SMART CARD NEWS

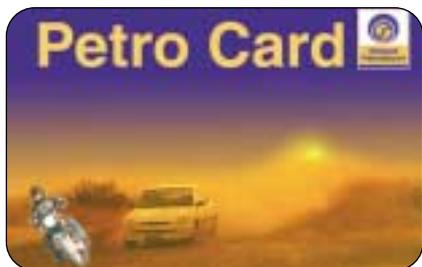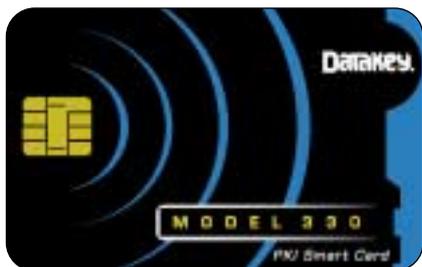*Schlumberger's Millennium Card: free to all subscribers with this issue of Smart Card News*

Schlumberger Announces $3m Investment in ActivCard

Schlumberger's Test & Transactions business unit has made a $3 million investment in ActivCard SA, subject to February 9, 2000 approval of ActivCard's shareholders.

The deal provides Schlumberger with 174,825 newly issued shares of ActivCard stock at $17.16 per share. Separately, ActivCard will include Irwin Pfister, Executive Vice President of Schlumberger, on its board of directors, subject to approval by ActivCard shareholders at its annual meeting planned in May 2000.
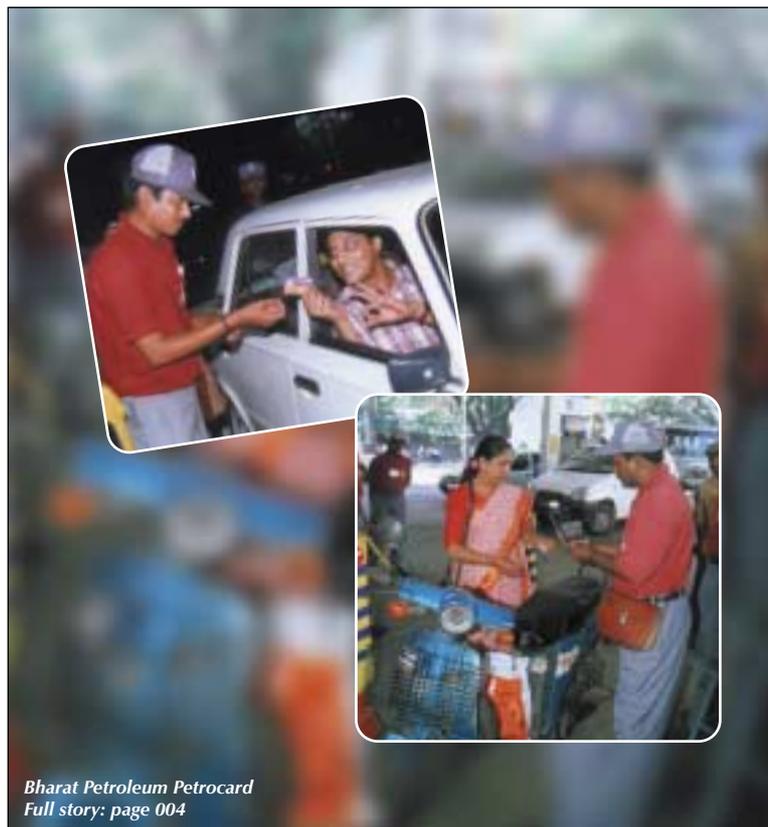
Bharat Petroleum Petrocard
Full story: page 004

CONTENTS

January 2000

News

Special Feature

Smart Card Tutorial

Cards on the Cover
**Schlumberger's
Millennium Card**
Front cover
Datakey
Page 004
ActivCard
Front cover
**Bharat Petroleum Retail
and Loyalty Card**
Page 004

Main Photograph
**Bharat Petroleum Retail
and Loyalty Card in use**

*If you wish to subscribe to Smart Card News
please complete the form on page 019*

Don't Forget!
Our On-Line Website, containing On-Line News, a Library of Smart Cards and information about the full range
of SCN services, can be found at the following address: **www.smartcard.co.uk**

Schlumberger Invests in ActivCard

Continued from page 001

"ActivCard's digital identity technology is a strategic component in the Schlumberger Smart Card-based corporate ID solution for physical and network access, which the company began implementing in five key international locations in 1999 using an internal LDAP directory and Entrust Technology's PKI technology," explained Ashok Belani, Vice President of Business Development at Schlumberger Test & Transactions.

The company says that by delivering Smart Card-based digital identity to ensure user authenticity, their e-business systems provide secure access control, user authorisation, data integrity, data confidentiality and non-repudiation.

Schlumberger has been providing Smart Cards to ActivCard for several years.

ActivCard has corporate headquarters in Fremont, California; Suresnes, France; and Singapore.

Contact

- **Kate Philipps** Schlumberger
  - ☎ +33 (0)1 47 46 70 20
  - 🖳 philipps@montrouge.tt.slb.com

Bull Sells its Stake in Ingenico

Groupe Bull, with the approval of the founding shareholders and the management of Ingenico, has sold its 29,7% holding in the company to a group of investors led by Marc Lassus, founder of Gemplus.

The transaction involved a total of 105 million euros. This operation is part of Bull's divestiture program.

Contact

- **Jean-Jacques Roulmann** Groupe Bull
  - 🖳 jean-jacques.roulmann@bull.net

Spanish/Italian Co-operation

Smart Card companies in Spain and Italy have agreed to work together in an agreement which they say is open to other card and Smart Card manufacturers to promote a worldwide technological co-operation of independent local manufacturers.

Microelectrónica Española SA, a leading Spanish Smart Card company based in Madrid, and Italian Smart Card manufacturer Incard SPA, of Marcianise, announced a co-operation agreement in the development of Smart Card operating systems and applications based on the existing standards for GSM Phase 2+ SIM Application Toolkit, Electronic Purse, EMV debit/credit and ISO 14443 B dual interface contact/contactless Smart Cards.

In addition, both companies agreed to provide each other with future developments in their respective fields of competence as well as to serve each other as second source supplier.

The companies said that the agreement is intended to be open for other card and Smart Card manufacturers in order to form a group of independent local manufacturers jointly developing operating systems and applications as well as Smart Card production and personalisation technology.

In the announcement, the companies said that Dr Lutz Martiny, currently President of the European Smart Card Industry Association EuroSmart, will be promoting the idea of worldwide technological co-operation of independent local Smart Card manufactures.

Contacts

- **Dr Lutz Martiny** EuroSmart
  - ☎ +49 5250 932039
  - 🖳 lmartiny@compuserve.com
- **Alberto Pérez Lafuente** Microelectrónica Española
  - ☎ +34 91 563 6847
  - 🖳 microele@accessnet.es
- **Simone Cavallo** Incard
  - ☎ +39 0823 630416
  - 🖳 scavallo@incard.it

Collector's Corner

The first card in SCN's Collector's Corner, the Millennium Card, could not be more topical and provides a splendid start to what should be an interesting collection of Smart Cards from around the world.

A promotional card, it was manufactured in France by Schlumberger to celebrate the new millennium.

Schlumberger is a pioneer in the Smart Card industry and provides Smart Card-based solutions worldwide which will play a key role in the 21st century's digital age.

003

003

003

003

Datakey Cards in Healthcare Pilot

Datakey Smart Cards have been selected for the HealthKey Minnesota Project, a pilot program designed to enable secure and private healthcare communications over the Internet.

The pilot is sponsored by the Minnesota Health Data Institute, a non-profit organisation dedicated to developing an integrated, state-wide healthcare data system to support providers, consumers, health plans, researchers and policy makers. The project seeks to develop an information infrastructure that will allow the secure sharing of data over the Internet to give users convenient access to information for assessing and improving healthcare.

HealthKey Minnesota will evaluate and test a PKI system for the secure exchange of clinical, administrative and governmental healthcare information.

