Social Security Card Pilot in Spain to Prevent Fraud

A major pilot scheme involving the issue of 500,000 Smart Cards to recipients of social security benefits is taking place in the Cordoue Province of Andalucia in Spain. Objectives are to control services and prevent fraud, reduce current paperwork, provide easier access to personal information and speed up the administration of services.

Responsibility for the project has been entrusted to the Treasury Department of Social Security. The card chosen for the pilot is the Bull CP8 TB100L 3K bytes EEPROM card manufactured and personalised by FNMT (Fabrica Nacional de Moneda y Timbre), the State National Mint which has the sole right to manufacture Bull cards in Spain.

The Forte Crest Hotel at Farnborough in England which will introduce a Smart Card check out system for business travellers

Smart Card News

Managing Director: Patsy Everett

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

Next Month

Smart Card Tutorial - Part 29
Tagging Devices by Peter Hawkes

CONTENTS

Contactless Cards from Bull

Bull CP8 of France and Racom Systems, Inc. of Englewood, Colorado, USA, have made a strategic move into the contactless Smart Card market currently dominated by the transport sector for automatic fare collection (AFC) and road tolling applications.

The companies have agreed to develop, manufacture and market contactless Smart Card transaction systems in a move aimed at increasing

their market share.

Effective immediately, the agreement enables Bull CP8 to market Racom products under its own name through its international sales network to independent OEMs, integrators and end users. In addition, Bull CP8 and its European manufacturing partners will assemble and personalise cards using Racom's contactless technology which is based on the integration of Ferroelectric Random Access Memory (FRAM) technology combined with wireless, batteryless communications technology.

Racom contactless FRAM cards are currently being used in the first phase of the Greater Manchester AFC project in the UK and are being tested in a trial of advanced AFC technology and IVHS (Intelligent Vehicle Highway Systems) for public buses in the California cities of Gardena, Los Angeles and Torrance.

The companies will also integrate Racom's contactless reader technology into Bull CP8 contact card readers.

Bull CP8's expertise in financial transaction card operating systems, high volume card manufacturing and cryptography will be combined with Racom's contactless card microprocessor technology to offer multi-application, multi-function contactless card systems. In addition to AFC and toll collection, emerging contactless system applications are found in customer loyalty, electronic purse, leisure and automated vending markets.

Contacts: Oliver Gatchell, Racom Systems, USA - Tel: +1 303 771 2077. Cedric Sarazin, Bull CP8, France - Tel: +33 1 39 02 43 92.

Part Three of EMV IC Card Specs

Part Three of the IC Card Specifications for Payment Systems jointly produced by Europay, MasterCard and Visa (EMV) has now been published and defines the termina and Integrated Circuit Card procedures necessary for a global

MPCOS Multi-application Card

Gemplus has widened its PCOS (Payment Chip Operating System) range of Smart Cards which have been used in major payment applications such as the Portuguese electronic purse and the NETS CashCard in Singapore, to include the new MPCOS card designed for payment applications and also

interchange of financial transactions. Revised versions of Parts 1 and 2 are also included and have undergone significant modifications following contributions and suggestions from members and manufacturers.

The EMV Joint Working Group is calling for interested parties to submit recommendations for review and expects the specifications will be revised and re-released around the end of the first quarter of 1995. They will include information on the specific public key algorithm and the hash functions which have not yet been specified.

It is felt that the interchange profile identified in Part 3 might not succeed in fully supporting the European business requirements and EMV is working on more flexible alternative solutions.

A separate Chip Card Terminal Specification document is to be developed by the Group for release in the second quarter of 1995.

Contact: Guido Heyns, Europay International - Tel: +32 2 352 5934.

China/Hong Kong Border Card

Bull Hong Kong and local company VICO are launching a Smart Card application to speed up cross border traffic on the frontier between China and Hong Kong.

The operation is targeted at truck traffic passing through the four customs posts in the Senshen Province to assist customs declaration, quarantine control and toll operations.

The current system being used is based on magnetic stripe cards which have shown a high failure rate, particularly in adverse climatic conditions. The new card, shown on the front page, is the Bull CP8 SCOT 10 card which will be used with Bull CP8 TLP 224 card readers.

transportation and healthcare.

The card is available with three memory sizes - 2K, 3K and 8K bytes EEPROM - and a user friendly development environment (MPCOS kit).

