leader," says Carson. "We were the first to have microprocessors, first to do public key cryptography, the SIM card, added value billing, true interoperable Java. We have to regain that and we are putting a lot of work into open platform technology to do that."

Whether open source will put ORGA back on the top of the tree remains to be seen, but the company's reputation for stability remains intact. "We have a reputation for being extremely reliable; so much so that we could almost be described as a relatively unexciting company!" quips Carson. With many of its more glamorous rivals falling by the wayside maybe 'unexciting' will prove to be the way forward.

You Or I – Who's Who, How Can We Help, and the URI Project

by Peter Tomlinson

Peter Tomlinson

You would have thought that suppliers of multi-application card platforms would have included standard ways to hold and use a common dataset. You would have thought that developers of card-based applications would work to such a dataset. Data *optionally* held would be a profile of the card-holder: name, address, sex, date of birth, preferred language, special needs. The dataset would be designed in a flexible manner, so as to allow for extensions: fingerprint template, for example. The data would be embedded in a security matrix controlling access, so as to meet Data Protection and civil liberties requirements.

Not so. But then you would expect a police officer, after arresting a suspect, to be able to fill in a single form with basic information, and then have that information automatically propagated through all the reports that have to be compiled. Not so (at least, not so in the UK).

There are fragments of the methodology: international standard ways of coding country of origin (ISO 3166), date (ISO 8601), preferred languages (ISO 639), special needs (EN 1332). There is also a standard way of identifying the information and building the small scale database: the oddly-named ASN.1. For those familiar with smart cards, the core standard, ISO/IEC 7816, has allocated data object identifiers (tags) to hold the data, and defined a method to allocate more such identifiers.

The European Commission, for all the gripes that we make about it mandating things like straight bananas, would dearly love us to improve the service to citizens: "Design for All" is the slogan. As I write, I have by my side a 187 page report from the ICT Standards Board (ICT = Information and Communications Technology – see www.ict.etsi.fr/About_ICTSB/Consumer_Principles.htm) entitled "Final Report of the ICTSB Project Team on How Consumer Requirements May Be Taken Into Account by Standards":

Certain issues appear to be of the highest priority in considering consumer requirements. Specifically, priority consideration should be given to the following in all ICT sectors:

- ☐ Consistency of interface
- ☐ Intuitive operation – where consistency of interface is not possible
- ☐ Cost transparency
- ☐ Security and privacy

You don't achieve that by wishing. Pigs might fly purely by the power of imagination, but delivering quality IT-based services is hard graft.

Something is indeed being done. It stretches back several years, to the DISTINCT ID project, in which several countries collaborated in developing smart cards that could be carried to various cities and regions across Europe and could be used to access public information kiosks. Insert the card and the screen starts to display in your preferred language, producing first a personalised welcome message. Then came the (again oddly named) URI project (URI = User Related Information). Now there is the Extended URI project (www.cenorm.be/isss/Workshop/URI/Default.htm), specifically to develop and describe implementation methods in the common classes of multi-application cards (there is, of course, more to life than Java Cards).

Why write this? Because we need a better name for the project than URI.

Biographical note

Peter Tomlinson MA (Oxon), age 58, is an Independent Consultant in the field of Smart Cards and related technology (terminal equipment, for example). One-time Physicist, designer of mainframe CPUs and more recently of Mondex-related equipment, he is currently working on transport ticketing technology and the Extended URI project. He is a Director of the ITSO transport ticketing specification management company. Contact him at pwt@iosis.co.uk.

C'mon, C'mon, Let's Work Together

by Mike Meyerstein, Numenor Consulting Ltd

Mike Meyerstein

"Our mission is the application of Smart Cards and security to e- and m- services."

A few weeks ago, three wise men (actually two men and a lady) came to seek my advice. Their ETSI project aims to provide every one of us with a single, personal Universal Communications Identifier (UCI), i.e. a single character string to replace the list of contact numbers that we all need today. We will interact with a network-based Personal User Agent (PUA) to tell it which calls to route to which network and which ones to send to voicemail, etc. We will programme our PUAs from a phone, email, Internet, etc.