Datakey Smart Cards will store and process users' digital certificates when they authenticate their identity to a secure Web site, encrypt private documents for secure e-mail, or digitally sign their e-mail or other documents.

Datakey's cards perform on-card key generation, which means that the private key is never available for someone to steal or copy.

Smart Cards also allow for two-factor authentication: to access a secure Web site or to encrypt sensitive information, users must possess both their card and know their password.

"As a result of HIPAA regulations, the healthcare industry must now seriously consider how its information systems will combine privacy and security at an operational level," said John Fraser, Director of Information Services at the Minnesota Health Data Institute. "A public key infrastructure clearly offers the best model. Smart Cards are an important component of this PKI model because they enable an increased level of practical security."

Contacts

- **Colleen Kulhanek** Datakey
  - ☎ +1 612 808 2361
  - ✉ marketing@datakey.com
- **John Fraser** Minnesota Health Data Institute
  - ☎ +1 651 917 6715
  - ✉ john.fraser@mhdi.org

Bharat Petroleum Petrocard

Bharat Petroleum has launched India's first retail and loyalty card for petroleum applications.

Known as Petrocard, the Smart Card system from Schlumberger, allows customers to use an electronic purse to pay for fuel and other goods and to receive loyalty points for purchases.

The oil company is the second largest fuel retailer in India and manages over 4,000 service stations. The card scheme has been launched at 35 petrol stations in Chennai and will be followed by 25 stations in Hyderabad, initially targeting around 30,000 customers. The scheme is being rolled-out nation-wide.

"The fuel retail business is changing rapidly, with moves into new automobile-related services such as car washes, and into new types of retail operations for the mobile consumer," explained S Ramesh, Deputy General Manager for Brands at Bharat Petroleum.

Schlumberger is supplying a microprocessor card from it Payflex family as well as point of sale terminals and a transactions processing server.

Contact

- **B K Wadhawan** Schlumberger India
  - ☎ +91 11 37 37 020
  - ✉ wadhawan@new-delhi.tt.slb.com

CSI Now CardBASE Technologies

Card Services International (CSI) changed its name to CardBASE Technologies as of January 1, 2000, to reflect the focus of the organisation and to provide a .com Internet address for customers and partners worldwide - www.cardbase.com

Founder and Chief Executive Officer, Aonghus Geraghty said: "The new name unifies the company and its product brand. Our core technology, CardBASE delivers the most advanced chip card management product available in the market today."

Contact

- **Aileen Carmody** CardBASE Technologies
  - ☎ + 353 1 284 3233
  - ✉ info@cardbase.com

Schlumberger $7.5m AFC contract

Schlumberger has won a competitive bid to provide a $7.5 million Automated Fare Collection (AFC) system for the Dallas Area Rapid Transit (DART) and the Fort Worth Transportation Authority. The contract includes an NT-based Central Data Collection System (CDCS), ticket vending machines (TVM6000), technical support, project management and installation.

Initially the system will control 65 ticket vending machines (expandable to 400) for the North Central Corridor and the Northeast Corridor light rail build-out projects in Dallas, and for the Trinity Railway Express commuter train which will link Dallas and Fort Worth in 2001.

Contact
- **Emily Hall** Schlumberger
  - ☎ +1 408 437 7268
  - 🖥 ehall@san-jose.tt.slb.com

Pathways $2.3m Private Placement

The Pathways Group, specialists in Smart Card technology, has closed a $2.3 million private placement of 845,200 shares of the company's common stock with a group of private investors organised by Creditanstalt AG of Vienna, Austria.

Carey Daly, Founder, President and CEO of Pathways said: "This private placement has strengthened our balance sheet and fully addressed our short-term capital needs."

Contact
- **Carey F. Daly II** President & CEO
  - ☎ +1 707 546 3010
  - 🖥 @pathwaysgroup.com

Reader for Multiple Card Types

Cubic Transportation Systems, a subsidiary of San Diego-based Cubic Corp has designed the first reader capable of processing three types of contactless Smart Cards, an innovation that will facilitate the mass transit industry's growing use of Smart Card technology.

Using the latest Digital Signal Processing technology, the Tri-Reader processes ISO 14443 Type A and B, and the Cubic GO CARD.

This "universal" feature gives transit authorities the flexibility to systematically build the infrastructure necessary to support a Smart Card-based fare collection system without having to be locked into a particular card type, says Cubic.

Contact
- **Kelly Williams** Cubic Corp.
  - ☎ +1 858 505 2378
  - 🖥 Kelly.Williams@Cubic.com
- **Kim Gregory** Cubic Transportation Systems Inc.
  - ☎ +1 858 627 4587

CyberMark Alliance

CyberMark, supplier of electronic commerce solutions for closed campus environments, has announced a strategic alliance with Coin Acceptors, Inc. of St. Louis, Missouri, to provide the Smart Card marketplace with a system for electronic cash and a loyalty application with vending machines from Coin Acceptors.

CyberMark has already teamed with Microsoft, Gemplus, and First USA, via the SmartWorld Partnership Program to offer comprehensive Smart Card solutions.

Contacts
- **Thomas K. Burke** CyberMark
  - ☎ +1 703 758 8710
  - 🖥 burket@cybermark.com
- **Kevin Ward** Coin Acceptors
  - ☎ +1 314 725 0100, ext. 209
  - 🖥 kward@coinco.com.

Smart "Pay-As-You-Use" TV

FutureTV has launched a Smart Card-based "pay-as-you-use" TV system into the US market. The viewers' account is debited only for the time actually spent watching programs.

Called Mi, the service enables users to navigate the Mi personalised electronic program guide, 24-hour access video on-demand and audio on-demand, receive an unlimited number of live digital TV and radio programs, send and receive e-mail, browse the Internet, shop for goods and services, play games and make low cost telephone calls.

Contact
- **Lynne McMinn** FutureTV
  - ☎ 011-44-20 7969 2749
  - 🖥 Press@futuretv.com

005
005
005
005

Personal ID Role for Smart Cards

Strålfors and Fingerprint Cards have begun collaboration on the development of electronic verification of personal identity for Smart Cards, access control and computer log-on using biometrics. The companies say that finger patterns will replace the PIN code on cards and card sensors, leading to more secure e-commerce, Internet banking and access to sensitive information.

A Letter-of-Intent was signed by the two companies to develop new products and system solutions utilising Fingerprint Cards' patented biometrics technology and Strålfors' know-how and sales channels in the fields of card and computer accessories.

The technology is designed to store the user's identity in the Smart Card chip as a digitized and coded finger pattern. Verification of identity takes place locally in the fingerprint sensor without external computer support.

A pilot project will be carried out by Strålfors during the first half of this year.

"The combination of biometrics and Smart Cards will become very competitive for systems in which a secure and user-friendly technology for determining personal identity is important," said Lennart Carlson, President of Fingerprint Cards.

Per Nyström, Head of Marketing and R&D at Strålfors, explained: "Our collaboration enables us to create more secure and comprehensive solutions in the fields of e-commerce, computer log-on and access control. Biometrics will become one of the most important technologies in the future in this regard."

Strålfors' business concept centers on IT, emphasising computer-related products and services. The group currently has sales of SEK 2.5 billion and operations in 11 countries.

Fingerprint Cards AB has developed a fully integrated, chip-based system for electronic verification of identity and has sold a license to Ericsson for use of the technology in mobile phones.

Contact
- **Lennart Carlson** Fingerprint Cards
  - ☎ +46 3110 0675
  - ⌨ lennart.carlson@fingerprint.se

Hitachi Ships 100 Millionth Chip

Hitachi last month shipped its 100 millionth silicon chip in Europe for its customers manufacturing microprocessor Smart Cards. The chips - ranging from 1 to 32K bytes of EEPROM - are used mainly in GSM SIM cards and banking applications.

"This is another milestone that shows our commitment to the industry and its future," said Ian Hay, Manager of the Smart Card Business Group at Hitachi Europe. "Since entering the market more than five years ago, Hitachi has grown to become a major player in the Smart Card market."

