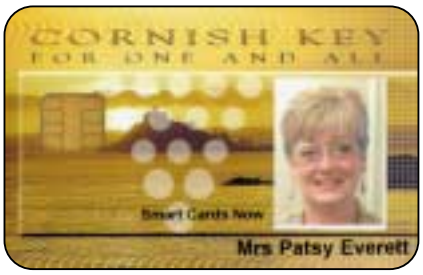
May 2002

Volume 11 • Number 5

Smart Cards Now

www.smartcardgroup.com



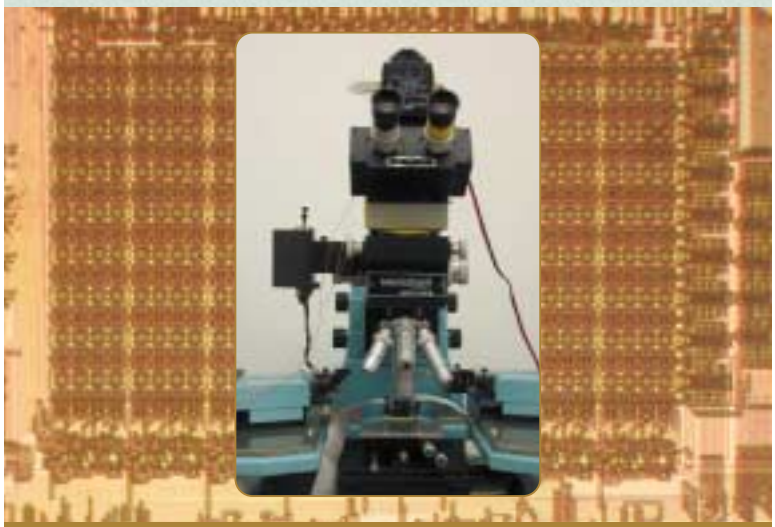
84 • Citizen Card for Cornwall

86 • Moscow Multi-application Card

86 • ACT Crosses the Pond

84 • Entrust Smart Portal in UK City

This Month's Lead Story



Above: SRAM memory array with 80x magnification (main); and Wentworth Labs MP-901 manual prober with Vivitar 550FD photoflash lamp (inset)

Also In This Issue

Featured Companies

Abbey National, Academy Bus, ACG, ACI, ACT, ActivCard, Alcatel, APACS, ASK, Aspects Software, Atlas Telecom Mobile, Banque de Luxembourg, Banrisul, Ben, Bluefish, BNC, Cardbase Technologies, Catuity, CH Jones, CIM, CMG, Compaq, Cornish Key, Datacard, eAnywhere Tech, Entrust, Eurosmart, Gemplus, Giesecke & Devrient, GlobalPlatform, Hana Bank, Hitachi, IATA, IBM, ICTS, ID TECH, Identicard,Identix, Infineon, Inside Contactless, MasterCard, Nokia, NTRU, Oberthur, OmniTek, Orange, ORGA, Perfect Printing, Philips, PKI Forum, Precise Biometrics, Qualteq, Samsung, SchlumbergerSema, SCM Microsystems, Sharp Microelectronics, Sita, Sospita, STMicroelectronics, Sun Microsystems, Supercom, TSYS, Ultra-Scan, University of Cambridge, VASCO, Visa, Visionics, Welcome Real-time

www.vasco.com

VASCO

The VASCO site does not appear to make any revolutionary steps forward in the design department but it does at least get the basics right. Everything is easily accessed from the home page and the intelligent dHTML menu system does appear to help the user rather than just look good which is usually the case. Content is grouped into sensible sections and is organised in such a way that is impossible to get 'lost' within the site. All current product documentation is transcribed and there is an impressive download section which suggests that the site is aimed toward current VASCO customers rather than the casual surfer. The site includes some interactive Flash based demos for its flagship Digipass product, but generally this is a solid, no-nonsense website that doesn't try to do more than it should.

Navigation
Content
Appearance

www.activcard.com

ActivCard

In stark contrast to the VASCO site, ActivCard tries to pull off every web gimmick in the book. Alongside the Flash presentations there are a number of videos (curiously all appearing to be in different formats) relating to ActivCard's involvement in the DoD Common Access Card (CAC) project but it is unlikely that many users would bother with the long downloads required. The same could also be said for the audio presentation of the company's latest quarterly results and it doesn't bare thinking about what would happen if a humble dial-up user attempted to access all the multimedia on offer. The rest of the site appears remarkably bland by comparison and useful content is fairly thin on the ground with no user support or download section to be found. Good fun if you've got the time but ultimately rather disappointing.

Navigation
Content
Appearance

www.entrust.com

Entrust

Although content is undoubtedly the key to any website one can't help thinking that Entrust could have aimed a little higher on the design front - the purple and yellow colour scheme is highly unpleasant and even the customary Flash sequence is missing from the homepage. However, there is plenty of useful detail on Entrust's wide ranging series of solutions even if you have to wade through all the standard PR hype to get to it. There is also a series of interesting articles in the resource section which serve as a useful introduction to digital signatures, secure e-forms etc. and links to all the relevant white papers, specifications and analysts reports which will make the site a useful bookmark.

Navigation
Content
Appearance

Fears Over Smart Card Security

Two new studies into the security vulnerabilities of Smart Cards have provoked fresh fears over the possibility of hacking attacks.

Researchers at IBM's Thomas J. Watson Laboratory in Yorktown Heights (New YorK) revealed a new class of side-channel attacks, called partitioning attacks, which extract secret key information from SIM cards by monitoring side-channels, such as power consumption and electromagnetic (EM) emanations.

In a paper entitled "Partitioning Attacks: Or how to rapidly clone some GSM cards", the IBM team claim the attack can be performed within minutes and is considerably easier than the traditional hacking methods such as breaking the cryptographic algorithms used by the card or using intrusive attacks to extract the key from the microchip.

Meanwhile, two researchers based at the University of Cambridge in the UK have discovered what they claim is a 'cheap and easy' way of extracting secret information from Smart Cards using only a camera flashgun and microscope.

According to the study, entitled "Optical Fault Induction Attacks", the researchers discovered it was possible to interrupt the operation of the Smart Card's microprocessor simply by exposing it to an electronic camera flashbulb. The researchers were then able to focus the flash on individual transistors within the chip by beaming the flash through a standard laboratory microscope.

Professor Ross Anderson, one of the authors of the Cambridge report, told *Smart Cards Now*: "The results we've published relate to microcontrollers. A whole family of Smart Cards have also been broken, and we're not naming them. Some have been broken without even using a microscope - simply depackaging the chip and inducing glitches at the right time with a flashgun was enough."

Both IBM and the University of Cambridge claim to have developed a series of Smart Card design modifications that would protect against the respective attacks.

However, a handful of leading Smart Card technologists have attempted to quash rumours that the new hacking techniques warrant a serious security risk. Vice President of R&D at Semiconductor Insights, Ed Keyes, said in a statement that only cards currently used in low end applications that are "fabricated in old technologies" were at risk from the flashgun attack.

Mike Paterson of Hitachi's Smart Card Business Group claimed the flashgun attack "did not represent a realistic threat to the viability of any well designed Smart Card system" and that the company had designed several countermeasures to protect against such an attack.

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**

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

InfoSecurity/Advanced Cards Awards 2002

Europe's leading IT security event InfoSecurity took place at London's Olympia on 23-25 April with over 200 companies taking part in proceedings. This year, SmartSolve, the Smart Card orientated event, was integrated into the main show.

Companies involved in the biometric and ID/authentication sectors inevitably generated the greatest interest with VASCO, ActivCard, Entrust, RSA and Utimaco all demonstrating their latest products on stand. Foremost among the Smart Card participants were Gemplus and SchlumbergerSema, although there remained some notable absentees including Giesecke and Devrient and ORGA.

Alongside the exhibition was the customary keynote speech and seminar programme. The highlight was Pentasafe's Chris Pick's speech on the Human Firewall project, which focussed on creating a link between IT and physical security.

Running parallel with InfoSecurity was the 4th annual Advanced Card Awards which took place at London's interContinental hotel on the 23rd April. The US Department of Defense Common Access Card program featured in three awards on the night: 'Best Security or Biometrics Implementation' (for ActivCard and SchlumbergerSema), the 'Outstanding Smart Card Application Award' and the all important 'Judges Award'.