I report this encounter because it reminded me of the old Universal Personal Telecomms projects. They foundered for several reasons; notably lack of a simple and secure user interface. Remembering "a few simple codes", usernames, passwords, etc., is not acceptable to most users on the move. The Smart Card automates and secures this process, but someone has to meet the cost of providing fixed-network terminals with Smart Card readers. Surely the mobile handset, being already provided with a Smart Card and IFD, should become the ubiquitous user interface to the PUA, especially now that we are talking about large-screen GPRS and 3G handsets which can really motor. I hope that I got the point across, for my ETSI inquisitors would hardly let me get a word in edge-wise!

The equipment-provisioning and service-providing parts part of fixed-network telecomms businesses can seldom agree on who is to pay for special hardware. The UCI problem is even worse because mobile and fixed network operators are nowadays separate, so the PUA network would likely be operated by a totally new enterprise, neither a fixed nor mobile operator. Squabbles over the apportionment of cost vs. revenue will be legendary.

We are similarly beset with non-cooperation in the world of m-commerce, where differences between the business models of banks, mobile operators and handset manufacturers are holding the world back. One hopes that the new Mobile Payments Forum will be able to do for the world what other bodies have so far been unable to achieve, i.e. to ensure that standardisation activities work to support a business model that is acceptable to all players. However, when I brought this up at the Mobile Payments Forum's first conference call, I was told that consideration of business models was out of scope. Sounds like the same old story.

So, IMHO, to make either the UCI or m-commerce happen requires real co-operation between fixed and mobile operators, handset manufacturers and financial institutions. Firstly on business models, then on standardisation and deployment of technology. I don't target Smart Card suppliers here, as I am assuming that the much-hyped era of write-once, run-anywhere, Javacards removes them from the problem equation. But even in that area, insufficient co-operation is causing a lamentable paucity of run-anywhere-ness, as recent tests by mobile operators have shown up.

So come on lads, let's start moving forward by working together!!

Events Diary

May

2 Wallet Wars: The Invasion of the Smart Card, New Connaught Rooms, London, UK

Contact: Sandra Hunter
Logica Consulting
Stephenson House
75 Hampstead Road
London
NW1 2PL
Tel: +44 (0)20 7637 9111
E-mail: HunterS@logica.com

11 - 16 TEPR 2002 - Four Conferences in One Venue: Electronic Healthcare, Wireless/Mobile, Security, and ROI, Seattle, USA

Contact: Marcy Robinson
Tel: +1 617-964-3923 #223
E-mail: marcy@tepr.com
Website: www.tepr.com/wireless

13 - 15 Cards Middle East, 3rd Annual Conference & Exhibition, Crowne Plaza, Dubai, Dubai, UAE

Contact: Stefan Nilsson
Tel: +44 20 7827 5997
Email: stefan.nilsson@terrapinn.com
Website: www.cards-worldwide.com/cardsme2002

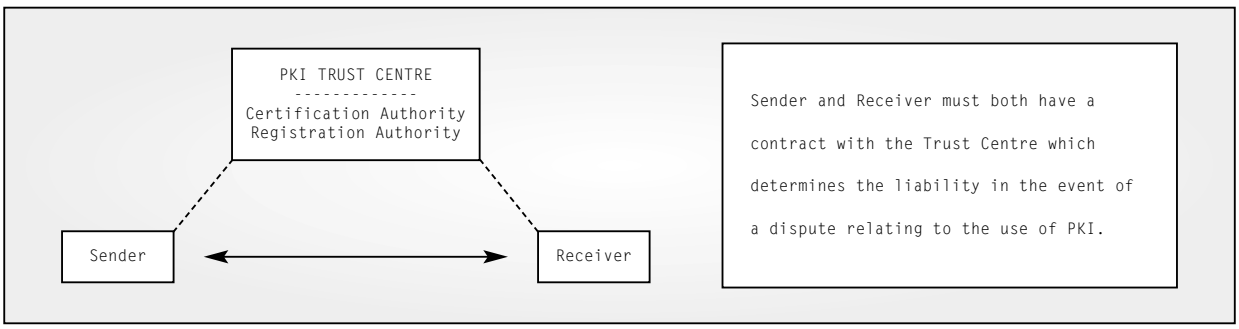
16 - 18 2002 Smart Cards, China & Users' Conference, China International Exhibition Center - CIEC, Beijing, China