According to the company, Hitachi has invested heavily to become the third largest Smart Card microprocessor chip supplier worldwide, doubling its production capacity in 1998 and again in 1999.

Hitachi has calculated that 100 million chip cards laid end to end would span the distance between Japan and Europe.

Contact
- **Vince Pitt** Hitachi Europe
  - ☎ +44 (0)1628 585163
  - 🖹 +44 (0)1628 585160

Racal Personalisation Package

Racal Security and Payments is offering a low-price off-the-shelf package to personalise Smart Cards for the increasing number of pilot schemes now being undertaken and is targeting Europay, MasterCard and Visa Member banks.

The company says its P3 software suite supports the EMV specifications and enables users to issue cards in-house at about a third of the cost of a full system.

Contact
- **Paul Hanbury** Racal
  - ☎ +44 (0)1344 388000.
  - ⌨ paul.hanbury@racalgroup.co.uk

PubliCARD in Top Ten Companies

PubliCARD was selected as one of the Top Ten Companies to Watch in 2000 in the January issue of Intele-Card News, the prepaid telecommunications industry publication. Every year, the editorial board picks the most promising prepaid and Smart Card companies for the coming year.

Proton/Visa Joint Marketing Plan

Proton World has signed an agreement with Visa International Latin America and Caribbean Region for the joint marketing of Proton-based e-purse Smart Card systems as "Visa Cash-compatible" in most of the Visa LAC region.

The agreement offers Visa member banks an alternative technology for launching new Visa Cash e-purse schemes, although the Visa Cash e-purse programmes in Argentina, Brazil, Colombia and Peru will continue to use the existing technology. Visa and Proton World will draw up joint marketing plans for each country in the region and will make joint sales visits to new and existing customers.

Daniel Skala, Executive Vice-President, Sales, at Proton World, said: "We are convinced that this agreement will open new markets for Visa Cash and Proton World in Latin America. It is a major step forward in our collaboration with Visa, combining the world's most advanced multi-application Smart Card technology with the world's leading international e-purse brand."

Javier Pino, Vice-President, Chip Technology, at Visa International LAC region, said: "Visa is committed to giving its members a choice of technologies and to protecting their investments in Smart Card systems. This agreement with Proton World gives our members maximum choice and promotes innovation in the market place."

Contacts
- **Mr Fran Valmaña** Visa LAC region
  - ☎ +1 305 228 3598
  - 🖳 fvalmana@visa.com
- **Ms Dominique Hautain** Proton World International
  - ☎ +32 2 724 52 53
  - 🖳 info@protonworld.com

EMV for Secure Internet Payments

EMVCo, the Smart Card standards organisation established earlier this year by Europay International, MasterCard International and Visa International to administer the EMV standards, has announced the publication of a jointly developed specification describing how EMV Smart Cards can be used for secure payments over the Internet.

Called Chip Electronic Commerce (CEC), the specification was created under the auspices of EMVCo to extend the EMV Smart Card and terminal standards for interoperability into the quickly evolving virtual world.

Europay, MasterCard and Visa created the CEC specification in an industry-wide effort to maximise member banks' investment in chip infrastructure by ensuring EMV Smart Cards can be used in the virtual as well as physical world. The specification was developed with the assistance of SETCo, the organisation that manages the SET Secure Electronic Transaction protocol, and leverages the open, global standard for secure electronic commerce.

The technical specifications are publicly available on the EMVCo website at: www.emvco.com and on the SETCo website at: www.setco.org.

Contacts
- **Richard Tischler** Europay International
  - ☎ +32 2 352 53 04
  - 🖳 rtt@europay.com
- **Christina Costa** MasterCard International
  - ☎ +1 914 249 4606
  - 🖳 christina_costa@mastercard.com
- **Colin Baptie** Visa International
  - ☎ +1 650 432 4671
  - 🖳 cbaptie@visa.com

First Wireless Banking Service

Canadian network operator Microcell Solutions is to use Schlumberger's Cyberflex Simera Subscriber Identity Module (SIM) Smart Cards and a mobile banking application for North America's first wireless financial services application.

Subscribers will be able to check bank account balances, lines of credit and credit cards, plus their most recent bank account and credit card transactions, any time, anywhere.

Contacts
- **Dirk Hinze** Schlumberger
  - ☎ +33 (0)1 47 46 79 50.
  - 🖳 hinze@montrouge.tt.slb.com

JCB and Sanwa Smart Card Plan

Card issuer JCB and Sanwa Bank are planning to issue Smart Cards as bank, credit and debit cards with an electronic purse in the first half of 2001. Mondex electronic cash is being considered for the purse function.

Industry Review 1999

During the year we saw the continued expansion of Smart Card applications worldwide and many new products appearing on the scene. There were numerous take-overs, company refinancing, joint ventures, agreements and partnerships as the industry geared for further growth in the new millennium.

Acquisitions

Atmel Corporation acquired the Smart Information Transfer business of the Semiconductor Products Sector of **Motorola** at East Kilbride, Scotland, making Atmel the third largest Smart Card IC provider in the world.

Bull merged its payment terminal activities with **Ingenico** making Ingenico the number two supplier of payment terminals worldwide with Bull its biggest shareholder (*see page 3*).

US Smart Card company **Amazing Controls! Inc** merged with **Micromodule Pte Ltd**, a microchip manufacturer and semiconductor packaging plant based in Singapore, to create **Amazing Smart Card Technologies (ASCT)** which was then acquired by **PubliCARD Inc.** Connecticut-based PubliCARD later bought **Absec Ltd.**, of Bangor, Northern Ireland, a provider of chip-based systems for campus environments.

American Banknote Corporation purchased **Transtex SA**, a supplier of transaction cards in Argentina, Chile, Uruguay and Paraguay.

Dutch-based **AXXICON Group**, specialists in Smart Card moulds, completed the take-over of French Smart Card mould producer **SEROPA**.

Hypercom acquired the payment security business of **ICL's Financial Terminals** division in Sweden which is now operated by Hypercom as a subsidiary marketing it's products and services under the name **Hypercom Financial Terminals AB**.

Consult Hyperion, the UK-based IT management consultancy specialising in e-commerce, acquired **Echidna Technology**, specialists in PKI (Public Key Infrastructure) development and integration.

Diebold, of Ohio, USA, acquired **Pioneer Systems Inc.**, a provider of Smart Card systems for college campuses.

Ecash Technologies, based in Seattle, Washington, acquired the technologies of **DigiCash**, including the patented "blind signature" encryption scheme for providing electronic cash on the Internet.

The Pathways Group, Inc announced that it was acquiring **Smart Card Solutions, Inc.**, a technology based company in Aspen, Colorado.

French Smart Card software integrator **Datagrams** bought out the **TouristCard Corporation** and now holds 84 per cent of its shares giving it exclusive rights to use the TouristCard application worldwide.

Schroder Ventures, an international private equity group, took over Swedish IT group **AU-System**. Schroder owns close on 75 per cent of the shares and is investing SEK 1 billion (US $135 million), including SEK 200 million to fund investments in new products and markets.

Financing

Payment terminal manufacturer **Dione** received a £4.7 million capital injection from **GE Equity** to increase working capital and fund further international expansion.

PubliCARD Inc announced a private placement of shares resulting in $19.3 million to finance the development of Smart Card products for the Internet and e-commerce markets and for strategic acquisitions within the Smart Card industry.

Thyron, UK provider of secure payment solutions for electronic and mobile commerce applications received a US $9.6million (£6 million) investment by US-based **Warburg Pincus Equity Partners** and **Warburg Pincus Ventures International**. The company is expanding its sales force and creating a global network of sales and support offices.

Card production

Gemplus and **American Bank Note Company** formed a joint venture, **Gemplus Bank Note Ltda**, based at ABN's existing factory in Barueri (São Paulo), to manufacture and personalise Smart Cards and develop software solutions for the Brazilian market.