The other winners were: Pin Protection Label from Schreiner GmbH (Best Security Product), Smart-Solution from Retail Logic (Most Innovative Product of the Year), Shetland Smart Card by Gemplus (Best Loyalty Implementation), NHS Occupational Health Smart Card Scheme by TSSI (Best Healthcare Implementation), Internet PG by KEBTechnology (Best Payments Implementation & Best E-Business Implementation using Digital Identity), Moscow Social Security Card by Rosan Group (Best Transport or Travel Implementation), WIQ from ORGA (MIPS Best Mobile Commerce & Communications Implementation), The Net1 'Malswitch' Project (Most Innovative Implementation of the Year) and the Blatchford Adaptive Limb (RNIB Usability Award).

The ORGA Advanced Card Hall of Fame Award was presented to Gemplus founder and chairman Marc Lassus.

Citizen Card for Cornwall

Cornwall in the UK (population 500,000) launched its citizen Smart Card last month. As part of the government's scheme for a switched on England, the Pathfinders project was set up and 25 pathfinders applied for grants ranging from £400,000 to £2 million. The Government has set aside £350 million to be spent over the next three years.

The Cornish Key Card was launched to replace a number of local authority cards with one. The idea is not new but what is unique is that the project took only five months and entailed working with seven partners and at least 12 suppliers.

According to Roy Cosway, Cornish Key Corporate IT Services Manager, there were many lessons to be learnt, in particular the need for a good full time project manager. There were also problems dealing with suppliers, some of whom considered the project too insignificant and were difficult to deal with, or over quoted to perform certain tasks, the lack of standards, and the issuing of the cards.

Cosway also named and shamed the difficult companies. Particular praise was given to ORGA who supplied, on time, the 50,000 dual interface Smart Cards and an application to enable cardholders to view their personal details, credit available and their last 10 transactions. Also praised was Smartex who managed the overall project.

The Cornish Key Card currently has attendance recording for schools, a library card, bus pass, car parking, proof of age, door entry into council offices, school meals and computer logon.

It is envisaged that after stage 2, when the scheme hopes to attract further government funding, to add applications such as tourism, leisure, time recording, voting and e-tokens for such benefits as bus ticketing, photocopying and vending. Also, the 7,000 diabetics in Cornwall could have their personal details on the card giving paramedics access to this information in an emergency.

Ukraine Smart ID Project

Israel's SuperCom has won a $17.5 million contract with the Ukrainian government for the implementation of the second phase of the government's multi-documentation project. The contract is part of a previous national ID Smart Card project in the country which was secured by Supercom in 1999. SuperCom will provide the equipment and consumables for the production of ID Smart Cards.

Entrust Smart Portal in UK City

Entrust has won a contract with Southampton City Council in the UK to develop a secure Web Portal solution enabling housing repair requests and processes to be conducted online.

The first phase will be piloted by 6,000 citizens and is based on Southamton's SmartCities multi- application Smart Card initiative launched in Spring 2000. The existing Smart Cards will be used to access the Web portal through public kiosks giving access to those without a home computer.

K Card Crime Unit

A two year pilot of a unique UK police unit created by the Association for Payment Clearing Services (APACS) and the UK Home Office has been launched to fight the organised crime syndicates behind steep rises in UK plastic card fraud losses which topped £411 million last year

The Dedicated Cheque and Plastic Crime Unit will focus on counterfeiting, which has become the UK's worst type of card fraud. Counterfeiting grew 50% last year and is estimated to have cost £160 million. Cheque, ATM, identity theft and card-not-present fraud will also be investigated where organised crime is involved.

APACS Chief Executive Chris Pearson said: "The banking industry recognises the need to share resources with the Government and police against organised card criminals. This unique approach is expected to rock the foundations of the organised criminal networks which damage society as a whole, not just through card fraud but also through the other types of crime financed by it."

APACS' member banks are funding 75% of the £5.6m ($8.1m) cost of the pilot with the Home Office providing £1.4m ($2m). The Association of Chief Police Officers and the National Criminal Intelligence Service will support the unit.

ATM Mobile Top-up Service

Abbey National is to launch a mobile phone top-up service in the UK using its ATMs. It has teamed with GSM network operator Orange and transaction solution provider Euronet in a scheme which will enable Abbey National customers with Orange pre-pay phones to transfer funds to their mobile account using one of the bank's 3,000 ATMs.

A pilot scheme is planned to start this month and roll-out of the service expected to be completed this autumn.

Gordon Webber, Head of Global Distribution at Orange, said that the growth potential in the UK was huge. "Orange Belgium, where customers have had access to cash machine top-ups for three years, now sees 30% of its Pay As You Go customers top up their talk time in this way," he said.

MasterCard Gears Up for Chip Migration

MasterCard has moved up a gear to position itself for the migration from magnetic stripe cards to chip cards by forming supply agreements with chip and Smart Card manufacturers.

An agreement with Infineon Technologies will enable MasterCard institutions of any size to purchase Infineon chips at volume pricing levels. The company's currently available 66Plus series microcontrollers support the MULTOS and Java multi-application Smart Card operating systems.

SchlumbergerSema will supply MasterCard member banks with Smart Card services that will support EMV (Europay/MasterCard/Visa) migration. The contract will be based on MasterCard's new Smart Card initiative, OneSMART. The company will offer chip capacities ranging from 16K bytes to 64K bytes, and either the MULTOS or the SchlumbergerSema Palmera Protect Java-based platform.

Giesecke & Devrient (G&D) is to supply the Smart Cards for MasterCard's $2.99 multi-application Smart Card program based on the MULTOS operating system. G&D will supply one million cards in addition to the existing three million cards already issued in Korea, Taiwan and the Philippines.

For more information visit ...

Advanced Card Awards
www.advancedcardawards.com
Cornish Key
www.cornishkey.com
APACS
www.apacs.org.uk
Orange
www.orange.com
Supercom
www.supercom.com
Infineon
www.infineon.com
Entrust
www.entrust.com
SchlumbergerSema
www.slb.com
Abbey National
www.abbeynational.co.uk
Giesecke & Devrient
www.gdm.de

Moscow Multi-Application Card

A multi-application Smart Card has been launched in Moscow by the Bank of Moscow, Rosan Finance, the Moscow Metropolitan (Metro) and Visa. It is intended for people who receive state aid - students, pensioners, members of the armed forces and others and provides reduced prices for a range of services including Moscow's underground rail system.

The new card stems from the introduction in 1998 of a MIFARE contactless chip card for students using the Metro system. Other organisations, including local government groups and benefit providers, have since joined the scheme. Up to 1.7 million cards have been issued for transport while 21,000 cards are being used for welfare benefit collection. They are accepted in some 200 stores and by pharmacists and clinics for the collection of medicine. Over 100 ATMs also accept the card.

For payment, the Bank of Moscow provides a Visa Electron debit card function. As well as using the card in stores, cardholders can withdraw funds from any branch of the bank or through its ATM network.

The Bank has also opened cash machines for pension payments at 10 post offices while the MMI system (Mandatory Medical Insurance) allows people to register for services at six district hospitals using the card. The payment application, currently held on the mag-stripe, will be moved to the card's microchip to improve security. The chip will have a contact/ contactless dual interface based on the EMV standard and will use GlobalPlatform specifications.

Java Card Technology V2.2

Sun Microsystems is set to release version 2.2 of Java Card Technology which features easier programming and improved interoperability of applications on Smart Cards from different vendors and well as improved support for wireless standards. The company says version 2.1 applications will run on the 2.2 platform without any modifications, ensuring a smooth transition.

First EMV Banking Cards for Italy

Oberthur Card Systems was chosen by 13 out of the first 15 Italian banks that are migrating to Smart Card technology to supply debit/credit cards for the initial roll-out. It is estimated that Smart Cards will be used by 35 million Italians by 2005. The first Italian EMV cards are all manufactured and personalised in Oberthur's Italian plants.

Vasco Hits Back at ActivCard

Vasco have launched a counter lawsuit against ActivCard over allegations that the company infringed upon ActivCard patents.

The Vasco lawsuit attempts to raise serious questions regarding the validity of the ActivCard patent. Vasco noted that ActivCard's product design is not unique and is "indistinguishable from a common pocket calculator." The lawsuit also alleges that ActivCard's behaviour in the marketplace constitutes unlawful business practices and interferes with Vasco's commercial relationships.