The MPCOS card is compatible with the PCOS card and the ISO 7816-4 standard. It contains the

administrative and security commands to handle several applications (payment, transport, etc.).

It includes input/output routines to provide fast transaction processing time for transport applications and can work up to 115,000 bauds.

To provide compatibility with existing terminals, the card can adapt its protocol to the application.

Contact: Isabelle Feneyhrol, Gemplus, France - Tel: +33 42 32 51 33.

Capacity for Six Million Cards

Denmark's largest plastic card manufacturer, dz danmark a-s, which has a market share of 75%, has established a new production line in Copenhagen with a production capacity of some six million Smart Cards a year.

Since the introduction of the DANMØNT electronic purse, dz danmark has taken an active part in the supply of these cards and in the first half of 1994 supplied 90,000 cards to Danish customers.

The company plans to market Smart Cards in its two geographic primary markets, the Nordic countries and South East Asia.

Contact: Flemming Breinholt, Managing Director, dz danmark - Tel:+45 42 84 44 11. Fax: +45 42 84 40 66

New Finnish City Card

Seinäjoki, a city in western Finland with a population of nearly 30,000, is to use the AVANT rechargeable electronic purse as a city card to pay for municipal services such as local public transport, parking and taxi travel as well as public payphone calls.

Esso MasterCard in Singapore

Oil giant Esso which captured the imagination of millions of motorists with its innovative "Put a Tiger in your Tank" slogan and stylish promotional advertising has put its power symbol on a Smart Card in the forecourt war where customer loyalty is a key issue.

It is estimated that the number of city card users will reach 6,000 during the next year and double within two years.

In the field of social services there are a number of services which can be paid for with the city card such as taxis for the disabled and transport connected with daily routines at old people's homes. As there is a user charge for social services, the user can now pay with the AVANT card.

The education service is another major user of taxi services and the possibility of monitoring services will help to develop an efficient division of labour between the different modes of transport. Other applications under discussion are health centre fees and school meals.

The city is introducing card-operated parking lot meters and there are plans for offering companies the option of in-car parking meters.

The city card can also be used to pay swimming pool fees, library fines and other service fees.

Seinäjoki is known for a summer music event dedicated to the tango, so next year residents and visitors wishing to listen to tango music will be able to purchase tickets using city cards.

Contact: Olli Harjama, Managing Director, Toimiraha Ltd., Finland - Tel: +358 0 894 100. Fax: +358 0 8941 4141.

Telekom Orders 15m Cards

Deutsche Telekom has awarded a contract to Solaic to supply 15 million phonecards in 1995. This brings the total of Solaic phonecards ordered by the telecommunications agency to 37 million.

With the DBS Bank, Esso Singapore has launched the Esso MasterCard which operates as a fuel card, credit card and ATM card.

Issued by DBS Card Centre, Singapore's leading card company, the Esso MasterCard is the first of its kind in Singapore to offer the global network of over 12 million MasterCard machines and 380,000 bank branches and ATMs worldwide

An aggressive marketing campaign includes waiving the annual fee for the first five years subscription for those who apply by 31 December. Other benefits are free accident insurance, bonus dollars programmes for Esso products, and the chance to take part in a prize draw with a $50,000 cash prize and ten family holidays for the winners. "It won't cost you a cent, but it could save you a fortune," says Esso.

Cardholder privileges include up to 55 days' credit from transaction date, 24-hour emergency worldwide assistance, 24-hour free car breakdown and towing service to Singapore Automotive Engineering plus discounts at SAE, Orix car rental discounts, free travel insurance cover up to $350,000 for Gold cardholders and up to $150,000 for contemporary cardholders, free insurance protection on purchases, free insurance protection on outstanding expenditure balance, preferential rates for selected DBS Bank loans and DBS Finance car financing loans, maximum liability of $100 only for lost card, discounts and privileges at selected restaurants.

Gemplus Technologies Asia has supplied GPM 896 Smart Cards of which some 100,000 have been issued. VeriFone has provided the hardware and software technology including terminals, printers and card readers.

Contact: Remey de Tonnac, Gemplus Technologies Asia - Tel: +65 776 1989. Fax: +65 773 0648.

GAUDI Project Goes Live

The GAUDI (Generalised Advanced Urban Debiting Innovations) project was scheduled to go live this month in the Marseille, France metropolitan area with an automatic payment system using contactless Smart Cards for payment on buses, metro, train, car parking and tunnel.