The largest IC card manufacturing plant in China was inaugurated in Beijing. A joint venture between **Tianjin Telephone Equipment Factory** and **Gemplus**, the **Tianjin Gemplus Smart Cards Co.**, can produce 80 million cards per year.

Giesecke & Devrient opened subsidiary companies in Australia and South America - **Giesecke & Devrient Australasia Pty Ltd** to deliver Smart Cards for the Australian and New Zealand markets and production support for G&D initiatives throughout South East Asia; and **Giesecke & Devrient Brasil** in Sao Paulo, Brazil, with two divisions: cards and currency automation systems.

Gemplus announced plans to manufacture Smart Cards in Melbourne, Australia, in a A$32.5 million joint venture with Australian-based plastic card giant **Leigh-Mardon**.

Giesecke & Devrient agreed with Russia's banknote printer, **Goznak** of Moscow, to design and build a chip card factory at Goznak's premises in Moscow to produce all types of plastic cards for the Russian payment card market.

Schlumberger purchased an 80 per cent share in **CardTech**, a Brazilian magnetic card company for financial markets. CardTech, which has headquarters in Curitiba and facilities in Sao Paolo and Curitiba, specialises in credit and debit and is Visa and MasterCard certified for card personalisation.

Oberthur Smart Cards USA launched its new manufacturing plant with the capacity to produce over 200,000 Smart Card modules a day. The 3,000 square-foot facility can process unsawn silicon wafers into encapsulated modules completely within Oberthur's Southern California manufacturing operations.

Gemplus shipped its 10 millionth contactless Smart Card. It was presented to **Cubic** for use by the Chicago Transit Authority.

The former **Siemens** microchip plant on North Tyneside, England, which was closed following a slump in the price of semiconductors, found a temporary occupant. **Orange** is to use the nearly-new £680 million plant as a call centre for its GSM phone network.

Chips
Hitachi announced a new Smart Card microcontroller, the H8/3158, with 46K bytes ROM, 1K byte RAM and 16.5K bytes of EEPROM.

Samsung Electronics and **Samsung SDS** unveiled a new combination card chip - the first of its kind in Korea. Samsung said the new combi-card with 8K bytes EEPROM and 24K bytes ROM, was the first single chip in Korea that included both contact and non-contact formats.

MasterCard International, **Keycorp** and **Infineon Technologies** announced the availability of the world's first 16K MULTOS chip based on Infineon's cryptocontroller SLE66CX160S. MULTOS is the open, multi-application operating system for Smart Cards.

Company changes
Bull's card production site at Byfleet, near London, changed its name from **Bull Smart Cards & Terminals** to **Bull Card Systems**.

The acquisition of the Scottish-based terminals business of **De La Rue** by French **Ingenico Group** resulted in the new company being named **Ingenico Fortronic**. Established in 1972 as Fortronic Ltd, the company had its name changed when it became part of De La Rue Card Systems in 1997.

ICL merged its five Swedish companies - ICL Svenska, ICL Sorbus, ICL Retail, ICL Financial Systems and ICL Financial Terminals - under the new name **ICL Sverige AB**.

Australia-based **ERG** brought two of its subsidiary companies under the ERG brand name. **AES Prodata**, specialists in automated fare collection, became **ERG Transit Systems**, and telecommunications infrastructure provider **Australian Power Industries (API)** became **ERG Connect**. The other subsidiaries which represent the core activities of the ERG Group are **ERG Card Systems** and **ERG Telecommunications**.

Gemplus announced **Gemplus Software**, a new division to focus on delivering software products to its Value Added Resellers (VARs), developers, partners and customers.

Siemens Semiconductors was spun off on 1 April to form **Infineon Technologies** with headquarters in Munich.

Datacard Corporation formed its three core business units into autonomous companies called **Datacard Worldwide**, **Credentia** and **MedAssure**.

Alliances

Schlumberger signed a memorandum of understanding with **Keyware Technologies** to combine Schlumberger Smart Card technology with Keyware's Layered Biometric Verification (LBV) technology such as voice, face and fingerprint.

Philips Semiconductors and **IBM Research** teamed up to develop next-generation 16-bit multi-function Smart Cards for secure uses such as banking, electronic purse, medical records, secure authentication and customer loyalty programs.

Software firm **UbiQ Inc** and French company **Gilles Leroux** agreed to provide a comprehensive solution for high-speed, high-volume Smart Card personalisation by combining UbiQLink Smart Card personalisation software with Leroux's Revolution 3000 line of card issuance equipment.

HyperSecur Corporation and **STMicroelectronics** signed an agreement giving STMicroelectronics the exclusive license to implement HyperSecur's Hyper-Proximity technology as a standard feature on its contactless microcontrollers.

Bull Smart Cards and Terminals signed an agreement with **Proton World** to become a worldwide, non-exclusive Value-Added Reseller (VAR) of Proton for Windows/NT.

Mondex International and **Digital Courier Technologies** announced an agreement to collaborate on a worldwide alliance providing for the integration of Mondex electronic cash payment capabilities with Digital Courier's Internet payment products and services. Digital Courier is installing a payment gateway in the UK and US that will "Internet enable" Mondex electronic cash. The gateway will allow Digital Courier to act as a currency exchange or Bureau de Change facility for value loading in multiple currencies.

Giesecke & Devrient, **Motorola** and **Atos** teamed up to offer GeldKarte customers multimedia banking and payment systems on the move, including e-purses.

Orders

IC One Inc and **Schimatic Cash Transactions Network.com, Inc (SCTN)**, which merged their technologies under the name IC One, Inc, announced a three-year $300 million contract with Global Capital and Rent Smart Publications to introduce the "Rent Smart Card" and Internet enabled set-top boxes to tenants in apartment communities.

Gemplus was contracted to supply two million Smart Cards and 5,500 card readers to the Slovenian Health Insurance Institute in a FF50 million contract for an advanced health and health insurance system.

Awards

The Advanced Card Awards 1999, presented during the Smart Card '99 conference and exhibition in London, went to:

BT Most Innovative Product of the Year: **NEC Electronics (France) SA** for FeRAM (Ferro-electric RAM).

Thomas Cook Global Services Best Loyalty Application: **Gemplus** for the Community Rangers loyalty scheme.

Bull Best Transport or Travel Application: **Transmo Citycard** for the UK's Hertfordshire County Council Smart Scheme for bus travel.

Best Communications Application: **Logica** for the Logica m-commerce server suite.

STMicroelectronics Best New Security Product: **Schlumberger** for Sishell which applies a silicon security shield over the chip during manufacturing.

Best New Chip: **Philips Semiconductors** for the MIFAREPRO dual interface Smart Card IC.

Best Marketing Campaign: **Touch** for the Nottingham Citycard in the UK.

A special award, the ORGA Industry Lifetime Achievement Award, went to Smart Card pioneer **Juergen Dethloff**.

France Télécom awarded its Cygne d'Or (Golden Swan) award to **Landis & Gyr Communications** "for exceptional standards of equipment and service."

Chicago O'Hare International Airport's Universal Air Cargo Security Access System combining Smart Card and biometric technologies won the Innovative Security Application Award at CardTech/SecurTech '99. The system uses Smart Card technology from **Schlumberger** and fingerprint biometric identification from **Identix**.

Canadian network operator **Microcell Solutions** was awarded the Outstanding Smart Card Award presented by the Smart Card Industry Association at CardTech/SecurTech '99, for its use of contactless Smart Card technology for an electronic road toll system.

010

010

010

010

Sesames 99 Awards at the Cartes 99 Show in Paris for the Best Applications went to:
Transportation: **ASK** for GTML (Generic Transport Mask) designed for secure multi-modal ticketing in automatic fare collection systems.

Banking and Finance: **Proton World** and **Gemplus** for the CEPS Compliant Proton Electronic Purse.

Loyalty: **Unicom Consulting** for uniLoyalty, a system for companies' customer relationship management, universities, exhibitions etc.

