P&O Passengers Enjoy Cashless Cruising

Passengers on the P&O cruise liner TSS Fairstar, operating out of Sydney, Australia, can use an electronic purse Smart Card to eliminate the inconvenience of carrying cash on board the ship. The system, called Cruise Cash, replaces the coins and banknotes usually required by the 1,000 or so holiday-makers to purchase merchandise, drinks and entertainment during the cruise.

The electronic purse system designed and developed by the Australian company Security Domain, based in Sydney, New South Wales, has the potential to offer other cruise and resort operators improvements in efficiency, service and security.

Continued on page 63

Smart Card News

Editor: Jack Smith

Technical Advisor: Dr David B Everett

Editorial Consultants:

Dr Donald W Davies, CBE FRS
Independent Security Consultant

Peter Hawkes,
Principal Executive
Electronics & Information Technology Division
British Technology Group Ltd

Chris Jarman
Orga Kartensysteme

Published monthly by:

Smart Card News Ltd
PO Box 1383, Rottingdean
Brighton, BN2 8WX, England
Tel: +44-(0)273-302503
Fax: +44-(0)273-300991

ISSN: 0967-196X

Next Month

Smart Card Tutorial Part 21 - Multi-application Smart Cards

CONTENTS

Cashless Cruising

Continued from page 61

The primary reason for introducing Smart Cards onboard the Fairstar was to control cash and prevent theft by employees - a major concern in all cash handling businesses.

Two different Smart Cards are used in the Cruise Cash system. One is the rechargeable electronic purse card (the Gemplus GPM896 card) issued to passengers, and the second is a microprocessor DES card with PIN protection to control access of crew members to the system. There are also two types of card readers - a retail terminal with integrated Smart Card reader for the various sales outlets, and a secure PIN pad used for access control by crew members.

A number of card management functions were identified, specifically, the ability to issue, charge and recharge the card, to reimburse outstanding value at the end of the cruise, and to blacklist and replace lost cards. This was done on standard PCs running Windows Graphical User Interface.

Each retail terminal and PC was connected to a Local Area Network and a small co-ordinating processor (A UNIX machine with a second for back-up) was installed to store the database and to manage the network.

Using the card

When a passenger embarks on the ship, he or she purchases a Smart Card at any of the bars. The card is pre-charged with $50 (of which $5 is a deposit). When the first purchase is made, the card is inserted into a retail terminal and is activated, which means that the cruise number is loaded into the card's memory. To recharge the card, the passenger goes to the purser's office and can load value up to a maximum of $1,000. It is at this point that the card is personalised so that it can be identified as the property of the particular passenger. Personal details are already held on the database prior to embarkation, so certain identifying data is loaded onto the card and the serial number on the card is linked with the record on the database.

While the holiday package covers accommodation and meals, the card can be used to buy drinks, snacks, a holiday photograph, a T-shirt in the duty free shop, or a ticket to play bingo, for example. If lost, the card can be made invalid and a replacement issued. At each purchase, a receipt can be issued indicating the balance remaining.

Until the introduction of Cruise Cash, passengers could not track their holiday expenditure, but now they can request a print out of all purchases.

Multiple cards can be issued against the one ticket number so that children can be provided with "electronic pocket money." If necessary their expenditure can be monitored - a facility welcome to parents if not by the children.

Passengers can still tip waiters and waitresses by requesting that value of the tip be deducted from the card. Credits can also be given to passengers, for example, a gambling win or an accidental overcharge, where a credit note is issued and the credit loaded onto the card at the Purser's Office. At the end of the cruise, passengers present their cards at the Purser's Office and the remaining balance is reimbursed.

Helen Sample, Director, Security Domain, says: "Revenue has increased not only because the problem of 'leakage' has been resolved, but also because passengers appear to be spending more. For example, before Cruise Cash, passengers had to queue up half-an-hour before bingo began to purchase tickets to play. Now, they can purchase tickets at any retail terminals which means that the number of players has increased. The electronic purse system makes it easier to spend money, but at the same time passengers have access to details of what they are buying."

Staff productivity has been improved while the marketing department has precise information on their passengers' purchasing patterns according to age, sex, time and nature of purchase etc. which can assist in planning facilities on board. The Smart Card has provided an important promotional opportunity and can be kept as a souvenir.

Contact: Helen Sample, Director, Security Domain, Australia - Tel: +61 2 954 5747. Fax: +61 2 954 5748.

Spanish Dental Card

Association Dental Espanola (ADESA), the Spanish dental association, an insurance company covering dental treatment in Spain, has proposed that all dentists in the country should integrate with their national network and introduce Smart Card technology.

To date, 80,000 Smart Dental Patient Cards (Gemplus GFM 4K cards) have been issued to ADESA members, and 5,000 Gemplus readers are in use by Spanish dentists.

Software, developed by STACKS, a software house specialising in medical developments, acts as a complete dental office management tool, even in the case of shared care in a dental centre.
Dental treatments are codified (for insurance purposes) and each code has a specific price. The software stores the financial values per code and automatically manages all treatment charges.
The software includes three odontograms (all the teeth drawn) - the first is the initial patient state, the second is the planned treatment, and the third is the treatment progress. Every time a treatment is planned, it automatically issues a program, taking into consideration the type of treatment and the materials.

The Smart Card contains patient identity information and insurance cover data. As well as information about dental treatment prescribed by the dentist and treatment costs, the card contains information about allergies or incompatibilities, and emergency data etc.

Contact: Dr. Bruno Lassus, Gemplus, France - Tel: +33 42 32 51 21.

Contact AFC for Denmark

AES Prodata, a subsidiary of ERG Australia, is to supply and install and Automated Fare Collection (AFC) system based on contact Smart Cards for two public transport groups in Denmark.

Vestjaellands Trafikselskab and Sydbus transport groups each oversee the functioning of a number of bus operators. depots. The system being supplied consists of driver's consoles, ticket printers/card processors, portable readers/ validators/ ticket issuers (Rangers) for use by inspectors, and a depot system which uses PCs and card processors to transfer information between the bus and a central computer system.

Contacts: Alex Danilov, Project Manager, Australia - Tel: +61 9 273 1100. Fax: +61 9 344 3686. Ulf Wassdahl, Stockholm, Sweden - Tel: +468 659 0800. Fax: +468 659 7730.

Changes at McCorquodale

McCorquodale Card Technology has sold its Reigate financial card facility to De La Rue Card Technology.