Contact: Frank XU
Tel: +86-10-6583 1718 / 6581 0479
Email: ait@263.net.cn
Websites: www.goldencard@gov.cn • www.cupta.net.cn

The End of PKI as We Know It?

by Dr David B Everett

Baltimore, one of the companies most associated with PKI is having a disastrous time. In its 2001 end of year figures it was reporting pre tax losses of £660 million. The miseries of Baltimore have been reported elsewhere but we should look at the core proposition, is PKI and Internet security a dead duck? The answer is yes and no, PKI as represented by many is overhyped and severely misunderstood but the need for security on the internet has never been stronger. The internet is agreed by all to be a most hazardous place to do business so we can safely assume that if the internet is to be a base infrastructure then adequate security is essential. Authentication, authorisation and integrity are the main business requirements where confidentiality may be a necessary option. Authentication and data integrity are best met by the use of cryptographic techniques whereas authorisation is more complicated and involves authenticating the actions of an authorised role holder. All of these security services are well known to the community and can be met using both symmetric (e.g. DES) and asymmetric (e.g. RSA) or public key cryptographic mechanisms.



PKI is usually associated with the concepts of using public key cryptography to effect the necessary security services. Digital signatures and their attendant public key certificates are the core cryptographic mechanisms. There is nothing new here, such ideas have been around for the last 20 years, it is the business framework in which they are used that matters and herein lies the nub of the problem.

In a closed community, for example a bank and its customers, it is relatively straightforward to set up a secure transaction between the bank and a customer using either symmetric or asymmetric cryptography. The bank is responsible for the security system and is liable for its vulnerabilities if they lead to misuse. The reasons for using a public key system are to achieve the properties of non-repudiation and possibly to simplify the attendant cryptographic key management.

Ask the Experts

Q: Is there a Smart Card which has a 2048-bit RSA public key crypto processor?

A: All the major Smart Card silicon manufacturers are looking at 2048 bit RSA but don't forget that using the Chinese Remainder Theorem which would always be the default implementation you only need 1024 bit registers. The Philips FameXE co-processor is programmable and can in priciple handle key lengths up to 5K bits. The Infineon Advanced Crypto Engine is 1100 bits while the Hitachi AE45C Montgomery processor is 1024 bits.

Q: I need a readers with a relay output, so that when a valid Smart Card (EG: payflex) is inserted it wil trigger the output.

A: Nearly all Smart Card readers have a card presense sensor. It is then a matter for the software to decide what is or not acceptable.

Q: Is it possible for the ATR of a Smart Card to be reset after it has been corrupted?

A: The ATR may be stored in mask ROM or EEPROM. It would be unusual for the ROM to be damaged so most likely the ATR is in the EEPROM as part of the application. You would need to

PKI is assumed to be an open system where participants can interact securely to do their business, but somebody has to be responsible for the security. It is pointless to use a digital signature created by a key which is not legally underwritten. The public key certificate is no more than a technical mechanism that vouches for the correctness of the public key. A certification authority must underwrite the attributes attached to that key in a legally enforceable sense. You then end up full circle because you need a closed system to control the key holder and his actions in a contractual form.

Companies such as Identrus and GTA (Global Trust Authority) have tried to address these problems by authenticating the holder of the public key and underwriting the identification through a legal contract. Companies such as Verisign make certificates available to all but haven't really got to grips with the necessary commercial structure. This is evident in the way that certificates pop up in the internet browser in an uncontrolled way. How many people just click continue? Its really academic because there is no contract in place that gives any legal redress. PGP is probably more effective because the participants have consciously set up their own certificate community.