Vasco CEO Mario Houthoof said: "Vasco was forced to file a suit because of the baseless claims and allegations made by ActivCard to Vasco's customers and potential customers. We are pleased to engage in a fair comparison of our products with any competitor in the marketplace, but we will not tolerate unfair competition and baseless allegations against our company."

Standards for interoperability

With so many different security schemes currently being implemented or promoted, SITA and IATA aim in the s-Travel project to ensure an interoperable global solution.

IATA will define the enrolment processes and procedures to be followed for airlines to authenticate frequent travellers or their own personnel, prior to them issuing a Smart Card containing biometrics and digital certificates. SITA will assist IATA with the development of industry standards and ensure that the various competitive biometric technologies available will be able to interface to, and are interoperable with, current and future airport infrastructures.

ACT Crosses the Pond

Applied Card Technologies (ACT), based in the UK and established in 1997 will be launching 50,000 New York Pass cards during the summer which will allow visitors to fast-track access to all participating attractions avoiding queues and saving money as well as providing special offers at selected restaurants and theatres.

The cards can be purchased over the web or from tourist authorities and travel agents either in the visitors home country or the target country. The New York Pass is run and promoted by Leisure Pass North America. The memory chips have been provided by ACG and other platforms are planned.

Contactless Smart Paper Cards

ASK has announced the shipment of over two million of the world's first contactless Smart paper tickets, called C.ticket.

The company has perfected a patented, printed antenna and the smallest ISO 14443 compliant contactless Smart Card chip to produce a paper-based Smart Card at a low cost.

C.ticket is currently being used in a highway toll system in Macedonia and RATP, the Paris Metro operator has ordered over one million cards for the Orly-Val shuttle which runs from Orly airport to the city. ASK says it already has orders for over nine million cards.

Air Travel Security Hots Up

Interest in the use of Smart Cards combined with biometric technology to increase security for airlines and airports has been given a new impetus by leading air transport organisations SITA, provider of global information and telecommunications solutions for the air transport industry, and the International Air Transport Association (IATA) who have teamed on a new pan-European initiative. They have joined with Smart Card manufacturer Gemplus and biometric technology integrator Keyware to develop and trial s-Travel (secure-travel) incorporating digital certificates.

At the same time, heavyweight IBM has announced it is working with the Schiphol Group to provide a new access control system using iris recognition technology, Visionics has received nine new orders for live scan biometric systems at US airports, Continental Airlines is piloting a biometric security system at Newark Airport and SAS Airline is to test Smart Cards and biometrics.

The aim of the s-Travel project is to achieve the highest level of identity verification for frequent travellers and contribute towards improving the security of the global air transport system.

It will be funded by the European Commission and Swiss Office for Education and Science and trials will take place in Europe later this year with the intention of the service being expanded globally.

IBM is joining with Holland's Schiphol Group to offer airlines and airports a security access system using biometric iris scanning technology. The new offering will be based on the existing Automatic Border Passage (ABP) system Schiphol Group has deployed at Amsterdam's Schiphol Airport.

This system identifies and verifies travellers by cross referencing a real-time iris scan with the travellers' pre-registered iris data, which is stored on a Smart Card (currently Schlumberger's TB200 2K card) and data is encrypted using the 3 DES algorithm.

IBM will work with Schiphol Group to extend a subset of the biometric security features in the system so it can be used by airlines and airports for passenger identification and tracking in functions such as ticketing, check-in, screening and boarding. They also plan to develop components to provide secure employee and staff access to restricted areas.

Visionics Corporation has received nine new orders, estimated to be worth $285,000, for its live scan biometric system at airports across the US. The system captures fingerprints and transmits the images to the Office of Personnel Management, which then submits the image for search against the FBI's IAFIS (Integrated Automated Fingerprint Identification System) database.

Aviation services company ICTS International has announced that it has launched a trial of its F@CTS system on a Continental Airlines flight at Newark airport in the US. The F@CTS system is designed to speed and simplify the processes of identification and security checks of passengers at airports and uses both biometric and Smart Card technology. The pilot follows a similar scheme the company has been running at London's Gatwick airport since January.

In a further development, Precise Biometrics and Scandinavian IT Group have contracted with SAS Airline for a test installation to make check-in and boarding procedures safer and more flexible using Smart Cards and fingerprint technology.

For more information visit ...

Visa
www.visa.com
Sun Microsystems
www.java.sun.com/javacard
ACT
www.card.co.uk
Academy Bus
www.academybus.com
Oberthur
www.oberthurcs.com
Sita
www.sita.int

IATA
www.iata.org
IBM
www.software.ibm.com
Visionics
www.visionics.com
ICTS
www.icts-int.com
Precise Biometrics
www.precisebiometrics.com
Scandinavian IT Group
www.scandinavianit.com

US Proposes Smart Driving Licence

The US government has proposed legislation that will require all driving licences to be migrated to a Smart Card that will include a thumbprint and digital photograph.

The proposals respond to calls for tighter national identification requirements following the September 11 terrorist attacks by enabling the cards to link to state ID databases for government checks. The bill proposes $300m to be made available through the Transportation Department and $15m through the National Science Foundation to fund the project.

Civil liberty groups have voiced fears that the card would be used as a national ID card.

Miotec Luxembourg Contract

Miotec and Utimaco Safeware are to supply Banque de Luxembourg with multi-functional biometric and PKI cards. The cards will also use RFID technology for access control functionality.

The solution uses Precise Biometrics' combined fingerprint and Smart Card readers, Miotec Hybrid cards including Precise Match-On-Card functionality, and the system integrator is Utimaco Safeware Belgium.

"The user now has a unique card for accessing bank buildings and parking, using the time-management system and the bank's lifts, paying in the bank's restaurant and accessing workstations and IT systems,"said René Chevremont of Banque de Luxembourg.

New Biometric Software Standard

A new standard aimed at speeding up the adoption of biometric technologies in the US has been released by the BioAPI Consortium. The specification defines open standards for how software applications communicate with fingerprint, facial recognition or iris recognition technologies.

Colin Soutar, Work Group Chairman, said: "The BioAPI standard breaks the log jam and gives large-scale deployers the guidance they need to move forward, particularly in Windows-based PC environments which are ubiquitous in government, medical and financial organisations."

R&D Semiconductor Alliance

STMicroelectronics, Philips and Motorola have announced a three-way research and development alliance which will see them invest €2.8bn ($2.5bn) in semiconductor manufacturing over the next five years. The R&D partnership will be based in Crolles (France) where ST and Philips already jointly own a factory.

Infineon Number One Chip Supplier

More than 50% of chip cards shipped worldwide last year contained an Infineon IC, according to Gartner Dataquest's 2001 chip card integrated circuit market study which places Infineon as number one in the market.

The study says that Infineon increased its share of the worldwide market by 4%, with total unit shipments surpassing 51% of all chips sold, including secure memory chips and Smart Card microcontrollers.

Samsung Targets Memory Market

Samsung Semiconductor has launched a new line of Smart Card EMV devices and predicts that it will achieve industry leadership in the Smart Card memory market by 2005.

The new devices include an 8bit CPU, a 32Kb ROM and a 784byte RAM with EEPROM in densities of 2Kb or 4Kb. Also available are 8Kb and higher-capacity EEPROM devices for SIM cards.

First for Philips

Philips has announced that it is the first company to achieve Visa's Level 3 technology approval for a Java Card Global Platform Smart Card controller IC that offers both a contact interface and a contactless interface in its MIFARE PROX card.

Hitachi Dual-Interface Controllers

Hitachi Semiconductor (America) has announced 16-bit Smart Card microcontrollers that provide a dual interface with contact and contactless capabilities in a single chip. The AE45X series devices have a large-capacity on-chip memory with a firewall management unit (FMU) - 36Kb of EEPROM, 128Kb of Mask ROM and 4Kb of RAM - and include a secure encryption processor.

Ericsson to Cut 17,000 Jobs

Ericsson, the Swedish telecommunications manufacturer, has announced plans to cut 17,000 jobs. The announcement has come as a shock to investors, and shares in the group plummeted by 24% - a record one day fall for the company.

The group said it faced a second year of losses, and

was unable to predict an upturn. The job cuts are scheduled to finish by the end of 2003, which follows 25,000 cuts already made since the start of the year.

Nokia Win $50m Thai GSM Contract

Nokia has signed a deal worth $50m with Thailand's largest mobile operator Advanced Info Service to expand the company's GSM network.