A Bowater Group company, McCorquodale is now operating out of Lewes, East Sussex, and focusing on developing its specialist card businesses, particularly telephone and Smart Card products.

The new address is: McCorquodale Card Technology Ltd, 27 Cliffe Industrial Estate, Lewes, East Sussex, BN8 6JL, England. Tel: +44 (0)273 475453. Fax: +44 (0)273 480715.

New Offices for Mikron

Mikron GmbH of Graz, Austria, which specialises in contactless read/write identification systems and chip cards, has moved to new offices in Gratkorn, a few miles north-west of Graz. Their new address is: Mikron GmbH, Mikron Weg 1, A-8101 Gratkorn, Austria., Tel: +43 3124 23033-0. Fax: +43 3124 23033-33.

Europay Appointment

Jim Rafferty, Director, Payment Services at The Royal Bank of Scotland since 1991, has been appointed General Manager for Europay International's UK/Ireland region.

He will be based at Europay's UK office at 4 Eastcheap, London, EC3M 1AJ. Tel: +44 (0)71 929 1008. Fax: +44 (0)71 929 1009.

Greek Road Toll Trials

An automatic multi-lane road tolling system has started in Greece with vehicles being successfully charged at speeds in excess of 160km/hour.

The pilot scheme at Malgara, near Thessaloniki, is funded jointly by the Greek Highway Fund and European Commission funded research programme ADEPT (Automatic Debiting and Electronic Payment for Transport).

Thessaloniki is the third of five European city sites to start testing, and the project is being managed by the University of Thessaloniki.

The pilot consists of a free-flow multi-lane debiting system situated on a gantry 500 metres in advance of the existing stop and pay toll plaza.
A two-way microwave communications link between the roadside and transponders on moving vehicles can be used on single-lane roads or multi-lane motorways and automatically debits units from the Smart Card in the vehicle's transponder as it passes the charging point.

Smart Cards have been supplied by McCorquodale Card Technology in the UK. Drivers can purchase credit on their cards up to a value of 99,999 Drachma (£275) and recharge the card with credit units as required. A full audit trail of transactions and purchases is stored on the card and can be accessed by the driver/car owner at card readers in service stations. This information is provided in Greek or English.

In-vehicle equipment consists of a small box attached to the windscreen. This contains the microwave communications transponder and is interfaced to a Smart Card and to a keyboard/display panel attached to the dashboard.

At the roadside, the system consists of communications beacons which may be mounted on a roadside post or on a gantry above the roadway. These beacons are controlled by a local or central computer which also controls the on-line video enforcement system and provides for connections to traffic control centres and an integrated payment network.

The ADEPT system offers flexibility to charge a fixed fee for a toll road or car park, variable road use based on predetermined parameters such as time of day, prevailing traffic conditions, time elapsed, distance travelled etc.

A revised Mk.II specification incorporating some minor changes to the microwave link employed in Goteborg and Cambridge is being used.

Tests have been conducted with two vehicles (each fitted with four transponders) passing under the multi-lane gantry at speed. All eight transponders performed correct transactions.

The system can also be used to monitor traffic on the road network and to provide real-time guidance and traffic information directly to the driver. Additional functions built-into the ADEPT system in Thessaloniki are: TMC (traffic message channel) coded messages transmitted to the vehicles over the microwave link; free text messages transmitted to all equipped vehicles passing under the multi-lane gantry; free text messages transmitted to a group or individual vehicles passing under the multi-lane gantry (for fleet management applications); and provision of parking and vehicle/bus scheduling information.

It is expected that the demonstration in Thessaloniki will run until at least the end of this year. The Greek Highway Fund is looking at the feasibility of extending the system to the tolled road network in Greece.

The situation on the other four field trials in the ADEPT programme is:

Goteborg (Sweden) - multi-lane debiting and enforcement, in-vehicle driver information (started November 1992).

Cambridge (UK) - congestion charging and other forms of road use pricing (started October 1993).

Lisbon (Portugal) - car park booking, guidance and automatic fee collection (May, 1994).

Trondheim (Norway) - integrated payment and the use of multi-service Smart Cards (late 1994).

Contact: Philip Blythe or Professor P J Hills, Transport Operations Research Group, UK - Tel: +44 (0)91 222 6547. Fax: +44 (0)91 222 8352.

Visa "Express Lane" to the EP

Visa International has formed an international consortium of market leaders in the consumer payments industry to develop common specifications for the Smart Card electronic purse. In has also announced the formation of a technology group of international manufacturers to ensure that the specifications developed by the consortium support low cost, efficient production of the necessary systems and equipment.

Wesley Tallman, President, Visa Products and Information Services, said: "Consultation with suppliers responsible for physically implementing the technology is critical to ensuring the viability of the product design. As market leaders in the payment systems field, all of those who have joined us in this initiative are truly partners in paving this express lane of the electronic payment superhighway."

National electronic purse schemes to replace cash for low value purchases in places such as buses, trains, car parking, retail outlets, and pay phones, are being developed in many countries world-wide. Visa says that the most critical step in making the electronic purse concept a global reality is the definition of open standards that can be shared among all participants.

International payments system participants are:

Banksys, based in Brussels, Belgium, and a leading European specialist in electronic funds transfer (EFT) and payment security, operates the ATM and point-of-sale network on behalf of all card issuing banks in Belgium and is developing a national electronic purse project with pilot testing expected to start in December 1994.

Electronic Payment Services Inc, based in Wilmington, Delaware, is the leading electronic funds transfer company in the United States and holding company for BUYPASS Corporation and Money Access Service Inc., operator of the MAC network, shortly to introduce an electronic purse.

Financial Information Systems Centre, based in Taipei, Taiwan, is a government organisation and through its members has issued 80,000 Smart Cards and installed more than 1,000 point of sale systems in its electronic purse project.

Groupement des Cartes Bancaires, based in Paris, is France's payment cards organisation and has more than 22 million Smart Cards in circulation.

NationsBank Corporation, based in Charlotte, North Carolina, is the third largest banking company in the United States with over 1,900 retail banking centres.

Soiciedade Espanola de Medios de Pago (SEMP) based in Madrid, is a sister company of Visa Espana, and is launching a Spanish national electronic purse scheme starting this year.

Sociedad Interbancaria de Servicos, SA (SIBS) is Portugal's leading bank payments company providing electronic clearing services and operating the national Multibanco ATM and EFTPOS networks. It is introducing the Mulibanco Electronic Purse (MEP).