So what happens next? Well in the first place there is a clear requirement when using the internet to solve two problems. Single sign on is fundamental if we are to move forward. The number of user names and passwords has become impossible to manage. The user name is probably the bigger problem because most sites allow you to control your own password. Our names are no longer unique but our e-mail address is, such a simple solution but few sites allow you to use an e-mail address as a user identity. This problem is solvable, even if we can't have unique IDs and user chosen passwords it is not beyond the wit of man to use a token as our access control interface. This token could manage the plethora of user names and passwords but offer the single sign on interface to the user.

The need to identify people and authenticate their actions securely over the internet is a more difficult problem. It has to be a public key system because symmetric cryptographic schemes are not easily scalable in an acceptably secure way. Also in a business environment the property of non-repudiation is usually fundamental. So we end up with PKI but not necessarily through the products currently being promoted by the companies in this field. All that matters is that an individual can be legally bound to the use of his digital signature, it is in this sense no different to a hand written signature accept that the latter exhibits forensic evidence. What is really necessary is that any business use of a signature requires the user to register that key with the recipient organisation. Users must be responsible for their own keys. The vouching organisation must be free to determine the strength of the authentication mechanism because he is taking the risk. It is in some ways no more than a progression from the user name and password. I think I have just re-invented PGP and interestingly certificate revocation is down to the key holder. The Liberty Alliance could be the space to watch.

reload the application which is in general only possible with a multi application card. If it is only the ATR that is corrupted you could still use the card by ignoring the ATR and setting the software to the ISO 7816 defaults (e.g. T=0, direct/inverse)

Q: I am working on a project for Smart Card ticketing. I want to improve the existing protocols for payment but I don't know how to begin programing these protocols in Java. Do you know of any existing protocols?

A: Payment systems using a Smart Card are based on bilateral authentication. It is necessary for the card to verify the terminal and the terminal to verify the card. This can be done with both symmetric and asymmetric cryptography. The payment protocol itself is based on on a cryptographically protected Request (for the payment) and a Response (the transaction message).

Q: What is the maximum range a contactless card can communicate with the reader.

A: Most of the contactless Smart Cards available today are based on the ISO 14443 standard which has a maximum range of 10cm. ISO 15693 defines a longer range card of up to 1 metre but these are used more as memory tags and its difficult to get this range withour having a battery in the card.

Smart Card News On Line: Round-Up

Smart Card Group's *Smart Card News On Line* service is emailed to subscribers every working day, reporting on industry events as they happen. This service is available FREE to *Smart Cards Now* subscribers (£100 per year for non-subscribers). For further details and to sign up please contact Amanda Pearce - amanda.pearce@smartcard.co.uk; tel: +44 1273 515651 (further contact details are available on page 62). Here's a selection of the headlines we covered in March:

Corporate

- ERG Price Slumps After Warning
- Infineon Deny Insider Trading Accusations
- Welcome And Cyberpro Merge
- Baltimore On the Edge
- Datacard to Market ChipNet in Americas
- G&D And Hitachi In Japanese Alliance
- Interchange Acquire UK Network Specialist
- ERG Write Down Knocks First Half Year Results
- Canal Plus And NDS In Digital TV Security Row
- Miotec and Eterra Forge Smart Card VAR Deal
- New Faces At GlobalPlatform And Oberthur
- SCM Microsystems to Acquire Towitoko
- Gemplus Management Reshuffle Rumbles On
- ActivCard And Vasco In Patent Theft Row
- Bull Pin Hopes On Government Handout
- Catuity Predict a Profitable 2002
- Altech Acquisition Boosts Card Subsidiary
- Ericsson In Tax Evasion Probe
- Former Customer Bails Out ESM
- Fujitsu Toshiba Chip Alliance On The Cards
- Xansa Hit By Further Financial Worries
- MasterCard SPA Wins Support
- Biometric Company In Employee Backlash
- US Digital ID Companies Join Forces
- EC Approves Infineon Cash Injection
- New Fears Over Gemplus Job Cuts
- Netsmart Remain Positive Despite Results
- New Alliance to Focus on Multi Application Cards