Nokia has also signed a three-year frame agreement for the expansion of Ben Nederland's GSM 1800 and GPRS network in The Netherlands.

Afghans to get GSM phone service

The Afghan Wireless Communication Company (AWCC) is to launch a GSM mobile phone network. It will put into place a primary telephony network that will substitute for the lack of fixed-line infrastructure as Afghanistan has virtually no land-line telecommunications. The system has been launched in the capital Kabul, but is expected to expand to Herat, Mazar, Kandahar and Jelalabad in the coming weeks. The Motorola handsets, which will cost $350, will be unaffordable for the vast majority of Afghans so it is hoped that citizens will use the service via public call offices.

Mobile Payment Alliance

Giesecke & Devrient and Euronet Worldwide have signed an agreement to co-operate on marketing mobile phone-based payment solutions. G&D is to provide SIM cards and SIM Toolkit Applications for bill payment, mobile commerce and prepaid reloading of SIM card features, whilst Euronet Worldwide will contribute its mobile recharge, banking and bill pay service applications.

GSM Phones for China

Infineon Technologies has announced that eAnywhere Tech has started mass production of GSM mobile phones for the Chinese market based on Infineon's wireless system platform. Infineon says it will support eAnywhere in the development of GPRS products for the Chinese market.

Largest Asian GPRS Network

Asian GPRS Roaming Exchange (GRX) provider Aicent has announced agreements with leading local mobile operators to create what will be the largest commercial GPRS roaming network in the region. Currently participating in the scheme are China Mobile, Chunghwa Telecom, CTM Macau, Far EasTone Telecommunications, Hong Kong CSL, Hutchison Telecommunications (Hong Kong), Indosat Multimedia Mobile, KG Telecom, MobileOne (Asia), SingTel Mobile, SmarTone Mobile Communications, StarHub and Taiwan Cellular Corporation. The operators collectively represent about 135 million subscribers or 70% of the total Asia Pacific GSM/GPRS subscriber base.

Bluefish SIM Contract in West Africa

Bluefish Technologies has won a contract to supply Smart Card SIMs to a number of mobile operators in West Africa. The deal was initiated with Scancom, part of the Investcom Group. Scancom runs the Spacefon network and has taken on a purchasing role for several other Investcom networks with Bluefish as a partner for SIM card supply.

Other networks include Spacetel in Guinea, Spacetel Benin, Spacetel Burundi and Lonestar Communications in Liberia.

First SIM Card for Pre-teens

Atlas Telecom Mobile and Oberthur Card Systems have developed the first SIM card for pre-teens allowing young users easy access to a wide range of information and entertainment services by SMS via the phone's menu.

Youngsters need only buy a SIMPA SIM card to insert in his/her parent's old mobile. For a minimal one-time investment, the user can send and receive short messages from any GSM phone, anywhere, anytime, and enjoy a high level of control over spending. They can chat with friends, entertain, play games or listen to music. Also, the callback function allows young users to make calls to pre-listed phone numbers (home, parents office and three friends) for the cost of a premium SMS.

For more information visit ...

Visionics
www.visionics.com
Philips
www.philips.com
Samsung
www.samsung.com
Precise Biometrics
www.precisebiometrics.com
Sita
www.sita.int
IBM
www.us.ibm.com
Banque de Luxembourg
www.bdl.lu
Infinion
www.infineon.com
Hitachi
www.global.hitachi.com
Atlas Telecom Mobile
www.atlastelecommobile.com
Oberthur
www.oberthurcs.com
Nokia
www.nokia.com
Ben
www.ben.nl
Bluefish
www.bluefish-tech.com
eAnywhere Tech
www.eanywhere-tech.com
Giesecke & Devrient
www.gdm.de

CTST 2002 in New Orleans

CardTec/SecureTec held this year in New Orleans, USA was a smaller show than usual but most exhibitors agreed that the visitors were genuinely interested in Smart Cards. The fall in exhibition visitors might have had something to do with the fact that if you had not pre-registered you were charged $50 to enter the exhibition. Also, a number of high profile companies were missing, the obvious being Gemplus, Oberthur and IBM.

The main news doing the rounds was company partnering. For example ORGA and Perfect Printing who have 20% of the American market, and TSYS, IBM and Gemplus who plan to create a multi-application Smart Card management system. Visa, Catuity and Welcome Real-time (who appear to have put their differences aside) announced an agreement to collaborate on the development of interoperable solutions for rewards and incentives.

Staff from Smart Card Group entertain visitors to their stand (above, and above right facing page); whilst representatives from Fargo get a head inadvertising (left).

SCM Microsystems and Precise Biometrics said they were jointly developing a Smart Card reader with fingerprint capabilities. Inside Contactless (formerly Inside Technologies) said it was giving OmniTek access to its reader technology and also partnering with NTRU to strengthen their contactless security, and with BNC to provide end to end contactless security for documents used by the Mexican Army. Philips signed an agreement with Sospita to address software piracy.

MasterCard announced specifications for MasterCard Open Data Storage (MODS) an application programming interface (API) for storing and retrieving data - a new addition to OneSMART. Ultra-Scan launched their ultrasonic fingerprint scanner and ASK revealed it had shipped two million contactless paper cards and also met common criteria for their CT2000 contact/ contactless microprocessor card.

Qualteq said it would be licensing its proprietary Foil Card technology to Schlumberger. Sharp Microelectronics introduced an LSI Module with a 1MB Flash memory card with over 125 times more memory capacity. Aspects Software showcased their IDE, a Java Card development tool using a visual environment and templates for rapid applet development.

The PKI Forum published two new papers, PKI Basics - A Business Perspective and PKI Note: Smart Cards.

ID TECH introduced a new reader that reads magnetic and Smart Cards. Both Oberthur and Giesecke & Devrient announced agreements to use biometric security technology from Identix while Datacard said it had signed a letter of intent to use Identix technology for its digital identity solutions.

CTST 2002 proved to be a quieter event than in previous years

ACT announced details of its contract with CH Jones, a fuel-bunkering provider, to provide, initially 50,000 cards with a further 300,000 sourced from ACG. Banrisul announced the imminent release of a public tender for the acquisition of 1.5 million MULTOS cards as Brazilian banks migrate from magnetic stripe to Smart Cards.

MULTOS again received certification ITSEC E6 from the UK's IT Security Evaluation Certification Body for the joint Hitachi/Dai Nippon Printing/MXI MULTOS v4 on the Hitachi AE45C silicon. Philips gained Visa's Level 3 technology approval for a Java card Global Platform Smart Card controller IC offering both contact and contactless interfaces, the first company to do so.

Cardbase Technologies announced the successful completion of interoperability trials of its ChipPurse CEPS for use with Visa's Columbus project which enables interoperability of two different Visa cash technologies based on CEPS using multiple currencies for off-line and on-line transactions.

Identicard showed an interesting contactless multi-layered structure that included an antenna printed onto a new substrate called Teslin. Gemplus announced it had shipped 10 million GemXpress Java technology based cards. Eurosmart released their latest forecasts of chips shipped (see page 99).

Visa unveiled its Rewards Platform to accelerate the adoption of rewards services on multi-application Smart Cards and announced that they had been chosen by South Korea's Hana Bank in conjunction with Daejon city to supply dual interface low cost multi-application cards. Visa also announced that they will be supplying Russia with cards which will combine benefits and payment applications.

GlobalPlatform announced the delivery of the first phase of its Card Compliance Program, a kit consisting of procedures and testing components. SchlumbergerSema introduced its ICitizen card to support Government programs and CIM unveiled its new multi-feeder card processing system.

ST Acquire Alcatel Microelectronics

STMicroelectronics is to acquire Alcatel's Microelectronics business in a deal valued at €390m. Under the terms of the agreement, the two companies will enter into co-operation for the joint development of DSL chip sets and ST will become a preferred supplier of Alcatel.

Chip Revival Lifts Samsung Profits

South Korea's Samsung Semiconductor surprised the depressed semiconductor market by achieving record net profits for the first quarter 2002 of Won1900bn ($1.45bn). The company attributed the success to a recent recovery in semiconductor prices and increased mobile phone sales.

SCM First Quarter Results

SCM Microsystems announced Q1 revenues of $43.4m, which was above the guidance previously communicated by management of $39m to $42m but down 4% compared with revenues of $45.1m in Q1 2001.