Visa International is the world's leading consumer payments system with more than 333 million cards issued, more than 11 million acceptance locations, and the largest global ATM network.

Wachovia Corporation is one of the United States' leading debit card issuers and provides credit card services to three million cardholders nationwide.

Technology group

The first suppliers to join the technology group are VeriFone Inc., US provider of point-of-sale transaction systems, and Gemplus, the French manufacturer of Smart Cards. The two companies have formed a joint venture, called VeriGem, to pursue electronic purse opportunities.

Visa says that additional organisations who have invested energies in electronic purse applications will be invited to join the group. It is expected that these will include some of the members of the manufacturer's group formed in December 1992 to support development efforts for security specifications of integrated circuits on payment cards. They include Bull CP8 (France), Giesecke & Devrient (Germany), Schlumberger Industries (France), and Toshiba Corporation (Japan).

Contact: Albert Coscia, Visa International, USA -

Tel: +1 415 432 2039.

York Park and Ride Scheme

York City Council, which operates the only Park and Ride system in the UK using Smart Cards, has sourced supplies from US^3 in America.

Last year the service, which started in July 1992 and operates from the Askham Bar car park, near York Technical College, to the city centre (a distance of 3.5 miles), carried nearly 500,000 paying passengers and is estimated to have kept over 250,000 cars out of the city centre.

Currently about 850 cards are used on five buses operating on the first Park and Ride link, and Smart Cards account for around 9% of payments.

The contract is operated by Stephensons Nationwide Travel on a fixed price contract which minimises the risk for the operator and maximises income to the City Council.

The AES Datafare 2000 system is used which comprises Datafare electronic ticket machines and Smart Card readers, a depot system and hand held portable card readers.

Regular travellers can purchase the card at an office at the car park where the card can also be recharged with value. Passengers pay a deposit of £2 for the card.

There are two types of passenger cards used in the York system. These are period cards which give unlimited travel during a set time period, currently either a week or month, and are popular for daily travellers; and stored value cards where a minimum of £5 is loaded onto the card which is then used to purchase travel.

Passenger cards are given a unique number so that cards can be tracked within the system should they be lost or stolen.

An interesting feature is that the system has a "passback" option which prevents a period card being used twice within 10 minutes thus stopping two passengers using one card by passing it back to another passenger.

Each driver has his own Smart Card. This is an 8K byte card with PIN protection against fraudulent use of ticket machines. At the end of his shift, the driver downloads the data from the machine to the card which is then taken to the depot reader where the information is transferred to a PC for printing and storage. At the same time, the PC transfers the current "Hot list" to the driver's card so that ticket machines can stop illegal Smart Cards from being used.

The ticket inspector has his own card which is also PIN protected and gives him access to machines to change date, time and machine number. It also provides him with information on the number of tickets sold on the current trip so that he can carry out a ticket check. The inspector uses a portable Smartscan unit for checking the validity of Smart Cards.

John Bann, Transportation Planning Manager, said the system started with nine ticket machines (for eight buses and one for the office), 750 passenger Smart Cards, 12 driver cards, a driver card depot reader, PC software, three inspector cards and an Inspector's Smartscan reader. The total cost of this package to the Council was £11,000, including set up training.

Due to a higher than expected take up of Smart Cards, supplies ran out and emergency stock was borrowed from Milton Keynes Borough Council which use Smart Cards on city buses. Part of the difficulty, said Mr Bann, was that passenger Smart Card prices sought by AES Scanpoint, were increased to £8 per card (up 400%) and as a result the City Council sought alternative suppliers. One thousand US^3 cards have now been ordered via Cristel UK.

He added: "The cost of the new passenger Smart Card is much less than the revised AES price, but this is still more than double the original price."

Stuart Dalgleish, Transportation Planning, York City Council, said it was planned to open another Park and Ride route in November and others would follow with a target of five facilities by the year 2006. He added that the system might be extended to cover parking charges and possibly other Council services such as leisure services such as entry to swimming pools.

Contact: Stuart Dalgleish, Transportation Planning, York City Council, England - Tel: +44

(0)904 650357.

Four New Projects in Russia

French company Innovatron Ingenierie has announced its involvement in four new Smart Card schemes in Russia.

Residents at the Laes nuclear plant - a town in its own right - near Sosnoy Bar, close to St. Petersburg, can now do their daily shopping with Smart Cards. Ten thousand employees at the plant receive part of their salaries as credits on a Smart Card that can be used as a debit card with some 20 merchants. The project is supported by the Kredo Bank, St. Petersburg.

In Tver, 300 kms from Moscow, some 30,000 Smart Cards have been issued by Moscow's Tveruniversal Bank, and are accepted in more than 200 stores. The card, which is issued when opening an account in one of the bank's branches, is a debit and credit card. The system is designed to run on UNIX and will obtain authorizations for payments above a pre-defined ceiling.

The bank is said to be conducting a vigorous campaign to attract new customers and is developing a clearing system for electronic money with the 300 banks that already belong to its interbank clearing system for bank money.

The Kommon Card processing company financed by Konversbanque is supplying the inhabitants of Doubna, 200 kms north of Moscow, with a Smart Card for buying gasoline at Konversbanque service stations. Kommon Card has issued 1,000 cards to date for use at a dozen service stations.

The Nefteproduct Bank, whose main customers are major oil companies, has also set up a Smart Card service for buying gasoline in its own service stations.

Cardholders in Zizhnii Novgorod, the former closed city of Gorky, and those of two other towns near Moscow, can purchase gasoline at some 25 service stations. About 16,000 cards have been issued. Like the Tveruniversal Bank system, this system is designed to run on UNIX and allows for both debit and credit payments.

Contact: Genevieve Boeuf, Communication Manager, Group Innovatron, France - Tel: +33 1 40 13 39 42. Fax: +33 1 40 13 39 59.

Research will Help the Blind

Research into how Smart Cards, used as alternatives to cash or as electronic keys, can be adapted for the needs of the disabled and elderly, is one of the projects being carried out in England at the new sensory disabilities research unit at the University of Hertfordshire.

Called the Saturn Project, it is being assisted by AT&T, who will be supplying ATM terminals; ICL, Sweden, who will be supplying Smart Card terminals; and Gemplus, France, who will be providing Smart Cards and equipment.

The projects from the European Union's TIDE (Technology Initiative for Disabled and Elderly persons) programme, involve a number of partners across Europe including the Royal National Institute for the Blind, and have a total funding of £4.5 million.