GSM: **Oberthur Card Systems** for Mobile Commerce SIMphonIC, developed as a new payment method for **France Telecom Mobile**.

e-commerce: **Euritis SA, groupe Gemplus**, for Sedodel System, described as providing electronic contents to visually impaired people.

Healthcare: **Novacard** and **Zorg en Zekerheid** (health insurance card issuer) for Smart Card with integrated fingertip sensor (FingerTIP from **Infineon Technologies**). Currently being used in a pilot scheme for patients with Parkinson's disease, the project was also awarded the National Chipcard Award 1999 of The Netherlands.

Identification/Security: **Xiring** for XI-SIGN, a pocket device for secured payment and digital signatures communicating wireless with any multimedia PC or any phone.

Technological Innovation: **Gemplus** for SMARTX technology which allows Smart Card programming to jump directly from first generation, low-level languages to modern fifth generation, high-level development environments.

Sesame for the Best Application (among the winners) - **Oberthur Card Systems** for SIMphonIC.

Third Millennium's Template-on-a-Card security solution incorporating tssi's Verid fingerprint reader, won the Millennium Innovation Security Product Award promoted by Security Management Today and Security Installer. The system allows a user's fingerprint template to be stored on a magnetic stripe or proximity Smart Card.

AU-System was named the IT Company of the Year, 1999 by Swedish weekly business magazine Veckans Affärer. AU-System Mobile is a company within the AU-System group that develops and sells software for value-added services based on Smart Card technology (SIM cards) to GSM operators.

Some highlights

One of the highlights of the year was the market gains by two companies - **ERG** of Australia and **Motorola's** Worldwide Smartcard Solutions Division in the US. Mainly in partnership they blazed their transit trail across a large part of the world - Hong Kong, Singapore, Australia, USA, Germany, Italy and the UK

ERG was awarded a HK$23 million contract by New World First Bus to bring its 700 buses into Hong Kong's multi-modal contactless Smart Card fare collection system known as the Creative Star Octopus System.

The Alliance, as part of a consortium involving **Singaporean Technologies Computer Systems**, **Keppel Engineering and Knowledge Engineering**, was awarded a US $78 million contract to supply an integrated Smart Card fare collection system for the public transport network of Singapore.

Australia's largest private bus operator, Westbus, announced it was equipping its fleet of 400 buses in Sydney with ERG's Smart Card-based Automated Fare Collection (AFC) system. ERG has already supplied AFCs for all State Transit Authority buses and is currently supply STA ferries.

The Alliance was contracted by BVG, the Berlin Transport Authority, to trial Smart Card electronic ticketing covering Berlin and the surrounding greater Brandenburg area. BVG expects full system implementation and public availability by 2002.

Further good news for ERG came with the announcement of an Aus$3 million grant from the Commonwealth Government's Industry Research and Development Board to further develop ERG's multi-application Smart Card system originally designed for Hong Kong. The Octopus system (see above), will be used as a base for a similar system which can be scaled down to meet the needs of any city. ERG will supplement the grant with a further Aus$14 million on the project over the next 12 months.

011

011

011

011

The Alliance also landed the largest Smart Card fare collection system contract yet in the United States covering train, light rail, bus or ferry public transport throughout the nine-county San Francisco Bay Area using a single regional Smart Card by the year 2002. The system is called TransLink and the Alliance will receive between $114 million to $157 million - depending on rider usage - to install and operate the system for 10 years.

Rome's Metrebus Integrated Smart Card Fare Collection project contract was awarded to the Alliance. Under the nine-year contract, the Alliance will design, supply and operate the system for the bus, rail and tram networks in the Italian capital and the surrounding region, involving 5,000 buses, three light rail lines and 76 rail stations.

Motorola was awarded a 14 million guilders (£4.1 million) contract to trial a contactless Smart Card AFC system, called Tripperpas, on buses in the city of Groningen in The Netherlands.

ERG, **Stagecoach** and **Sema Group** joined forces to provide multi-application Smart Card technology across the UK, with Manchester as the first British city to have a large-scale Smart Card-based public transport ticketing system. Stagecoach Holdings plc and Sema Group bought shares in ERG-owned **Prepayment Cards Limited (PCL)**. Stagecoach owns 20% of PCL, Sema 10% (with an option over a further 10%) and ERG 70% (and has committed to sell down to 20%). PCL also announced a major contract with Stagecoach to provide Smart Card payment systems for all of its buses in the region.

ID Data entered Smart Card market
Plastic card manufacturer ID Data Systems of the UK suddenly entered the Smart Card market, and within a few months claimed the number one position in the UK and credibility as a major player on the international scene. It began with a joint venture with the **Toshiba Corporation** and **Toppan Printing Co** of Japan to form **TTI Card Technology Europe**. (ID Data and Toshiba hold an equal shareholding of 43% with Toppan holding the remaining 14%.) Then ID Data acquired the assets and staff of **GPT Card Technology's** Smart Card operations based in Coventry, UK. The deal gave ID Data the capacity to produce some 150 million Smart Cards and become GPT's card supplier under a five-year agreement. This was followed by the purchase of the assets and business of **McCorquodale Card Technology**.

Chip card roll-outs
UK banks began the nationwide roll-out of bank payments cards with an EMV-compatible chip to replace magnetic stripe cards.

Visa of Brazil, with 13 member banks, announced plans to replace 21.5 million magnetic stripe credit and debit cards with multi-application chip cards over the next three years.

Slovenska Sporitelna - one of the biggest issuers of Maestro debit cards in the Slovak Republic - began migrating its 300,000 cardholders to EMV-compliant chip technology.

Japan's **MYCAL Card Company** began converting its five million-plus cards from magnetic stripe to multi-application Smart Cards. The first phase includes the issue of more than 500,000 MasterCard cards using the MULTOS operating system.

Top ITSEC security rating
The first implementation of the MULTOS Smart Card operating system on **Hitachi's** 8K bytes EEPROM H8/3112 chip was awarded **ITSEC Level E6 certification** - the highest security rating achievable in ITSEC (Information Technology Security Evaluation Criteria), security evaluation. In another announcement, **Mondex International** said that Mondex electronic cash had become the first MULTOS application to also attain ITSEC Level E6.

De La Rue sold card business
De La Rue sold its Card Systems division to **Francois-Charles Oberthur Fiduciaire** of France. The £200 million deal involved a cash payment of £170 million and Oberthur taking over debts of around £30 million.

Multi-application cards will fail, says Forrester
Forrester Research rocked the Smart Card industry with the prediction that multi-function cards, viewed by many companies as the way forward, would never materialise. In its report called *Europe's Smart Card Fallout*, Forrester Research said the current move towards multi-application Smart Cards would fail. Instead, the report predicted that firms would issue company-specific cards that allowed customers to access networked applications and that electronic identification would be a key functionality.

Amex on-line credit card

American Express launched Blue, a Smart Card credit card enabling customers to pay bills on-line, download information and review a variety of entertainment content with a fraud protection guarantee. Amex is said to have spent $45 million on the launch but remains coy about the actual number of cards issued, telling SCN only that the number of applications are "extremely high." The Blue card retains the traditional magnetic stripe that can be read at point-of-sale terminals when shopping in the physical world.

Internet services

Belgacom, the communications and multimedia Internet Service Provider, announced Carte Jeunes to provide Internet services plus personal Smart Cards for youths in Belgium, using cards supplied by **Giesecke & Devrient**.

Schlumberger supplied **La Poste**, the French national postal service, with Smart Cards for its Cyberposte program providing "Internet for all," via multi-media kiosks located in post offices.

Biometrics

ORGA won a multi-million DM contract to supply India's first Smart Card-based driver's licence system using fingerprint technology. The project, in the state of Gujarat, is for an estimated 10 million driver's licenses.