NDS Posts Record Results

News Corp's NDS Group, the UK based pay-TV company currently involved in a court case for the alleged disclosure of Canal Plus' Smart Card seurity technology, has confounded critics with a strong financial first quarter performance. Revenues increased by 11% to a record £60.1m ($86m) and operating income rose by 44% to £14.6m ($20.9m).

Gemplus Confident

Smart Card leader Gemplus posted a Q1 net loss of €62.46m ($56m). The company said the loss was smaller than expected and while it expected significant first-half losses it was confident of returning to profit by the end of the year. Operating loss amounted to €66.68m, compared to a loss of €2.52m a year earlier.

PubliCARD Post Mixed Results

PubliCARD reported Q1 sales dropped to $1,199,000 compared to $1,520,000 a year ago, but net loss was cut to $1,125,000 compared with $3,509,000 in Q1 2001. The company attributed the decline in the net loss to work force reductions and other cost containment measures associated with the PubliCARD's exit from the Smart Card reader and chip business.

ActivCard Loss

ActivCard saw revenues increase by 15% in Q1 to $8.2m compared to $7.1m in the comparable period in 2001. However, net loss for the quarter also rose, totalling $28.6m compared to net loss of $371,000 in 2001.

New CEO for Oberthur

Oberthur Card Systems has appointed Pierre Barberis as Chief Executive Officer succeeding Thomas Savare, who becomes Vice President of the Oberthur group in charge of strategy and development. Barberis previously worked for Trigano SA, Crédit du Nord and Group Axa. Since 1991, he has been President of VEV.

SC Alliance Appoint Acting CEO

The Smart Card Alliance has appointed Randy Vanderhoof as Acting President and CEO for the remainder of its fiscal year (ending August 31). A former Smart Card Alliance Board member and Assistant Secretary on the Executive Board, he has recently been serving as a consultant to the Alliance.

Changes at Hypercom

Hypercom Corporation has announced the appointment of John W Smolak as Executive Vice President, Chief Financial Officer and Chief Administrative Officer to succeed Jonathon E Killmer who was COO and CFO and will retire on June 30. Previously, Smolak was the CFO for Suburban Propane, LP.

Catuity Sales Appointment

Douglas Kilgour, former VP for Financial Services at Xdrive Technologies, has been appointed Vice President, Sales and Marketing at Catuity. He replaces Rob Kosnick, who has left the company.

Poor SIM Sales Hit Oberthur Results

Oberthur's Q1 2002 figures reveal that total revenues dropped 10% to €103.6m compared to the previous year. The company cited the lack of demand for SIM cards and an 'unfavourable' comparison with an unusual first quarter 2001 for the shortfall. Oberthur SIM volumes dropped 29% but the microprocessor card, banking and network security sectors all achieved positive growth. However, Oberthur stated that trends in the US market and in the SIM card market were weakening growth objectives for 2002 and prompting the group company to a cautious approach.

For more information visit ...

SCM Microsystems
www.scmmicro.com
Oberthurcs
www.oberthurcs.com

Alcatel
www.alcatel.com
STMicroelectronics
www.st.com

Out of the Box With ACI

by Matt Ablott

Richard Crookston

Smart Cards Now talks to Richard Crookston, Head of Solutions Marketing at ACI, about the launch of EMVEasy.

ACI is not a company high up in the public consciousness despite the fact that is the leading provider of the software sitting behind most of the world's ATM's. According to Richard Crookston, the company would generate a great deal more publicity if its flagship 'BASE24' platform broke down occasionally, but it remains the unspectacular, solid platform that banking institutions like to rely on.

However, ACI's recent work alongside Gemplus and Compaq in launching the EMV midrange banking solution, EMVEasy, has catapulted the company into the public eye. According to Crookston the idea of the 'out of the box' EMV solution arose from a general confusion in the marketplace over the effects of the EMV revolution. Hooking up with Gemplus and Compaq meant that the consortium could handle the entire EMV process from beginning to end and therefore offer a complete solution package.

Gemplus proved an ideal partner for ACI ("It was a mutual coming together," claims Crookston) with the Smart Card giant offering a product range that did not overlap with ACI's core areas - which was not true of many of Gemplus' rivals such as SchlumbergerSema. Compaq were brought on board to supply its ubiquitous Himalaya server.

The EMVEasy solution targets what the consortium calls the second and third tier markets. The banks are defined on card numbers with a third tier bank producing up to 50,000 cards, and tier two covering banks issuing up to 750,000 cards.

"You can't approach a big bank with a packaged solution because they are big and complicated and already have lots of established processes," says Crookston. "However, we decided that a packaged solution would help the smaller banks. There are 23,000 visa member banks globally and we realised that at least 15,000 are ACI customers so the market was already there for us."

Aside from its technical functionality, Crookston emphasises the importance of knowledge and training within EMVEasy. "Because we sit in the middle of the whole transaction process people tend to come to us for advice and guidance," he says. "There is a lot of uncertainly over what EMV really is and what it means for the banks so we decided to go for an consultancy led approach where we could educate and guide. We need to educate the customer. Everything from 'what does EMV stand for?' to the card personalisation and hosting side of things. This means we can ship a box which has all the necessary 'knowledge' to go with it alongside the cards."

In its quest to deliver the complete EMV solution (the project's code name was 'EMV in a box') the company faced some serious hurdles. Foremost amongst these was the regional variations on the EMV theme. In France, for example, Cartes Bancaire has developed a national standard based around existing implementations. Crookston: "In the basic package we are not putting in support for national variations. However, the package has been designed so that where there is national variation, we can add components and launch, for example, EMV Easy Italy. Crucially, the bit that we do in the middle is not effected and the Compaq hardware is not effected."

The other problem was to avoid creating what Crookston calls a 'dead-end' system which would be so rigid it would be impossible to reconfigure. "We wanted to put a pre-configured system in, which is easier to support and easier for the user to change," says Crookston. "This means that if we change the software in six months time we can just send them a new copy to install. The downside is its not quite as flexible as, for example, a Citibank or Bank of America system. The upside is the cost-reduction is quite dramatic."

In December 2001, seven months after the project began, EMVEasy was formerly presented to potential associate members (including Visa and MasterCard). Wincor Nixdorf and NCR were signed up on the ATM side and payment terminal companies' Thales, Ingenico, Intellect and Hypercom were signed as PoS partners. According to Crookston, these associates are currently working on their own programmes that will complement EMVEasy.

Crookston estimates that a three year cost of ownership (a lifecycle that was chosen to match the average life span of a Smart Card) for the entry level system could reach €1m. This could rise to €3m for a mid range customer with a 250,000 card customer base.

"We know we can beaten if someone comes along and says we can do this for a $1m," says Crookston. "But we know we won't be beaten on the completeness of the delivery, and that's the whole objective of the program."

Seizing The Initiative:

Why British Banks Need to Act Now to Promote the Use of Credit Cards in Europe

by Dave Parratt, CMG

Dave Parratt

Like it or not, the Euro is here. With its arrival, traditional barriers to change have had to come down as people are taken out of their comfort zone when it comes to financial matters. An air of receptiveness has ensued as people look forward and consider new ideas like never before. In fact, there has rarely been a better time for UK banks to seize the initiative and mount an attack on the European plastic cards market.

UK cardholders put 8.5% of GDP on plastic compared to less than 1% in France, Germany and Italy. Germany still largely uses cash and Holland favours cheques. Whatever the preference, there is a very large, untapped market which is ripe for the taking. And UK banks, with their ever tightening margins, increasing competition and struggle for lucrative customers, need to be the ones to begin tapping first. The question is how?

At home, the credit card has become more than just a way to postpone paying bills. The payment card is also a sophisticated marketing tool which has been used successfully to increase customer loyalty through incentives such as air miles and points to be exchanged for gifts. In Europe these are relatively new ideas, so UK banks have an instant differentiator. Of course, an element of persuasion will still be required. The answer to this? Marketing and lots of it. The main challenge facing the banks will be a cultural one as people consider why they should abandon methods of payment they are comfortable with. But as guards are down, building a brand and winning customers over should be easier than usual. And isn't paying for cross-border payments by credit card so much easier than grappling with Euro notes and coins?

There is the small matter of competition. In this case, it is actually small. European banks have been preoccupied with preparing for the Euro. In addition, all banks must move to the Europay, Mastercard and Visa (EMV) chip card standard by January 2005. A Smart Card chip will replace the magnetic strip to reduce fraud, cut telecoms costs and improve credit risk management. Such migration requires careful planning, meticulous organisation and efficient processes. It's this kind of major distraction which will ensure that overseas banks have difficulty mounting a challenge to their UK counterparts.