Contact: Dr Helen Petrie, Head of Research Team, University of Hertfordshire - Tel: +44 (0)707 284629.

VeriFone Vice President

VeriFone has appointed Jan-Erik Rottinghuis as Vice President for Europe, the Middle East and Africa.

Based at VeriFone's European headquarters in Paris, he will be responsible for planning and directing the marketing, sales and support of the company's Transaction Automation systems throughout these regions.

Mr Rottinghuis was previously European Marketing and Sales Director for the Polaroid Corporation. Earlier he was Business Development Manager, Southern Europe, for Wang Laboratories.

A Danmont First

The Danmont pre-payment Smart Card system in

Denmark has been assigned the application number A000000001 as the first to be numbered by ISO the International Standards Organisation.

Pay-One Parking System

Pay-One, a parking management system for local authorities based on Smart Card technology, has been launched by Schlumberger. It also offers compatibility with electronic purses.

The system consists of pre-paid Smart Cards (which can be either rechargeable or disposable), pay-and-display terminals, and a computerised management system.

The Smart Card stores parking tokens and, if required, personal information, with PIN access control. It can be custom-designed to carry the colours and logo of the town, or provide an advertising medium for traders.

Pay-One is simple to use. The motorist inserts the Smart Card into the pay-and-display machines, selects the length of stay, and validates the transaction. The machine debits the appropriate amount and issues a ticket as the card is removed.

Special categories of users such as residents or town centre workers, can be allocated special tariffs. Individual user codes can be recorded on the card so that they automatically pay at any special rate to which they are entitled.

The card can be distributed in various ways, for example, sold by shops, sent through the post, or given away as promotional gifts.

Contact: Helene Victor-Pujebet, Schlumberger Technologies, France - Tel: +33 81 54 56 16. Fax: +33 81 52 76 38.

Smart Card '94 Figures

Quality Marketing Services, of Peterborough, say that the International Smart Card '94 Conference and Exhibition in London in February attracted over 300 conference delegates.

There were 53 exhibitors, and a total of 2,700 visitors attended the three-day exhibition.

Contact: Jane West, Event Organiser, QMS, England - Tel: +44 (0)733 394304.

Solaic Targets US and Canada

Solaic, the Smart Card manufacturing subsidiary of Sligos, France, is setting its sights on the United States and Canadian markets with the announcement this month of an agreement providing Direct Data Inc. with marketing rights to Solaic Smart Cards in both countries.

Francis Lavelle, Chairman of Solaic, says: "Our Smart Cards technology has already gained significant acceptance around the world, and we believe the time is ripe to introduce our products in the United States and Canada."

Last year, Solaic supplied 95 million transaction cards, including 53 million Smart Cards, in more than 20 countries in Europe, Africa and South America and has six facilities - two in Spain and four in France.

Direct Data Inc., headquartered in Hartland, Wisconsin, has sales offices in major US cities and recently merged with its sister company Stone-West Inc., which until the beginning of this year was the only American independent sales contractor for VeriFone.

In addition to Direct Data's alliance with Solaic, the company has established a reciprocal marketing relationship with the transaction automation company NBS Inc., based in Montreal, Canada, and is also the exclusive North American distributor of Paris-based Sinfa SA's integrated Smart Card terminal, DesCartes.

Contacts: Dick Draper, Chairman, Direct Data Inc., USA - Tel: +1 414 367 5120. Charles Juster, Communication Manager, Solaic, France - Tel: +33 1 49 00 96 33.

Danmont in 17 Towns

The Danmont pre-payment card can now be used in 17 different towns and cities in Denmark. Laundrettes are the most popular installations closely followed by canteens.

Transaction volumes are increasing with a total of 70,081 transactions in the fourth quarter of 1993

- an increase of 68% from the third quarter. The total number of transaction last year was 183,991.

Amphenol Smart Card Reader

A new Smart Card terminal from Amphenol-Tuchel Electronics GmbH is designed for the easy handling of data storage on a Smart Card.

Smart Cards can be tested and, if possible, repaired. Data can be stored on the card out of a file or via Smart Card/Smart Card data transfer.

The C705-2 Series terminal can be used at the point-of-sale, as a terminal for initialisation of Smart Cards for the mobile phone D1 and C net, and as a reading device for the German health insurance Smart Cards, etc.

Contact: Ralf Stegmann, Communication Manager, Amphenol - Tel: +49 7131 486-303. Fax: +49 7131 486-400.

Slumberger SIM Card Success

Schlumberger has announced that the market for its SIM (Subscriber Identity Module) phone Smart Cards has grown from zero at the beginning of 1992 to 250,000 by the end of 1993. They forecast sales of 600,000-800,000 for this year.

The company's SIM cards, available in 3K or 8K EEPROM, are now in use by 15 GSM operators around the world, including VodaCom in South Africa, SFR in France, and PTTs in Ireland, Scandinavia, Portugal, Singapore and South East Asia.

Contact: Bertrand Dussauge, Communications Manager, Schlumberger Technologies, France - Tel: +33 1 47 46 62 47. Fax: +33 1 47 46 68 66.

New Terminal from DataCard

DataCard's new 50-IC terminal provides a Smart Card interface for PCs and other intelligent hosts via an RS-232 communications port.

As well as functioning as a reader/writer terminal for administrative systems and other Smart Card-based schemes using PCs or other intelligent devices, it is a powerful tool for developing Smart Card systems or designing card formats.

A development kit is available providing explanations of Smart Card technology and the programming tools required to develop successful applications. Sample programs are included.

Two slot terminals

DataCard 485-IC and 680-IC transaction terminals are equipped with two card slots - one for magnetic stripe cards and one for Smart Cards.

The 680-IC includes a modem for on-line or batch off-line authorization, settlement or database access. The 485-IC is designed as a Local Area Network workstation or a data entry device to a PC or electronic cash register.

A built-in security application module with DES encryption is available for both terminals for PIN

pad functionality from the terminal keypad.

Contact: Mark Iverson, Communication, DataCard Corp., USA - Tel: +1 612 931 1763.

Washington Intermodal Card

A fully integrated intermodal rail, subway, bus and parking application using contactless Smart Cards starts this month on the Washington DC transit system.

The present system uses magnetically encoded tickets for rail travel, cash and paper transfers for buses, and cash payment on leaving the rail associated car parks.

It is planned to issue 5,000 Smart Cards in the course of the demonstration of the technology. Those taking part will include Washington Metro employees and selected individuals from the public sector.