Israeli Ministry of Defense announced plans to combine Smart Card and biometric technologies to control border crossings on the Gaza Strip and awarded the contract to an international consortium headed by **EDS Israel** with **Oberthur Smart Cards USA** and **On Track Innovations** as the prime Smart Card contractors. The system will authenticate an individual's identity by incorporating the use of contactless microprocessor-based Smart Cards and two biometrics - face recognition technology from **Visionics Corporation** and hand geometry from **Recognition Systems Inc**.

Record sales

Hypercom announced the shipment of its three millionth point-of-sale terminal.

MULTOS

MULTOS, the open Smart Card operating system, started to penetrate the market with cards issued, a reported order bank in excess of 1.5 million cards and commitments for 14 million. The operating system also won the approval of the Australian Government which said that all government tenders would be based on the MULTOS platform.

Loyalty Rail Card

French national rail operator **SNCF** launched Grand Voyageur one of the first French loyalty schemes to be based on a microprocessor card. SNCF decided to reward its best customers - the five per cent of passengers who account for a third of all main line revenue. In exchange for points, Grand Voyageur cardholders receive rail travel bonuses (in the form of train tickets) or a range of ancillary services (hotel accommodation, restaurants) supplied by partners. **Bull** supplied SNCF with over 300,000 microprocessor cards manufactured at its UK plant.

New Crypto Java Card

Schlumberger launched a new Java Smart Card combining multi-applications with built-in cryptography. The card allows transactions, including the remote loading of applications, to be authenticated using digital signatures. Called Cyberflex Access, the card has 16K bytes of EEPROM and a comprehensive cryptographic library including RSA, DES and triple DES algorithms and the SHA-1 hashing utility.

Microcontroller for Java Cards

STMicroelectronics' ST19SF64 chip - aimed at high end telecom, Java cards and similar multi-application cards - entered volume production in the first quarter of the year. The new device featured an enhanced Memory Access Control mechanism, 64K bytes of EEPROM and 32K bytes ROM.

First version of CEPS published

A further step towards achieving interoperability of electronic purse programmes was taken with the publication of the first version of the Common Electronic Purse Specifications (CEPS), jointly developed by **Europay International**, **SERMEPA** of Spain, **Visa International** and **ZKA (Zentraler Kreditausschuss)** of Germany.

Microsoft toolkit

One year on from **Microsoft's** announcement that it was developing a new operating system, the company unveiled its Windows Smart Card Toolkit.

Electronic purses

Securecard Trust Company, of Lagos - set up to develop a national Nigerian electronic purse scheme - became **Proton World's** first licensee in Africa.

013

013

013

013

BBS (Bankenes BetalingsSentral AS) acting on behalf of the Norwegian banks signed an agreement with Proton World for the pilot implementation of an electronic purse based on the Proton Smart Card technology. It is planned to issue the cards to pay-TV subscribers who will load value into the e-purse from their bank accounts to pay for pay-per-view television programmes via existing set-top boxes.

Mondex International demonstrated the first multi-currency Smart Card capable of carrying an electronic version of the Euro in January - only 13 days after the official introduction of the new European currency.

Mondex International sold its electronic cash franchise for Japan to a consortium of three major financial institutions - **Sanwa Bank**, **JCB** and **MasterCard International**.

Five financial institutions - **Banco Mercantil CASA** (Banco Universal), **Banco Union CA**, **Consorcio Credicard CA**, B**anesco Banco Universal SACA**, and **InterBank CA** - purchased the franchise rights for Mondex electronic cash in Venezuela.

The Eastern and Southern African Trade and Development Bank (PTA Bank) purchased the franchise rights for **Mondex** electronic cash. The deal, on behalf of the Committee of COMESA Central Bank Governors, followed five existing Mondex franchises in Africa (South Africa, Lesotho, Namibia, Swaziland and Ghana).

Mondex Korea is to roll-out in Year 2000 nearly 400,000 multi-application Smart Cards using the MULTOS operating system for debit and credit application, loyalty programmes and ID and access. Gemplus was selected as a strategic partner to supply the cards and to provide consulting services.

Also in Korea, **Visa** and its Members in Korea are planning to phase out magnetic stripe technology in favour of EMV compatible Smart Cards supplied by **Schlumberger**. The first 40,000 cards will be introduced in the Yoido financial district of Seoul.

Government
The UK government said it was backing road toll collection trials to take place on motorways and roads around Edinburgh in Scotland and Leeds in England to charge drivers for entering congested areas. Smart Cards would be placed in the windscreens of vehicles; roadside sensors would read the cards and the toll would be automatically debited from the card or the driver's account. No charges would be made during the trials and no start date was given.

Finland announced it was launching a Smart Card-based electronic identification programme which is the first of its kind in the world. The first cards, known as EIDcards, will be issued by the **Finnish Population Register (VRK)** and allow holders to be positively identified over the Internet when exchanging data or using e-business applications.

A Smart Card ID to electronically deliver a range of government services to over five million citizens is being launched in **Portugal**. **Certipor**, a consortium of Portuguese businesses, will issue digital certificates as the country's National Certification Authority (CA) on behalf of **Imprensa Nacional** (the Portuguese National Mint), which will establish the infrastructure to support the government's electronic services initiatives. Each citizen will receive a Smart Card with identification information to be used for voting, health services, library access, school and college activities.

The Portuguese tax authority (**Direco das Contribuices e Impostos**) introduced Smart Card technology to simplify tax payments and reduce the volume of paperwork. The project involves **SIBS (Sociedade Interbancaria De Servios)**, the Portuguese Inter-bank Consortium, which signed a contract with **Bull** for a first delivery of 100,000 microprocessor cards.

The **US government's General Services Administration (GSA)** launched the first Open Platform Smart Card programme in the US using **Sun's** Java Card technology. It partnered **Citigroup's** e-Citi unit and **Visa USA** in the scheme. The multi-application GSA Smart Cards combined official GSA employee identification with applications such as access to buildings and IT resources, secure e-mail and property management, and the standard credit payment of a government travel and purchase card. Technology components included magnetic strip, contact and contactless Smart chips and fingerprint biometrics.

Mexico selected Smart Card technology for its national vehicle registration system starting early in 2000. A consortium, including **Gemplus**, **Talsud** and Mexican entrepreneur **Henry Davis**, won the contract to supply and operate the system.

BoA Smart Card Authentication

Bank of America, the largest bank in the United States, is to implement a Smart Card-based authentication product based on public key infrastructure (PKI) security technology for its electronic commerce customers.

Litronic, a developer of Internet security solutions, will implement the Identrus platform and provide Smart Card integration, including card issuance, life cycle management and card use by clients.

"Identrus is a global effort through which Bank of America plans to deliver a standard and open solution that securely confirms a trading partner's identity and works for all members worldwide," said BoA's Program Manager, Marilyn Bullock.

Contact
- **Gina Ray**
  - ☎ +1 949 224 4023

Nanopierce $4 Million Financing

Nanopierce Technologies has closed an equity financing of up to four million dollars with Equinox Investors, LLC, of New York City.

Paul Metzinger, CEO, said, "This financing will permit the company to immediately implement our strategic business plan to capture our share of the explosive growth in the Smart Card industry."

Contact
- **Paul Metzinger** Nanopierce Technologies
  - ☎ +1 303 592 1010
  - 🖥 www.nanopierce.com

Bridging the Wired & Wireless

Datakey is to use Certicom Corporation's elliptic curve cryptography (ECC) technology to enhance its Model 330 Smart Card, the first 2048-bit RSA Smart Card offering 32K of EEPROM, to address public key security issues in both the wired and wireless technology environments.

Contacts
- **David Krane** Certicom Corp.
  - ☎ +1 510 780 5420
  - 🖥 dkrane@certicom.com
- **Colleen Kulhanek** Datakey
  - ☎ +1 612 808 2361
  - 🖥 marketing@datakey.com

Smart Readers for Notebooks

Gemplus is to license its GemCore technology to O2Micro, a supplier of ICs to notebook manufacturers, to deliver a new CardBus IC, SmartCardBus, providing built-in reader technology for notebook computers.