About 1,000 users will be supplied with a Smart

Patientline Hospital System

A new Smart Card-operated bedside TV/telephone system is being installed at Northwick Park Hospital in Harrow, Middlesex, England.

Patientline is investing £1.5 million in the project starting in January 1995 at the National Health Service (NHS) Trust hospital where terminals will be installed at around 650 beds.

Card and a PCCR card reader to make quick contactless payments.

The GAUDI programme is sponsored by the European Commission and involves projects in four other major European cities - Barcelona (Spain), Bologna (Italy), Dublin (Ireland) and Trondheim (Norway).

McCorquodale Card Technology has supplied its 3K bytes EEPROM Smart Card with a Motorola SC21 chip for the project.

The PCCR pocket Smart Card reader/writer which enables bi-directional data transmission through an infra-red link between the Smart Card and fixed equipment, is supplied by TOPCARD Monétique, France. It has a 10 character liquid crystal display and three push buttons. The Smart Card is inserted in the PCCR for quick contactless transactions (from 300 to 500 ms).

Contacts: Gérard Coquet, Project Leader, Régie des Transports de Marseille, France - Tel: +33 91 10 56 85. J M Mathieu, TOPCARD Monétique, France - Tel:+33 42 58 61 62. Fax:+42 58 69 96. Bill Waller, Marketing Manager, McCorquodale Card Technology, UK _ Tel: +44 (0)1273 475453. Fax: +44 (0)1273 480715.

ETAM Orders Bull Card Readers

The ETAM Group in France has equipped its 400 ETAM, KIOSK and 1,2,3 women's ready-to-wear stores with Bull CP8 PinPadLINK card readers. These are connected to IBM 4684 and 4694 point-of-sale terminals.

Contact: Yves Girardot, Communication, Bull CP8, France - Tel: +33 1 39 02 44 00. Fax: +33 1 39 02 44 02.

The system includes a sophisticated computer controlled switchboard, voice mail system and satellite and video distribution centre.

It will be installed at no cost to the hospital or the NHS and will be controlled and maintained by 20 on - site Patientline staff.

Each terminal measures 9" x 9" x 2" and incorporates a 6" LCD colour television similar to sets now available in business and first class

sections of aircraft, and a push button telephone.

Twenty channels

Patients will be able to watch up to 20 channels of satellite and terrestrial television, including films, sport, news etc. for a daily or weekly charge. The hospital will also be able to show information videos about healthcare, patients' ailments, hospital facilities, meal selection etc. on separate hospital channels. Patients will also have access to ten radio stations free of charge.

The use of headphones to minimise disturbance can be enforced at certain times of the day or in certain wards, and automatic diversion of incoming calls to a patient's personal answerphone can also be selectively activated.

The telephone on each terminal will allow patients to make outgoing calls and receive incoming calls at their bedside.

Patients will pay for telephone calls and television viewing by inserting a Smart Card into the side of the terminal. The Smart Cards will be available from vending machines situated in the hospital.

Any patient who does not wish to pay for the chargeable facilities will have access to the hospital TV channels, radio programmes and can receive incoming calls and answerphone messages free of charge. A coin operated payphone and standard television will be available on each ward as an alternative to the Patientline system.

The nuisance of telephones ringing in an open ward has been eliminated by the terminal which flashes a silent "incoming call" message on the television screen. If the patient does not answer the phone within a given time, the call is automatically transferred to his or her personal answerphone.

Visa Prototype Technology

In a major announcement Visa International says it has moved "off the drawing board" with the signing of agreements for the development of prototype chip cards and terminals with 20 of the world's leading technology suppliers to the payments industry.

It says that the availability of prototype equipment based on the worldwide chip specifications recently completed by the Visa, MasterCard and Europay

Messages can then be replayed by pressing the "message" button on the terminal.

It is anticipated that visitors will buy Smart Cards as presents for patients as an alternative to flowers or chocolates. Patientline says that its research shows that patients welcome access to this wide range of entertainment facilities as well as the ability to speak directly to friends or relatives from their hospital beds.

Friends and relative have been "very enthusiastic" about the prospect of being able to keep in touch directly with loved ones, and they welcome the opportunity to give a gift which provides entertainment and communications links to a patient during a stay in hospital.