Fourteen rail mezzanines, 22 buses and 15 parking lanes will be equipped with Smart Card readers designed by the Cubic Automatic Revenue Collection Group, a subsidiary of Cubic Corportion.

The demonstration starts this month with the card being used for rail travel, and will progress to buses in August, and then rail parking in November. The trial will then continue for a further three months through February 1995.

The GO CARD

Cubic's Smart Card, called the GO CARD, is a credit card-size solid-state electronic device which contains a microprocessor, read/write memory (80 bytes) and a Radio Frequency (RF) inductive circuit that communicates with a target reader. Communication between the card and the reader is within two inches, so the card need not be removed from a wallet or purse to be used.

The Cubic Mark II GO CARD, which contains a battery, will be used in the demonstration, but their most recent Mark III version, which is batteryless and provides greater memory capacity, will also be tested.

Cards will be issued from a Point-of-Issue (POI) computer system which encodes the required information in each card (card type, dollar value, date, time, etc.) and will be networked to the Washington Metropolitan Area Transit Authority (WMATA) central computer where the card transaction data base will be maintained.

Cards can have value added to them at a POI or a standard WMATA ticket vending machine (TVM) equipped with a Smart Card reader. TVMs are located in rail mezzanines. TVMs and gates are connected to a Station Computer System through which they relay card transaction information to the WMATA Central Computer.

Bus equipment interfaces to the central computer via a portable device which extracts bus card data from the bus equipment and transmits this to the Station Computer System for onward transmission to the Central Computer.

Parking fees are deducted from the card on exit from the parking facility.

How it works

The customer obtains a GO CARD at the POI which forwards card issue information to the Central Computer (card serial number and dollar value encoded on the card).

The customer drives into the rail parking facility, then uses the card to enter the rail system via an entry gate. The customer exits the rail system through an exit gate where both the rail and parking fees are deduced from the card as appropriate. Card transaction information is sent to the Central Computer.

The cardholder may board a bus at which time he or she may receive a credit, if any, for the rail journey. The maximum bus fare for the route in question is deducted from the card upon boarding and this transaction is recorded in the bus Automatic Fare Collection (AFC) equipment. (The bus may, in travelling the route, cross either zone or state boundaries which are entered into the AFC equipment by the driver.)

As the passenger leaves the bus, if the maximum route distance has not been travelled, the unused portion of the maximum fare is added to the current value on the card. Information on this transaction is recorded in the AFC equipment.

Contact: Ramon Abramodich, Project Leader, Washington Metropolitan Area Transit Authority -Tel: +1 202 962 5274.

UK Card Fraud Cut by 21%

Bank and building society losses from plastic card fraud in the UK in 1993 totalled £129.8 million, a reduction of £35.2 Million (21%).

This reduction, announced by the Association for Payment Clearing Services (APACS) last month, has been achieved by increased on-line authorizations and secure delivery of cards; bank, police and retailer co-operation; and the Card Watch education and awareness campaign.

Richard Allen, Chief Executive, APACS, said there was a clear and urgent requirement for proving that both the card and the cardholder were genuine.

The task was to identify and develop the technology to secure the card from counterfeiting by first establishing a card authentication method (CAM) to confirm that the card presented at the point of sale was genuine.

No firm decision

"No firm decision has yet been taken in the UK as to the most suitable method, but the industry is giving serious consideration to a chip-based CAM, which is more able to keep pace with the dynamism of the fraudster," he said.

Any decision had to take account of the fact that fraud was a world-wide problem, requiring a world-wide solution, so they were therefore working in conjunction with the international card schemes to ensure that any UK CAM was compatible in the international environment.

A second task was to develop a cardholder verification method (CVM) to prove that the person presenting the card was the authorised cardholder.

Investigations included biometric solutions such as dynamic signature verification and finger-scanning, but these solutions were still some way off meeting the standards they required.

"We have no intention of rolling out new technology that is in any way unreliable or unacceptable to our customers, " said Mr Allen.

Contact: Lorna Harris, Head of Fraud Prevention Unit, APACS, UK - Tel: +44 (0)71 711 6200.

Yorkshire Electricity Pilot

Yorkshire Electricity are to pilot a prepayment system for customers using Smart Cards.

A spokesman said there would be a small-scale

trial during 1994 to enable them to evaluate the technology and assess customer reaction.

Midland Electricity has already embarked on a Smart Card cashless prepayment system, called Smart Power, in a joint development with Landis & Gyr. It plans to install 25,000 Smart Card meters in the first year.

AT&T 8K byte Contactless Card

AT&T has announced an 8K byte EEPROM contactless card which more than doubles its current generation 3K byte card.

The company believes that in the future Smart Cards will typically contain multiple applications, partly because of the economic advantages, and partly for user convenience.

John Bermingham, President of AT&T Smart Cards, says: "This card is particularly useful for situations in which one wants to put several applications on a single card, especially where some or all of the applications involve executable commands, extensive transaction logs or independent security controls for each application."

The new card is compatible with readers and software developed for AT&T's 3K byte card.

New manufacturing process

The company says both cards will benefit from a new manufacturing process coming into production in June that dramatically improves the strength and flexibility of the card's embedded microprocessor chip, and therefore the overall card durability.

Mr Bermingham adds that their proprietary process allows them to produce a chip that is more flexible than the industry standard. Cards made with this process exceed ISO flexibility and torsion standards and they anticipate failure rates less than half of the industry average.

Contact: Michael Jacobs, AT&T, USA - Tel: +1 201 581 3880.

Spanish Multi Purse System

The Spanish Electronic Purse to be launched in the second half of this year by the banking consortium Sociedad Espanola de Medios de Page (SEMP) will be a multi-purse scheme, says Jose-Maria Peres Soria, the project leader.

Speaking at the Prepaid Systems '94 Conference organised by Analyses & Syntheses in Paris last month, he said the system will be based on one open electronic purse, allowing transactions interchange through SEMP for clearing and settlement purposes, and several closed electronic purses that are generated by the card issuer bank based on private agreements with service providers that do not have the capacity to link with the open system.

This concept could offer to the financial institutions, not only the opportunity of financial interchange, but also the ability to do private agreements with service providers.

Different currencies

Although there was no plan yet to interchange international electronic purse transactions, the Smart Card structure could hold several electronic purses each related to different currencies, to allow international use of the electronic purse.

In addition the Smart Card operating system design anticipated new integrated circuit card applications, like Visa, to be fitted in with the SEMP multi-purpose Smart Card.