GemCore is a Smart Card reader solution that provides electronic equipment manufacturers with access to Gemplus' reader operating system, interface chips and engineering support. By combining the capability of a Smart Card reader and a CardBus controller in a single chip, O2Micro's new SmartCardBus product line will eliminate the need and additional costs of supplying an add-on PCMCIA reader.

Contacts
- **Tarvinder Karsandh** Gemplus
  - ☎ +1 650 654 2917
  - 🖥 tarvinder.karsandh@gemplus.com
- **Richard Brayden** O2Micro
  - ☎ +1 408 987 5920, ext. 8004
  - 🖥 richard.brayden@o2micro.com

ICMA Spring Workshops

The International Card Manufacturers Association (ICMA) has announced that its Educational Institute 2000 Spring Workshops will be held in Houston, Texas on March 29-30, and in Paris, France on April 11-12.

Contact
- **Mary Kay Metcalf** ICMA
  - ☎ +1 609 799 4900
  - 🖥 mkmetcalf@icma.com

Appointments

The US Smart Card Forum has appointed to its Board of Directors Ann Kennedy, Vice President and General Manager for global Smart Card business development at First Data Corporation; and William Randle, Executive Vice President and Managing Director of Direct Access Financial Services for The Huntington National Bank.

Mars Electronics International has appointed Matthew Shaw as Sales Manager responsible for MEI's cashless payment system MultiCard Smart, a Smart Card-based solution for vending, catering and security applications.

015

015

015

015

Briefing notes on Multi-Application Smart Cards – Part 3

Before looking at the open Platform (OP) in more detail it is useful to go back to basic principles and look at the underlying concepts necessary to install an application onto a multi-application Smart Card. The first point to appreciate is that there are two classes of security domain (*figure 5*), the platform security domain for which there is only one and the application security domain for which there can be more than one. In the limit there could be one security domain for every application loaded onto the card. In fact if the application providers are commercially unrelated you would expect them to manage their security on an individual basis.

It is clear that the security of an application is totally dependent on the security of the platform. This means that the platform must be implemented correctly against a well founded design. In terms of the implementation we include the operational processes by which the software and cryptographic keys are installed in the card. The risk taken by the application provider is actually based on the risk presented by the platform. It is pointless for the application provider to carefully protect his cryptographic keys if the platform hands them out to all and sundry. This is why it is essential for the platform to be subject to some evaluation and certification process. Later on we will look at ITSEC and Common Criteria which are the two main processes used to provide this necessary assurance. We also note here that the application provider needs to be assured that he is installing his application on an authentic platform which has been correctly certified. One obvious attack is to persuade the application provider to load his application onto a platform masquerading as the authentic platform but containing trap doors that allow the application security to be disclosed.

There are principally three security services involved in the management of multi-application cards:

- Entity authentication
- Data Integrity
- Data Confidentiality

Various cryptographic algorithms can be applied to produce these security services. We refer to symetric algorithms such as DES (Data Encryption Standard) and asymmetric algorithms such as RSA (named after the inventors Rivest, Shamir and Adleman).

For our discussion here the principle properties can be understood by referring to *figure 6*. If the keys used for the encipherment and decipherment operation are the same then the cryptographic algorithm is symmetric. When the keys are different then the algorithm is asymmetric. The problem with symmetric algorithms is that the source and destination nodes must share the same secret key. The security of distributing the keys and their storage is dependent on both parties applying the necessary security processes. We shall see later that the key management for symmetric algorithms is more involved than that for an asymmetric algorithm. Of course nothing is for free, the execution of asymmetric algorithms is more processing intensive and we need to be assured of the authenticity of the public part of the key pair. For such an asymmetric or public key algorithm one of the keys is normally made publicly available but we shall note that this is not a necessary property and some security schemes keep both keys secret.

The data confidentiality service is provided by enciphering the data with the secret key in the case of the symmetric algorithm or the public key in the case of the asymmetric algorithm. The data is recovered by deciphering the cipher with the same secret key in the case of a symmetric algorithm or the secret key of the public key pair in the case of the asymmetric algorithm.

The data authentication and integrity services are often combined as one operation. In the case of a symmetric algorithm a hash of the data is generated using the secret key. This hash is variously called a message authentication code (MAC), cryptographic check value (CCV) or signature. Strictly speaking the later term should be reserved for an asymmetric cryptographic process. The receiver repeats the same operation using the same key and compares his hash with that provided by the transmitter. Whilst data integrity is assured in that any modification of the data will be detected the authentication process lacks the property of non-repudiation. This is because either of the source or destination nodes could have produced the CCV since they are both using the same secret key.

For an asymmetric algorithm the source node computes a digest of the data often using a publicly known hash function. This digest is then enciphered using the secret part of the key pair to provide a digital signature.

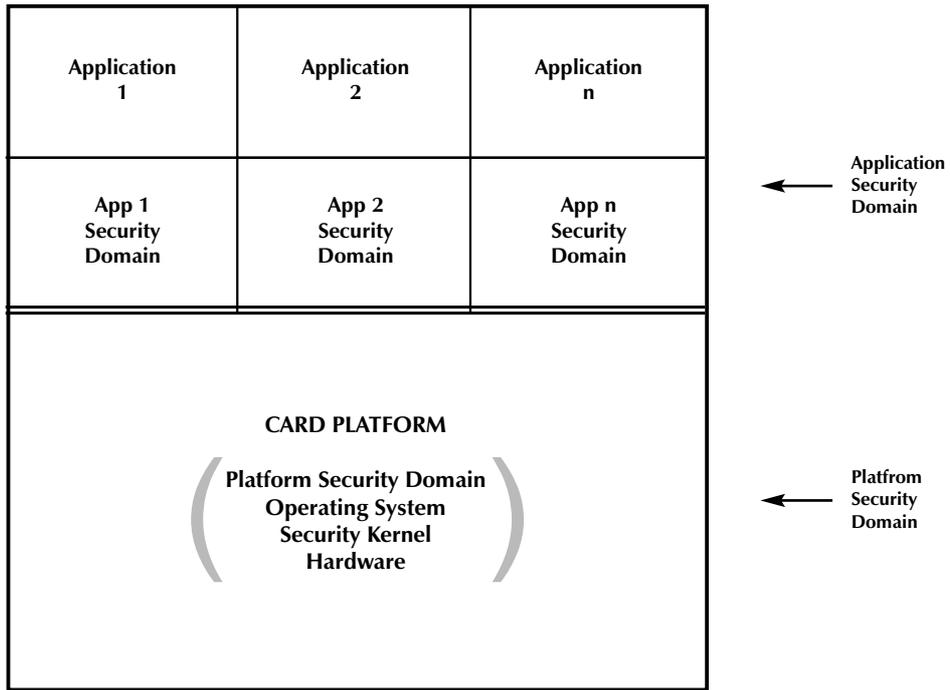| Application 1	Application 2	Application n
App 1 Security Domain	App 2 Security Domain	App n Security Domain

← Application Security Domain

CARD PLATFORM

(Platform Security Domain
Operating System
Security Kernel
Hardware)

← Platfrom Security Domain

Figure 5
Multi-Application Security Domain

Data

↓

Key 1 → Encipher

Cypher

Key 2 → Decipher

↓

Data

Symmetric Algorithm Key 1 = Key 2 (eg: DES)