There is also the opportunity to persuade customers in one swoop that a credit card means more flexible finance. In many ways, Europe is more advanced in the use of Smart Cards than the UK, but most schemes are very local and in the early stages of development. If UK banks move quickly, they can steal the march not only on the plastic card market, but also on developing a single, multi-functional Smart Card linked to the medical profession, education, government and other conveniences. ▸

Events Diary

June

3 - 5 Alliance Washington DC Educational Institute and Symposium "Smart Cards in Government - Symposium on Secure Identification Initiatives", Washington Hilton & Towers (off Dupont Circle stop on Metro) Washington, DC, USA

Smart Card Alliance Website: www.smartcardalliance.org/alliance_activities/event_information.htm

4 - 7 International 4 Day Workshop: "Cryptographic Security Aspects of Smart Cards and the Internet", Amsterdam, the Netherlands

Euroforum
Emmasingel 33
Postbus 845
5600 AV Eindhoven
The Netherlands
Website: www.euroforum.nl

19 Latin Cards, Mexico

19 - 21 Smart Cards for Public Transport and Smart Card Security, Fraud Reduction and Revenue Protection (June 21), ExCel Conference Centre, London, UK

IIR Conferences
Tel: +44 (0) 20 7915 5055
Email: registration@iir-conferences.com
Website: www.iir-smarttransport.com

24 - 27 Retail Systems 2002, Conference and Exposition, McCormick Place, Chicago, IL USA

PO Box 332
77 Oak Street, Suite 201
Newton Upper Falls
MA 02464

UK banks need to find another revenue stream if they're to avoid being squeezed out of their own market altogether. Either they take the plunge and transport their bag of tricks abroad to develop and exploit a credit card payment market of £250 billion, or they remain at home and stagnate. The window of opportunity is narrowing as the destablising effect of the Euro reduces over time, so if action is to be taken, it must be taken now. The earlier the European market is approached, the more successful their efforts are likely to be.

Smart National ID Cards:

Practical Use of Technology or Nanny State Gone Too Far?

by Graham Carson, MD ORGA UK

Graham Carson

There is no doubting the potential for the use of Smart Card technology relating to authentication or validation of cardholders. This is a key requirement when attempting to verify identity. It follows therefore that Smart Cards will be seriously considered as part of the ongoing industry and governmental discussions related to identity cards. Identity cards evoke passionate feelings ranging from "I don't want big brother watching me" to "If you've nothing to hide, why worry". When considering identity cards, many argue that we should address the public perception before considering the technology. This argument, however, fails to address the fact that the use of Smart Card technology can only alleviate some of the concerns associated with the use of identity cards.

A citizen may be happy for his or her identity to be verified, but they do not want their every action or movement tracked. Several types of card technology, notably magnetic stripe, would require the use of extensive on-line systems where verifications are processed due to the insecure nature of the card. The intrinsic security of data on the Smart Card, specifically its ability to actively participate in an authentication process, enables validation of identity to be performed in a local environment. Storage of the reference template on the card (probably using biometrics) allows the terminal to perform a verification of identity, without the need to go back to a central database. Terminals could be programmed to verify, but not record. Potentially this could alleviate the need for a central backup. If alternative fallback procedures exist for cases when terminals cannot verify the card or identity, governments would need to present strong arguments for the retention of a backup reference image.

Smart Card technology therefore has a positive role to play in the debate. It would be naive to suggest that it will sway the argument. Smart Cards can provide solutions that other card technologies cannot. Smart Cards also place more of the control into the hands of the public, while providing the identity validation function that governments insist on.

USA
Tel: +1 617 527-7595
Email: info@retailsystems.com
Website: www.retailsystems.com

July

3 - 5 In-Vehicle Telematics, The Mayfair Conference Centre, London, UK

IIR Conferences
Tel: +44 (0) 20 7915 5055
Email: registration@iir-conferences.com
Website: www.iir-conferences.com/telematics

August

19 - 21 Cards Australasia, Sydney Convention & Exhibition Centre, Darling Harbour, Sydney, Australia

Chris Rodrigues
Terrapinn
Tel: +61 2 9210 5756
Email: chris.rodrigues@terrapinn.com
Website: www.cards-worldwide.com/cards_aus_2002

September

9 - 10 Retail EPOS & Cards - Moving Towards EMV, The Hatton, London, UK

Andrew Gibbons
SMi Conferences
Tel: +44 (0) 20 7827 6156
Email: agibbons@smi-online.co.uk
Website: www.smi-online.co.uk/retailepos.asp

16 - 18 e-Safety Congress and Exhibition, Lyon, France

Tel: +31 (0) 30 666 73 88
Website: www.lyon2002.itscongress.org

The (In)Security of Smart Card Chips

by Dr David B Everett, Techical Director - Smart Cards Now

This month has seen the security of Smart Card chips being challenged once again. First there was IBM's attack on the GSM SIM card COMP128 cryptographic algorithm followed shortly afterwards by Ross Anderson's team at Cambridge University with their optical fault induction attacks. Both of these attacks are reported elsewhere in this newsletter.

Some writers in the technical press have described these attacks as one more nail in the coffin of Smart Cards and have proposed that their use in security applications should be discontinued. As always the stories are incomplete and here we will try to give a more balanced view of the real picture.

There can never be perfect security and that has to be the starting proposition for any look at the security of Smart Cards. If you have perfect skills, tools and knowledge then intrinsically you can break the security of any component device such as the Smart Card but not necessarily the overall system. However this situation is not real in that it would require collusion from all the participants, no security system could withstand such an attack. In a more real situation the information is incomplete and the attacker has to use special techniques and tricks to piece together all the detail required to accomplish the attack. The success of these techniques determines the level of skills and resources necessary to complete the attack.

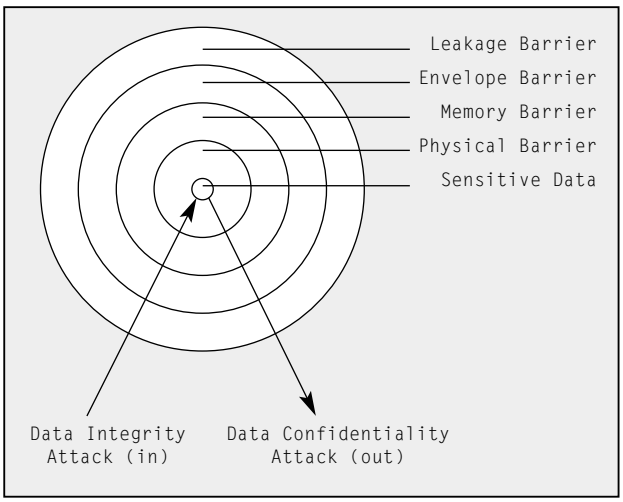


Figure 1: Smart Card Chip Security Barriers

A Smart Card may be considered as a secure store and processor of sensitive data. This data is surrounded by a number of logical barriers that prevent the data being either read or modified. If the data can be read then we have a breach of confidentiality, if the data can be modified then we have a data integrity vulnerability.

In *figure 1* this sensitive data is defined to be surrounded by four logical barriers:

- Physical barrier
- Memory barrier
- Envelope barrier
- Leakage barrier

The physical barrier is concerned with the resistance the chip offers against physical tampering with the electronic circuits whilst the memory barrier is concerned with the hurdles the chip provides against direct reading or modification of the memory cells. The envelope barrier relates to the controls that the chip provides to ensure that the circuit remains within its correct operating environment, halting operation in the event of an unacceptable excursion. The leakage barrier refers to the properties that the chip offers against information being leaked on some covert channel that relates to the underlying sensitive data and in particular the cryptographic keys.

In the early days attacks against Smart Card chips were really attacks against the physical chip where the attacker would probe the circuitry to obtain sensitive information often working on the test mode which used to be a particular point of vulnerability. The process technology of today's Smart Card chips is very small typically 0.35 micron and rapidly moving to 0.18 micron.

Ask the Experts

Q: Are contactless cards more secure than contact cards?

A: The method of communicating with the card should not in itself be part of the security equation. Whether contact or contactless the designer would always assume that the communications path is insecure. Confidential data would normally be communicated to the card in an enciphered form and some form of digital signature would be applied to create source authentication and to protect the data integrity of the message.