The trials will be carried out at several Spanish universities this year using SX microprocessor Smart Cards from Solaic, France.

Contact: Jose-Maria Peres Soria, Project Leader, New Technology Department, SEMP, Spain - Tel: +34 1 346 5300.

Europay Strengthens Lead

Europay International has claimed a 57% market share in Europe with total card issuance by Europay Member banks having increased to 94.4 million cards at end 1993.

Francis van den Bosch, Director of Commmercial

Affairs, commented: "In the last five years the market share of new cards issued bearing Europay brands has consistently increased, and for 1993 this market share climbed to 77%, an overall increase of approximately 14 million cards in 1993 for Europay."

Contact: Richard Tischler, Europay International, Belgium - Tel: +32 2 352 5304.

Smart Card Diary

Co-branded, Loyalty & Affinity Cards, The Hyde Park Hotel, London, England, 27/28 April.

Conference includes case studies on the Vauxhall GM Card and the Ford Barclaycard - the two biggest recent developments in the UK card market - plus other case studies. Contact: AIC Conferences, England - Tel: +44 (0)71 329 4445.

The 8th Financial Self-service '94 Conference and Exhibition, Sheraton Grand Hotel, Edinburgh, Scotland, 10/11 May.

Contact: Ms Paula Biagioni, Scottish Electronics Technology Group - Tel: +44 (0)41 553 1930.

Bankcards with Chips, Palais Ferstel, Vienna, Austria, 16/17 May.

Speakers from eight different countries will discuss chip card payment systems, including the electronic purse, and their use in public transport, road pricing and the retail industry etc. Contact: a la Card Conference Services, Germany - Tel: +49 40 66 86 09 17. Fax: +49 40 270 80 66.

Prepayment Cards and Electronic Purse, The Kensington Hilton, London, 26/27 May.

Leaders in prepaid cards will talk about their systems, including the banking partners in the MONDEX project. Contact: Kate Briscoe, AIC Conferences - Tel: +44 (0)71 329 4445.

Cards & Technology '94, Hamburg, Germany, 16/17 June.

An a la Card symposium. Contact: Hans H Huber, a la Card Conference Services, Germany - Tel: +49 66 86 09 16. Fax: +49 40 270 80 66.

Developments, Applications and Implementation Strategies in Smart Card Technology, Sheraton Walker Hill Hotel, Seoul, Korea, 16/17 June.

A chance to hear about the Smart Card market in Korea as well as technology issues and applications. Contact: Elsa Dana, Centre for Management Technology, Singapore - Tel: +65 345 7322. Fax: +65 345 5928.

Plastic Card Fraud & Security, The Cumberland Hotel, London, England, 16/17 June.

International speakers include representatives from Europay International, Banksys, APACS, Visa UK, and New Scotland Yard. Contact: AIC Conferences - Tel: +44 (0)71 329 4445.

ESCAT 1994 (European Smart Card Applications & Technology), Hotel Inter-Continental, Helsinki, Finland, 7-9 September.

Three days of Smart Card applications and user experiences from international speakers from ten countries. Contact: Congrex, Finland - Tel: +358-0-752 3611. Fax: +358-0-752 0899.

Smart ID Cards

AT&T plans to issue its 256,000 employees in the United States with Smart ID badges for use both for identification and for physical access control to buildings.

Currently, many employees carry two cards - an ID badge and a card that opens electronically controlled entrances to buildings. The Smart badges will consolidate both functions.

The company is considering adding debit card applications to the card for use in vending machines and company cafeterias; access control for photocopy machines, computer networks and parking lots; a charge card for inter-departmental services and purchasing transactions, a benefits eligibility card, and a log for attendance reporting.

Re-badging will start with some of the company's buildings in New Jersey during the third quarter of

this year and will be completed by 1997.

AT&T will be using its own contactless Smart Cards. Smart Card readers will be supplied by the Nippondenso Company of Japan, and will interface with security systems supplied by Westinghouse that are already installed in many AT&T locations.

Contact: Michael Jacobs, AT&T, USA - Tel: +1 201 581 3880.

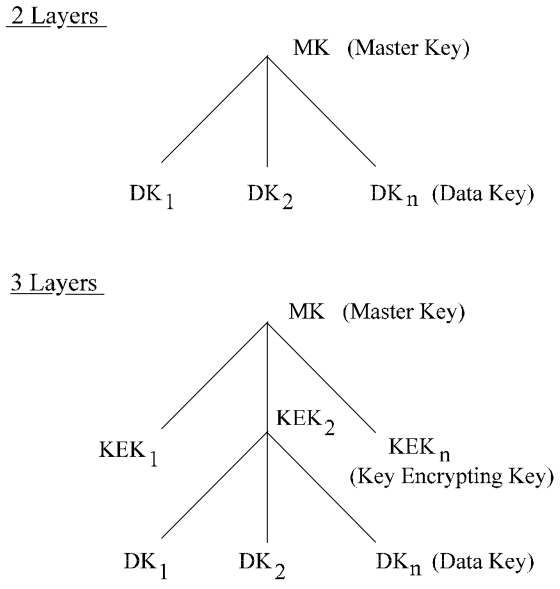

Fig. 1. Key Hierarchies

Smart Card Tutorial - Part 20

Smart Cards and Key Management.

We have discussed the use of Smart cards for implementing various security functions such as data integrity and authentication. There is however an even more fundamental role for the Smart Card in the implementation of key management architecture. All cryptographic schemes require the use of a key transport module by which means the secret security keys can be distributed in the system as required. We should note immediately that any security scheme relies on the use of trusted entities and the necessary procedures for their use. In this part of the tutorial we will examine the establishment of security in a network of Smart Cards. The key management scheme involves the four phases of the security keys, generation, storage, distribution and destruction. Any such scheme involves the use of a trusted key centre and the necessary key hierarchy. The principles are the same for both symmetric and asymmetric cryptography although the mechanism and the practicality of the operation can vary considerably. For the purpose of our discussion we will assume that the Smart Card acts as a tamper resistant module with adequate protection against physical and logical attack. Key schemes are always arranged in some hierarchy for which the root of the key structures is the master key. Such schemes may involve three or more layers but for our discussion we will consider only a two layer scheme as shown in fig. 1. The principle may easily be extended to additional layers.

Key Generation

The root of the key hierarchy is defined as the master key from which all other keys are devised. Clearly this is the critical key in the system and must be non deterministic. It goes without saying that we should not allow any one person to obtain knowledge of the secret key. However human beings are intimately involved in the key management process and we must therefore ensure that we can enforce the necessary procedures to maintain secrecy of the keys.