Asymmetric Algorithm Key 1 ≠ Key 2 (eg: RSA)
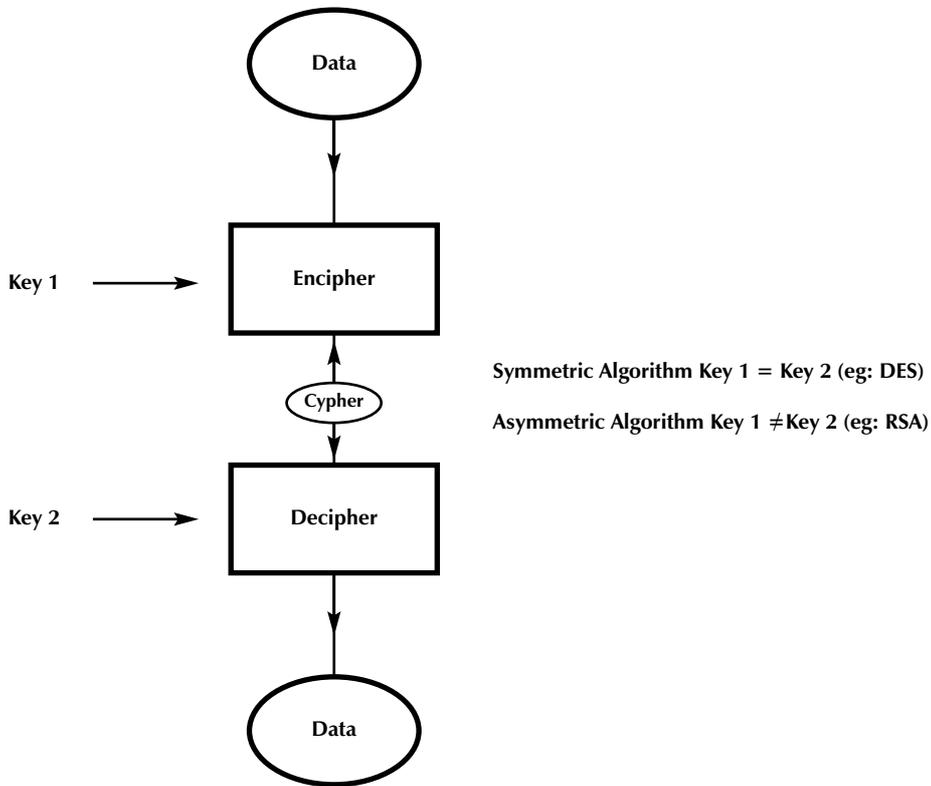
Figure 6
Classes of Cryptographic Algorithm

017

017

017

017

Application Code	Application Data	Secret data (eg: Cryptographic key)

Encipher

Application Code	Application Data	Enciphered secret data

Authentication / Integrity operation

Application Code	Application Data	Enciphered secret data	Signature or CCV
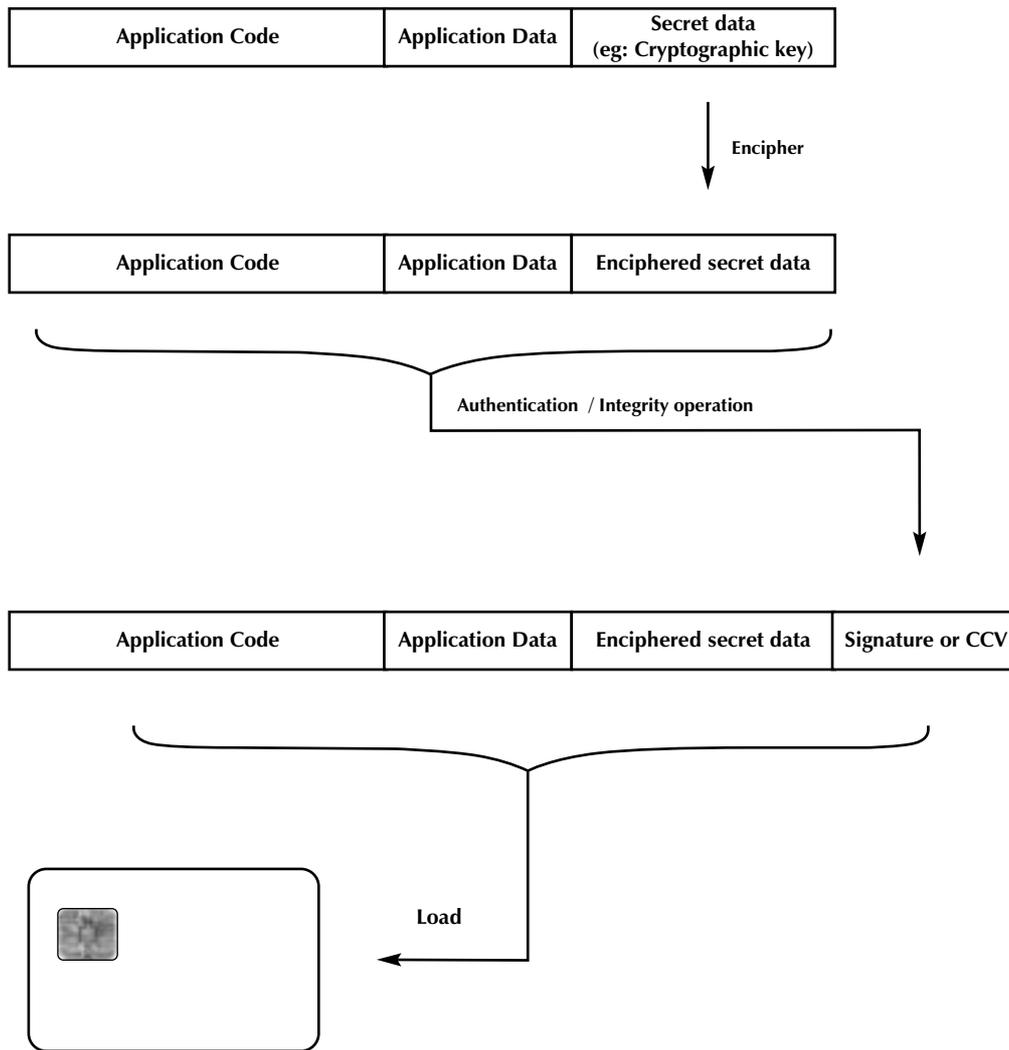
Load

■ **Check Digital Signature or Cryptographic Check Value (CCV)**

■ **Decipher Secret Data**

■ **Load application and data into memory**

Figure 7
Preparing or loading an application

The receiving node recomputes the message digest and recovers the digest from the provided signature using the public part of the key pair. The two digests are then compared to confirm the integrity of the data and to provide the necessary source authentication property.

Let us now look at the steps involved in loading an application onto the multi-application card. The core operations are shown in *figure 7*. The application provider produces his application and data. Some of this data will generally involve secret cryptographic keys. At least these keys but perhaps all the data and code will be enciphered. The application provider will need to generate (or obtain) a digital signature or CCV of the application and its data as produced by the previous operation. This application load module is then presented to the card.

During the load process the platform software will need to check the signature or CCV and decipher that part of the load module that was previously enciphered.

Let us now look at these operations one at a time. Checking the signature or CCV is the responsibility of the platform owner because it is his choice whether or not an application is loaded onto his platform. Therefore from a business point of view the platform owner should generate the signature or CCV in such a way that the target card is capable of checking the signature or CCV. He could choose to use either a symmetric or asymmetric algorithm since he effectively owns both ends of the operation. The property of non-repudiation is not required since he is managing the key(s) used to create and check the signature or CCV. The advantage of a public key system is that the card only needs to contain the public key necessary to check the load signature. This key could safely be put into the ROM mask of the chip when it is manufactured. If he uses a symmetric algorithm then the platform owner has to find some way of securely getting the secret key into the chip before any application can be loaded.

The data encipherment involved in preparing the load module is an entirely different matter. In this case the application provider should be responsible for the keys and their use. It matters little whether the process uses an asymmetric or symmetric cryptographic algorithm because in both cases the card will need to contain a secret key to undertake the decipherment operation. On the grounds of efficiency the application provider would generally use a symmetric algorithm for the encipherment operation. The tricky part of the process is how does the application provider get his secret key into the card?

To be continued next month
David B Everett

Postscript

In order to help our readers understand the operation of Multi-Application Smart Cards SCN is going to make available some Smart Cards and readers to accompany these briefing notes. We are going to assume that our readers have no previous programming experience. We do not intend to teach you Java or any other programming language but by explaining just a few chosen modules we hope you will gain experience in the concepts behind setting up and using a multi-application Smart Card. We will provide more details next month.

019

019

019

019