Government

- SCM Deliver Extra 85,000 Readers to DoD
- Hong Kong ID Card Plan Underway
- TimeTrade Win US Air Force PKI Contract
- UK Government Smart Card Plan Revealed
- Australian e-Purse to Use Oberthur Smart Cards
- Scotland Considers National Student Smart Card
- Brazilian Smart Cards Make Slow Progress

Banking

- G&D Chip to Migrate Swiss Banks to EMV
- HSBC Choose SchlumbergerSema For EMV Strategy
- ANZ Bank Debut Verified by Visa
- Finland Adopts Verified by Visa
- NEC Awarded Visa Approval
- New KeyPad Smart Card Tackles Fraudsters
- Bell ID Win Two European Contracts
- ABN Amro Launch Middle East Solution

ID & Authentication

- Identix Launches itrust Access Platform
- Australian Airports to Adopt Iris Biometrics
- $700m Lost in Online Fraud in 2001, Says Report
- Cansec Launch Access Fingerprint Reader
- Five US Airports Order Identix Biometric Solution
- Fingerprint Biometrics Make US Campus Debut
- Airport Biometric Trial Expands to US
- Canadian Airport Pilot FRS Access System
- Sun Platform Integrates ActivCard Identity Solution
- Facial Recognition Debuts On Mobile Phones
- Business School Adopts Rainbow Token

Transport

- LA Awards Smart Card Transit Contract
- PCL To Deliver Smart Transit Cards in Wales
- ACT Win UK Fuel Smart Card Contract
- MasterCard Offers Travel Itinerary Service
- Radiant Install Indian Transport Solution
- First Dutch Fare System Underway
- TransLink Pilot Program Expands
- German RMV Adopts Smart Card Ticketing System

Telecoms

- Philips And Huawei to Develop 3G ASIC chipset
- Sony Ericsson Turn Up Heat in Handset Wars
- 3G Handset Battle Set for Third Quarter
- Handset Market Suffers First Decline in 2001, Says Report
- South Korea in Mobile Payments Trial
- China Unicom Goes Live With SchlumbergerSema Solution
- Toshiba and Mitsubishi To Work On 3G Platform
- Vodafone And T-Mobile Launch e-Wallet Mobile Platform
- US Carriers Sign Up to Microsoft Smartphone
- Incard Supply SIM Cards For Brazil GSM
- ORGA Deliver SIM Cards to MobilCom
- SchlumbergerSema Reaches SIM Card Milestone
- Mobile Transactions To Reach £25bn in 2006
- Mobile Users Wait on Payment Capabilities
- China Unicom Hit By Weak CDMA Uptake

Retail

- NEC Launch Secure Shopping PC System
- Performance Technology Launches Smart Card Trial
- Canadian University Adopts Smart Cards

Leisure

- 'Smart Money' For Philippine Teens
- World Cup Visitors to be Issued Smart Cards
- First US Smart Village Underway

Technical

- SCI Launches Smart Card Development Kits
- DNP Launch MULTOS and JavaCard PKI Solutions
- Infineon Launch New 'Short Range' Mifare Chip
- Sharp Launch New Java Enabled SoC
- NTRU Launch First RFID PKI Solution
- Toppan Java Smart Card In The Pipeline
- ORGA Launches PKI Smart Card System
- Gemplus Develop New JavaCard Technology
- Infineon Develop Chip Watermark
- Atmel Launch New Smart Card Microcontroller

Misc

- Scottish Lawyers Employ Secure Network
- Wave Integrate Chip into Samsung Keyboard
- Cryptomathic Joins GlobalPlatform
- Rainbow Launch Security Token For Windows 2000
- Infineon Launch In-Car Application Device

www.visaeu.com/smartcards/main.html

Visa EU

I was prepared for a long, tough battle to find Visa's Smart Card section amongst its huge site but I was pleasantly surprised by how easy it was to find the right pages. Once there, the content was intelligently grouped into sections tailored toward consumers, merchants or vendors. As well as being informative, the site served as a useful research resource with a wealth of data relating to the EMV rollout in Europe, including some strong graphical analysis. However, the US version of the site (www.usa.visa.com) featured a notably less impressive Smart Card section, which focussed primarily on card specification. The site remained useful but US visitors seeking slightly more in depth Smart Card information would be well advised to visit the European site. Page design, especially in the European version of the site, was highly impressive throughout, boasting a modern and clean appearance that never interfered with navigation or usability, although the occasional 'pop-up' pages remain as unwelcome as ever.