The real security issue relates to the architecture of the chip. Most contactless cards in use today are relatively simple memory chips and they cannot be as secure as a specially hardened microcontroller chip. Newer products entering the market place are effectively contact type microcontroller chips with an additional contactless interface. These dual interface cards are sometimes called Combi cards. Such chips present a high work function to the attacker which is the same whether the card is used in contact or contactless mode assuming the appropriate security controls have been applied.

Q: Are contactless cards faster than contact cards?

A: There are actually two separate issues here, the speed of communication and the processing speed of the chip. Contactless cards have a much faster communications rate than contact cards being 106Kbaud versus 9.6Kbaud. There is no intrinsic reason why contact cards shouldn't operate at similar speeds since most now contain hardware UARTs (Universal Asynchronous Receiver Transmitters). However the ISO 7816-3 standard defines initialisation settings that tend to lead to 9.6Kbaud as the normal operating speed. Although the standard includes protocol type selection for enhancing speed after session initialisation very few commercial products take advantage of this feature. Some new Smart Card chips have a USB interface which offers communication rates even better than the contactless cards currently commercially available.

The underlying processing speed is totally dependent on the architecture of the microcontroller and the internal clock speed. Contactless cards have limited power availability and accordingly operate at lower clock speeds than that possible with contact cards. The power consumption is directly related to clock speed. Some of the newer RISC chips often operate with an internal

This makes any form of physical probing attack practically impossible to implement and the attacker is forced to revert to more sophisticated machinery such as focussed ion beam (FIB) devices. In addition it is necessary to know where to probe and since modern chips use complex logic topologies it is very difficult to identify the underlying chip structure. This presents an enormous hurdle to the attacker.

The subject of leakage attacks has attracted the most attention over recent years because in principle they offer the benefit of a 'back bedroom' attack. Three such forms of attack have been exploited in the last few years:

- ☐ Timing attacks (Paul Kosher)
- ☐ Fault induction (Boneh et al; Bellcore Labs)
- ☐ Power and EMR signal leakage (Paul Kosher)

All of these forms of attacks were well known many years ago but the implementers of Smart Card products had under estimated the viability of these attacks and had inadequate controls in their products. The timing attack is based on the principle that sensitive operations take a variable time to execute depending on the data being processed or the keys being used. The fault induction attacks are based on the principle of transiently throwing the processor out of its operating envelope so that it miscalculates some defined part of a cryptographic algorithm thereby enabling the attacker to mathematically deduce the keys. The power signal attack is based on the vulnerability of the silicon chip leaking information in the current (or EMR) signal which is statistically related to the cryptographic keys enabling them to be discovered. Today's Smart Card chips have been designed to offer a high resistance to these forms of attack using a combination of hardware and software defensive features.

Ross Anderson's team have come up with a simple (relatively) way to throw the chip out of its operating envelope using visible light generated from a commercially available photographic flash bulb. What really matters is whether the attacker can use this perturbation in an exploitable way. As mentioned previously defences against all these attacks are dependent on both the hardware and software. Since it is difficult to imagine that the hardware will ever be perfect you need to apply defensive coding to ensure that such attacks cannot be exploited and this is the situation today with most modern Smart Card chips. A well engineered Smart Card product in terms of both hardware and software is not economically feasible to attack.

The particularly interesting point of the Cambridge University paper is their solution to these forms of attack. They have proposed the use of clockless (or asynchronous) logic using complementary dual rail logic. This redundancy makes both fault induction and power signal analysis potentially more difficult. Steve Furber's team at Manchester University first proposed the use of asynchronous logic for Smart Card applications and such an approach certainly has a number of merits. The complementary dual rail technique should help to alleviate the fundamental problem of asynchronous logic in that the power signal is directly related to the data being processed.

Whether such an implementation will prove to present a higher attack work function remains to be seen but it is in many ways a more intrinsically secure approach to the hardware design that may minimise the necessary defensive software programming.

At the end of the day it seems unlikely that any chip would ever be perfect and that the overall security will still be dependent on the quality of the program code. Techniques such as Watchdog Timers provided by some manufacturers can be made to monitor the correct operation of the microcontroller and invoke the old security adage that you can't stop an attack but that you must always detect that it has happened.

Modern Smart Card chips may not offer perfect security but well implemented they offer an unacceptably high barrier to the potential attacker.

clock speed of 40MHz or more and with a 32 bit architecture are potentially much faster than the simpler chips found in the older contactless cards.

Q: Is it better to use Smart Card readers on the USB port of the PC rather than the serial port?

A: Smart card readers are available for the USB port, serial port, and PCMCIA card slots. In all cases (for the Windows platform) your application software would normally interface to the card reader using the PC/SC interface. Although in principle you can interface the card directly using OCF (Open Card Framework) you still need the necessary hardware drivers for the reader and these are usually only provided in PC/SC form. The serial port provides the slowest interface to the PC, this in itself should not be a problem but unfortunately the serial port PC/SC drivers seem more problematic than for USB. In most cases the driver takes charge of the port from start up and cannot be released under software control which is a problem if the port is required for any other application.

The PCMCIA readers are most applicable for Laptop use although these days USB is becoming the cheapest and most reliable connection for Smart Card readers. Most manufacturers have a USB reader in their product range.

Q: Are USB Tokens better than Smart Cards?

The difference between USB tokens and Smart Cards is largely one of form factor and the fact that in a PC environment the USB token does not require a separate card reader. Given that many Smart Card readers emerging today use a USB interface you could argue that the USB token is a better bet. Inside the card or token you will find the same sort of chip. The fabrication of a Smart Card is cheaper than the USB token which requires an expensive connector. In your business case you need to look at the availability of readers in the existing infrastructure and the ratio of cards or tokens to terminals.

It seems highly likely that in the PC world the USB token will be dominant over Smart Cards. The GSM market already has an infrastructure in the phones that uses the ID-000 SIM card format and there seems no reason why this should change. In the financial world the existing and emerging infrastructure is based on the ISO ID-1 form factor and this seems equally unlikely to change.

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 83). Here's a selection of the headlines we covered in April:

Corporate

- ITV Digital To Sue NDS Over Lost Revenue
- PubliCARD Release 2001 Figures
- Chip Sales To Rise In 2002
- Oberthur Release 2001 Figures
- Oberthur Shares Slip After 2001 Loss
- MasterCard Launch US Smart Card Project
- First Data Corp. Acquire Paymap
- Samsung Target Smart Memory Market
- Vodafone Share Collapses Over Growth Fears
- NDS Underfire As Court Case Begins
- Intel Cut Chip Prices
- Compaq And Schlumberger Extend Alliance
- Smart Card Alliance Appoint New CEO
- ST Acquire Alcatel Microelectronics
- Gemplus Shareholders Take On TPG
- US Chipmaker To Acquire Hynix
- Chip Revival Lifts Samsung Profits
- Ericsson to Cut 17,000 Jobs
- Visa Brings Catuity and Welcome Together
- SCM Release First Quarter Results
- G&D Joins MasterCard $2.99 Chip Program
- Poor SIM Sales Hit Oberthur Results
- Visa Sue First Data Over Card Processing Scheme
- NDS Posts Record Results Despite Court Battle
- CardBASE Join Verisign Partner Program

Government

- Dutch Public Record Smart Cards Roll Out
- Entrust Build Smart Portal in UK City
- US Govt. Adopts Datakey Smart Cards
- Ukraine Smart ID Project Enters Second Phase
- Hong Kong ID Card 'Needs Safeguards'
- SchlumbergerSema Introduces ICitizen Smart Card
- Databac Deliver Pass Cards to London Police
- UK Card Fraud Police Unit Goes Live

Banking

- KBC Banks To Issue Proton Smart Cards
- Malaysia Look Toward ATM Smart Cards
- Oberthur And Caradas Launch US Banking Solution
- UK PIN Payment Trial Underway
- Burgan Bank launch ACI Payment Portal
- Visa Launch B2B Payment Service
- ECard Wins Visa Certification
- Oberthur Push Italian EMV Cards
- Hitachi Introduces PIN Secure MultiMediaCard
- CardBASE Completes Multi Currency Visa Cash CEPS Trial
- US Banks Look Smart Despite Slow Uptake
- Cyota And Caradas Launch Verified by Visa Solution
- Paymentplus To Resell Arcot's Verified by Visa Program
- Trintech Solution Certified By UK Acquirers
- VASCO Win Three Latin American Contracts
- Russia Launches Complex Multi-Application Smart Card
- Oberthur Launch Multi Application Smart Card