Where does this master key come from? Well to be non deterministic it clearly needs to be a random number or to be derived from a random

number. This random number must of course remain secret for all time. The subject of random numbers occupies the minds of academics the world over, which the reader may correctly assume confirms the difficulty of the subject. There are two sorts of random number, pseudo and real. A real random number generally uses the properties of physical science (such as shot noise from a semiconductor device) that can produce an endless stream of uncorrelated numbers. The pseudo generator uses some mathematical algorithms to generate a stream of random numbers. John von Neumann first proposed such a method for computers using what was called the middle square method. Let's assume we wish to calculate a string of 5 digit random numbers then starting with 12345, we square to give 15[23990]25 where 23990 is squared to give the next number 57[55201]00. This operation is repeated as necessary. Unfortunately many such simple generators have unacceptable weaknesses. In particular they may lead to short sequences before they repeat. For the middle square method a particular problem arises when the middle digits becomes zero since there will perpetuate a string of zero's. The reader is referred to Knuth (Semi number algorithms vol.2) which is the classical treatise on this and many other mathematical topics relating to security for more information.

Although von Neumann's method is not suitable as a pseudo random generator there are many other choices. In particular we could use the DES cryptographic algorithm which by definition must be non deterministic. If it were otherwise it would be totally unsuitable as a cryptographic algorithm. A way of using DES would be to take our first number as the key and then consecutively encipher the full range of input numbers (each of 64 binary bits). This will generate a non repeating sequence of 2^{64} numbers.

The observant reader will already have noticed the deliberate oversight, where did that first number (in our case 12345) come from? Clearly this should be equally non determanistic or the whole sequence will be exposed. Yes, we also need a random number `Seed' to start the sequence.

The problem is not actually circircuital since we only need in practice to find one good random number and a good pseudo random number generator. For all practical purposes our pseudo random number can do the rest. Several methods are widely used of which the favourite on a computer is to use the time differences generated by the user in entering a sequence of key strokes.

Let us now refer to our problem of starting off the root of the key management hierarchy. First of all we need to produce a tamper resistant module that contains our master key. For the moment we will assume a symmetric scheme such as an DES. In this case our master key (MK) is just the random number. Now either the master key has to be entirely calculated within the security module or we have to calculate it outside the module and inject it. It is clearly preferable to calculate the random number inside the module but in practice it is often inserted. The problem here is that just having one copy of the master key does not allow us to regenerate the key for fall back in the event that our security module fails. We obviously have to devise technigues to handle this problem. The oldest method for handling this problem is to generate the master key in parts. For example we can use three trusted officers each of whom have $^1/_3$ of the key. Each officer enters his part of the key into the module which then calculates the master key as say, the exclusive or of the three parts. Each part is stored secretly by each of the officers. The security here is dependant on the integrity of the three officers, the storage of each of the key parts and the randomness of the key parts.

Let us look at how this situation can be improved by using the RSA public key algorithm. We will consider a situation shown in fig. 2 where we will establish the source master key in three security modules. The security module 1 contains its own means to generate a random number which acts as the master key (MK). The security modules 2 and 3 are capable of generating their own RSA key pairs PK (Public Key) and SK (Secret Key). We should also note that this operation requires both modules to use an independently generated random number seed which is used to compute the keys. From previous discussions in the tutorial we remember the RSA algorithm as follows,

$C = M^e$ Mod N

$M = C^d$ Mod N

$de = 1$ Mod Lcm (p - 1)(q - 1)

$N = P * q$

where C = Cipher block

M = Message block

N = Modulus (entity public PK)

e = encipherment key (Global public)

d = decipherment key (secret key SK)

P,q are prime numbers; Lcm is the lowest common multiple

using our simple number described previously for p,q of 5 and 11 we chose e to be a global constant of 3 from which d can be calculated as 7,

7. 3 = 1 Mod 20
modulus N = p * q = 55

the point to be noticed here is that the security module computes the two primes p and q in a random fashion. The module then computes the secret key d (which never leaves the module) and the public modulus N.

The process of distributing the master key from module 1 to module 2 proceeds as follows,

a) The public key of module 2 (PK_2) is presented to module 1

b) Module 1 enciphers the master key with PK_2

c) The resultant cipher block is presented to module 2

d) Module 2 deciphers the block with SK_2 to recover MK

We can repeat the same operation so that all three modules now contain a copy of the master key generated by module 1. We canl see here that the only vulnerability of this operation is in the presentation of the public key to the master security module. This is not a matter of secrecy but one of authenticity. Only the genuine public keys from modules 2 and 3 may be presented. This is a much simpler practical procedure than managing the secret keys themselves. We may also assume that Smart Cards may be used as the security modules since they can exhibit the necessary properties for a tamper resistant module.

Key Distribution

Having established the master keys in these security modules it now remains to set up the data keys in the total population of Smart Cards for the particular system under consideration. We can see that these data keys are derived from the master

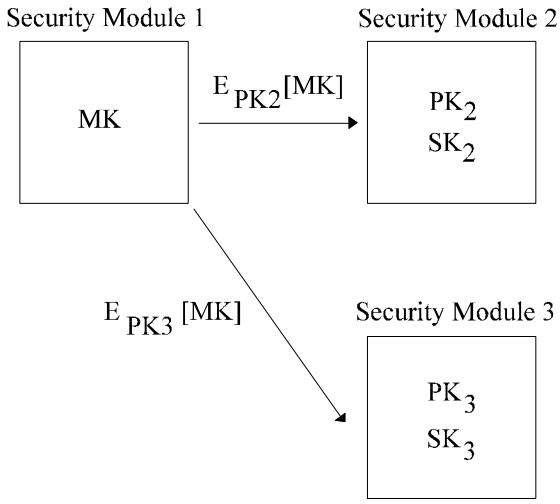

Fig. 2. Master Key Establishment

key (Fig. 1).

The problem now relates to the method of injecting the derived keys into the Smart Cards during the personization process. The master security module can easily calculate the derived key perhaps as a function of the Smart Card's serial number. However if this key is sent to the Smart Card across an unprotected channel then we must arrange comprehensive procedures to ensure this process is not compromised.