Navigation ■■■■■
Content ■■■■■
Appearance ■■■■□

www.mastercardintl.com/merchant/smartcrd.html
www.mastercardintl.com/newtechnology/smartcards/

MasterCard

Unlike the Visa site, there's nothing on the main homepage directing you towards Smart Cards. This inevitably leads to the laborious process of checking site maps, search engines and, in this case, linking to the country-specific sites in the hope that something would materialise. After much skipping between sites you eventually arrive at the Smart Card section which is hidden away in the merchant area of the site. MasterCard's Mondex e-purse continues to dominate proceedings although content is limited to the standard Mondex PR hype with very little in the way of new developments or technical information. The EMV page, on the other hand, is bland but useful, linking to PDF documentation for all EMV standards and specifications. Things improve over in the corporate section of the site, where MasterCard's new oneSMART Smart Card solution is given the full treatment. This includes a number of Flash animations demonstrating Smart Cards 'in action' which are entertaining to watch if ultimately rather pointless. There is a strong FAQ and technical section and a collection of interesting Smart Card related articles. A good resource, but many will give up before they get to what they're after.

Navigation ■■□□□
Content ■■■■□
Appearance ■■■□□

http://home4.americanexpress.com/blue/

American Express

Again nothing obvious to guide you from the main home page but Amex at least manage to include a search engine that actually works - an increasingly rare occurrence on the web. With issues such as EMV not of direct concern to Amex, the company are clearly more concerned with signing up new cardholders than promoting the Smart Card revolution, so relevant Smart Card related pages are thin on the ground. However, Amex's flagship 'Blue' Smart credit card section includes some useful information on how the card can be used with a reader for secure online shopping, and other useful background data. The only thing not directly concerned with the Blue card is a Smart Card FAQ which is worth a look for beginners. Navigation is acceptable and everything looks OK but this clearly not the place to find out about Smart Cards.

Navigation ■■■□□
Content ■■□□□
Appearance ■■■■□

Large Retailers Benefit from EPOS Program

Waqar Qureshi, Head of Chip Infrastructure, Visa International EU.

More than fifty of the largest retailers in the EU representing 40% of the Visa card sales volume are benefiting from the EPOS development and deployment program announced in February 2001. High street names selling food, clothing, petrol and household goods will leverage the EPOS development work sponsored by Visa EU to streamline their EPOS integration to EMV. "This will significantly reduce the time to market for the majority of retailers and provide a range of product choices from at least ten different vendors", said Waqar Qureshi, responsible for infrastructure migration.

At present the key solutions providers including Retail Logic, IBM, Wincor Nixdorf, Ingenico, and Thales have already been select to deliver solution by the end of this year and a further five more will be announced later this year. Since these vendors are also the existing suppliers of EU retailers and have a pan EU footprint, means that virtually every single EPOS retailer in the EU will benefit directly or indirectly. It is estimated that this initiative alone will save around 12 months of migration time. Furthermore, these EPOS solutions will be able to be deployed in other parts of the world without the need for major redesign, as EMV is an international standard.

Visa EU is going one step further by incentivising the placement of terminals at high Visa volume EPOS retailers. An estimated 600,000 terminals represents 70% of the Visa card volumes as transacted through EPOS retailers, and a total of 60,000 of this prime estate will be sponsored for EMV deployment by Visa through its member banks. This together with the readily available EPOS solutions from vendors will remove a major barrier and will give confidence to retailers and encourage them to convert the remaining of their estate of terminals to EMV before 2005.

The British Retail Consortium, the French Retail Consortium and the individual country EMV migration committees have all publicly stated the need to make this happen and 2001 was used to set-up the framework for acquiring banks and retailers to move forward together with a common migration plan per country. "This is a very exciting time in the history of banking and is likened to the migration from paper to magnetic stripe electronic transactions over twenty years ago", said Waqar Qureshi. •