ID & Authentication

- Security Biometrics Launch Biometric Signature
- Utimaco Safeware Implements Siemens Biometrics Technology
- Datakey Deliver Checkpoint USB Tokens
- Digimarc ID Software Used For Hong Kong ID
- Bell ID Delivers PKI Smart Card Solution to DSV
- Oberthur Join RSA Partner Program 11
- Datakey Introduces CIP Desktop
- Miotec Wins Luxembourg Smart Card Contract

Transport

- Paris Network Debuts New Ticketing Scheme
- EDS Work On US Flyer Smart Card
- Visa Traveller e-Purse Ready For Launch
- US Airports Adopt Visionics Biometrics
- Visa Smart Card Chosen For Payments And Mass Transit In Korea
- Visa to Focus On Airline Smart Card Standard
- Schiphol Group Enlists IBM For Airport Biometric System
- ICTS Launches Smart Card Aviation Pilot in US

Telecoms

- Gemplus And Telemac Launch Wireless SIM
- Alcatel Win African GSM Contract
- Afghans to get GSM phone service
- Broadcom Acquire Mobilink Telecom
- G&D And Euronet In Mobile Payment Alliance
- Operators Sign Up For Largest Asian GPRS Network
- Bouygues Set To Run French 3G
- Nokia To Expand Dutch GSM Network

Retail

- MasterCard Adopts Welcome Loyalty System
- Ingenico Launch Terminal in US
- Shell UK Adopt ReD Pay Terminal

Leisure

- Fraudsters Target Online Gambling
- First Smart Trading Cards Go On Sale

Technical

- New Biometric Software Standard Announced
- New R&D Alliance Eases Semiconductor Worries
- MBU Develop Croatian Smart Card Platform
- Atmel Launch High Security Smart Card IC
- Aspects IDE Java/Smart Card Launched
- MasterCard Publish Data Storage Spec

Misc

- Gemplus Readers Expand Into PC Market
- PayPal Makes First Profit Amid Takeover Rumours
- Imageware Secures Smart Card Printer Agreement
- Eurosmart Issues End of Year Figures
- Advanced Card Award Winners 2002
- SCM And Silitek Launch Smart Card Enabled Keyboard
- Hotel Chain Offers Smart Loyalty Card

Healthcare

- Infineon to Supply Health Smart Cards in Taiwan

Eurosmart 2001 Figures and 2002 Forecast

Eurosmart card shipment figures for 2001 show an increase of 9.2% over year 2000. This compares with the 23% growth rate experienced in 1999 and 12% in 2000. Eurosmart attribute this lower rate of increase to what it describes as the "harsh down-turn" in Global Mobile Telecom expansion. The 2002 forecast is down 5% to represent 60% of the overall chip card market. However, the Brussels-based Smart Card association predicts a 15% growth from year-end 2002 in the microprocessor card sector due to the progression of both the banking sector and to deployments in emerging sectors such as ID and transport. It expects this trend to continue in 2003, for example, in IT/Security where forecasts indicate a doubling of market share (2.1% of the overall chip card market). Pay-TV forecasts indicate a 5% growth in 2002.

Year	Memory	%	Microprocessor	%	Total	%
1999	1031	+14	389	+56	1429	+23
2000	1062	+3	541	+35.9	1603	+12
2001	1152	+8.5	599	+10.7	1751	+9.2
2002	1217	+5.6	689	+15	1906	+8.9

Global trend since 1999

Sector	Memory (Mu)	Microprocessor (Mu)
Government/ Healthcare	16	16
Telecom	1050	390
Transport	27	8
Pay-TV	0	25
IT/Security	0	5
Financial Services	2	140
Loyalty	37	11
Others	20	4
Total	**1152**	**599**

Shipments per sector 2001

Sector	Memory (Mu)	Microprocessor (Mu)
Government/ Healthcare	18	25
Telecom	1100	415
Transport	35	12
Pay-TV	0	35
IT/Security	0	15
Financial Services	2	170
Loyalty	40	12
Others	22	5
Total	**1217**	**689**

Forecast 2002

The Eurosmart figures are closely studied by industry watchers as members of the Smart Card association represent 85 to 95% of worldwide chip card supply in almost all market segments, particularly in the two principal areas of wireless telecom and financial services.

2001 (Mu)				
Area	Memory	%	Microprocessor	%
EMEA	440	38.2	346	57.8
Asia-Pacific	239	20.7	208	34.7
Americas	473	41.1	45	7.5
Total	**1152**		**599**	

Geographic breakdown of card shipments

Contact

- **Astrid Cousin** Eurosmart
  - ☎ +32 2 506 8868
  - Astrid.cousin@eurosmart.com
  - www.eurosmart.com

Smart Reading...

RFID Handbook

Fundamentals and Applications in Contactless Smart Cards and Identification

Second Edition

KLAUS FINKENZELLER, Giesecke & Devrient GmbH, Munich, Germany

Fully revised and updated to include all the latest information on industry standards and applications, this new edition provides a standard reference for people working with RFID technology. Expanded sections explain exactly how RFID systems work, and provide up-to-date information on the development of new tags such as the smart label.

- Updated coverage of RFID technologies, including electron data carrier architecture and common algorithms for anticollision
- Details the latest RFID applications, such as the smartlabel, e-commerce and the electronic purse, document tracking, e-ticketing and payTV
- Detailed appendix providing up-to-date information on relevant ISO standards and regulations, including descriptions of ISO 14443 for contactless ticketing and ISO 15693 covering the smartlabel

0-470-84402-7 April 2003 448pp Hbk
£70.00 / €115.50

Cleanroom Technology

Fundamentals of Design, Testing and Operation

WILLIAM WHYTE, University of Glasgow, UK

- A self-contained guide to cleanroom design, testing and operation
- Includes information and sources of the latest standards, recommended practices, journals, books and internet sites.
- Provides step-by-step guidance to the design and construction of cleanrooms, appropriate testing methodologies and operation for the minimization of contamination

0-471-86842-6 2001 324pp Hbk
£45.00 / €74.30

Smart Card Handbook

Second Edition

W. RANKL and W. EFFING, both of Giesecke and Devrient GmbH, Munich, Germany

From the reviews of the first edition:

Indispensable! ....an invaluable reference to all facets of smart card technology from system architecture to security methods and from manufacturing to testing and quality control.

H. HUBER, EDITOR-IN-CHIEF, CARD-FORUM AND CARD FORUM INTERNATIONAL

0-471-98875-8 2000 774pp Hbk
£80.00 / €132.00

Encyclopedia of Smart Materials

MEL SCHWARTZ

A-to-Z coverage of the entire field of intelligent materials, in a collection of concise entries from the world's foremost experts in the field – including scientists, educators and engineers.

- Includes extensive cross-referencing, bibliographies, and index
- Illustrated with photographs, tables, line drawings, and equations
- Available as an online reference from July 2002: www.interscience.wiley.com/reference/esm

0-471-17780-6 March 2002 1176pp Hbk
£425.00 / €701.30

Smart Card Manufacturing

A Practical Guide

YAHYA HAGHIRI and THOMAS TARANTINO, both of Giesecke and Devrient GmbH, Munich, Germany

- Step-by-step descriptions of the production processes for chip modules, traditional, contactless and dual-interface smart cards
- Guidance on the choice of materials for use in each smart card component
- Coverage of all the major reliability testing methods and test criteria for chip modules and smart cards
- Include the architecture and functionality of the full range of available smart cards along with outlines of the related standards
- An examination of future smart card applications and an overview of chips currently on the market.
- Contact details and relevant web sites for all the major smart card manufacturers and materials suppliers

0-471-49767-3 February 2002 232pp Hbk
£55.00 / €90.80

For the latest information in Communications Technology...

www.wiley.co.uk/commstech/

Featuring our extensive range of new and established titles, this site has been designed to meet the needs of practising engineers, researchers, administrators and students. Features include:

- **Book of the month**
- **What's new?**
- **Journal news**
- **Author news**

How to order...

John Wiley & Sons Ltd
Tel: +44 (0)1243 843294
Fax: +44 (0)1243 843296
E-mail:
cs-books@wiley.co.uk

www.wiley.co.uk

All books are available from your bookseller.

Prices subject to change. Postage and handling additional.

ALH

WILEY

3397