We can of course use similar operations to that described previously for establishing the master key, but one needs to be aware of the time overheads for the necessary public key operations. In practice the Smart Cards may not even be capable of implementing the cryptographic operations. A more practical procedure can be achieved by using a key encrypting key that is injected into the Smart Card chip earlier in the manufacturing process. The security module can be made capable of determining this key encrypting key and invoking the necessary operations. This considerably simplifies the procedural management of the personization process.

A total public key system offers significant security advantages albeit at the expense of the complexity of the Smart Card chip. A new problem arises at the key establishment phase. In order for the Smart Cards or integrated circuit cards (ICCs) to interchange it is necessary for them to exchange their public key certificates. (fig. 3; * = certificate) When the cards are personalised these certificates need to be stored in the chip. If the ICCs calculate their own public key pair then the public key must be read from the chip and presented securely to the master key module for certification using its master secret key. This certification process is equivalent to the digital signature process. Again the problem relates to authenticity control not confidentiality. Thus the procedures must ensure that it is not possible to insert a bogus key for certification. A solution to this problem is for the ICC to use an additional key that will provide a necessary authenticity check. This key inserted earlier in the manufacturing process should only be known by the master key module. A similar effect can be achieved by injecting both the public and secret keys as well as the certificate after generation by the master key module.

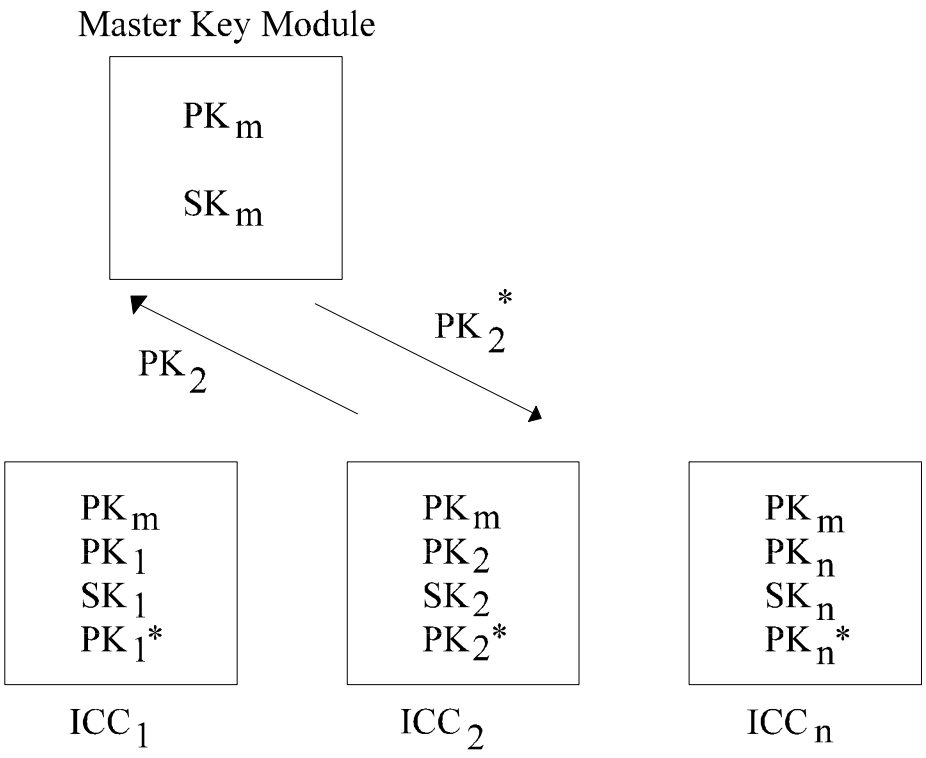

Fig. 3. Public Key Establishment

In this case the confidentiality of the secret key must be preserved by using a pre established key relationship between the master module and the ICC. The public key of the master module can be used to check the key certificate and therefore the authenticity of the keys.

The main lesson to be gained from discussing these two approaches to key management relates to the operational security problem. In the case of secret key schemes such as DES it is necessary to preserve the confidential of the keys. Public key systems such as RSA by comparison require the authenticity of the keys to be ensured. An obvious extension to this principle is the need to be assured of the authenticity of the ICCs before invoking the secret key operations.

David Everett

Next month - multi-application Smart Cards

Golf Club Smart Card

A low cost Smart Card system for cashless payment applications in golf clubs has been developed by Sharp Electronics (UK) and is in use at Gerrards Cross Golf Club, Buckinghamshire, and other clubs in the UK. The system uses Sharp 3110 series electronic cash registers with memory chip cards from McCorquodale Card Technology.

A typical system of five tills and 1,000 cards costs approximately £10,000 and is available through Sharp's national network of 90 value added retailers.

The cards are 416 bit EEPROM IC memory cards with PIN protection. Each card is initialised and serialised with the golfer's membership number

which is uniquely recognised by the cash register. This allows for cancellation and re-issue in the event of the card being lost or damaged, and for black-listing if required. The software also allows full audit of card transactions.

The card (shown on the front page) has a magnetic stripe on the back to operate with the existing physical access control system at the Gerrards Cross golf course. It also has a signature panel for further personal identification and has the golf club name and logo thermally printed onto the card.

Contacts: Jeff Griffiths, Sharp Electronics (UK) - Tel: +44 (0)61 204 2449. Bill Waller, Marketing Director, McCorquodale Card Technology - Tel: +44 (0)273 475453.

Orange PCN Launch

Hutchison Microtel has announced that its UK Personal Communications Network (PCN) is to be launched on 28 April with the brand name Orange - the company's trading name.

At launch, the service will cover 50% of the UK population spanning the major urban centres and connecting motorway routes from the south coast to Glasgow and Edinburgh in Scotland; extending to 70% by the end of 1994 and 90% by mid-1995. On completion the network will comprise over 2,000 base stations in a total investment in excess of £700 million.

A new feature, includes two lines on one phone, for example, one line for business and one for home with different rings and separate bills. Tariff details have yet to be announced, and will be studied closely by Orange competitors Cellnet and Vodafone.

Two phones will be available at the launch - a specially designed compact digital phone from Nokia in a joint development with Orange, and one from Motorola.

The Smart Card SIMs (Subscriber Identification Modules) used to activate and personalise the handset and for billing are available in small plug-in format and standard Smart Card size. The system is being launched using SIMs supplied by Orga.

Hutchison Microtel is part of Hutchison Telecom (UK) which is owned by Hong Kong-based Hutchison Whampoa (65%), British Aerospace (30%) and Barclays Bank (5%).

Contact: Orange Customer Help Line - Tel: +44 (0)800 168168.