Nursing staff perceive that the time saved on answering calls from concerned relatives, who will be able to ring direct to the patient, will give them more time to carry out their medical duties.

Throw-away cards

GPT Card Technology is supplying 50,000 Smart memory chip cards for the launch. These are throw-away cards with values of £5, £7.50, £10 and £20. Patientline expect to use between 150,000 and 200,000 cards a year in this one project. The terminals have been designed by Patientline and are currently being manufactured by an undisclosed supplier.

Patientline is a new British company with 50% of the equity owned by a syndicate of institutions lead by 3i plc (Investors in Industry). It plans to establish the system in 40 hospitals over the next 3-5 years, creating up to 1,000 new jobs.

Contact: Colin Alton, Patientline, UK - Tel: +44 (0)1844 213999. Fax: +44 (0)1844 216111.
(VME) consortium will accelerate the development and implementation of chip card technology.

William L Chenevich, Group Executive Vice President, says: "This allows us to validate the specifications and perform internal testing that is critical to the implementation of chip technology. Our goals are to provide unparalleled support to members around the world and to ensure a seamless introduction of this new technology when members decide that their markets need it."

Companies involved

The development will take place in two stages. Companies involved in the first stage are Gemplus, Schlumberger and VeriFone who will carry out alpha development.

The second stage will expand development to 17 elected vendor partners for manufacturing and beta testing of cards, terminals, automated teller machines and personalisation devices.

These vendors are AT&T Global Information Solutions, Bull CP8, DataCard, Dassault AT, De La Rue Card Technology, De La Rue Fortronic, Hypercom Inc., IBM, ICL Payment Security AB, Diebold, International Verifact Inc., NBS Technologies Inc., Omron Corporation, Philips TRT, Racal-Transcom Ltd., Security Card Systems Inc. and Toshiba Corporation.

Vendor partnership

Visa is stressing the importance of its "Vendor Partnership Programme" in ensuring the active participation of key vendors in the development of equipment critical to the global introduction of chip cards.
Schlumberger says that the contract covers the development of the software architecture for a powerful microprocessor-based Smart Card chip possessing a high degree of flexibility for the creation of future financial service applications.

It will deliver its card during the second half of 1995 allowing Visa to begin validation. Its work will meet ISO 7816-1/2/3/4 hardware and software standards, and the VME banking card specification. It will also be validated by testing in existing Smart Card EFTPOS terminals from Schlumberger's

ESCAT Honour for Dethloff

Delta range, and via cross-compatibility checks with other suppliers.

Visa expects to complete necessary chip processing modifications to its VisaNet systems by the fourth quarter of 1996 at which time the association will be in position to support member implementations.

Contact: Albert Coscia, Visa International, USA - Tel: +1 415 432 2039.

New Operating System from ODS

ODS Oldenbourg Datensysteme, a leading supplier of chip card systems and securities in Munich, Germany announces the development of a powerful operating system for multi-functional chip cards which optimises the management of limited resources on the chip and provides security, flexibility and an open architecture.

ODS-SCOS (Smart Card Operating System) is ROM-resident and handles generic functions and features which are being used by all applications in more or less the same way. Application-specific features are loaded into the EEPROM.

It is an open system according to ISO 7816-4 standards. Depending on the use of the Smart Card, new applications can be loaded onto the chip. There are several security related functions which have to be executed with positive results: PIN verification of the user, external authentication of the terminal and the use of security messages.

Contact: August Lammersdorg, Director Marketing & Sales, ODS, Germany - Tel: +49 89 45019-310. Fax: +49 89 45019-315.

Juergen Dethloff has been honoured for his pioneering contributions to Smart Card innovation by becoming the first member of the ESCAT (European Smart Card Applications and Technology) Conference's Hall of Fame. The award was presented by ESCAT Chairman Juhani Saari.

Mr Dethloff of Hamburg, Germany, is an engineer,

inventor and entrepreneur who started his own electronics company in 1949 and spent the 50s and 60s developing marine and factory electronics before it was sold to ITT. In 1956, he founded his R&D company, Intellectron, which he still owns.

His Smart Card patents are issued in three generations. The first ones (Austria 9/13/68; Germany 9/10/69; USA 8/17/70) stated "...each card contains integrated circuits providing safety against falsification, and the identifier has means to detect any tampering with the integrated circuits."

His second generation (Austria 9/6/76; USA 8/8/78) described an identification card with interior circuits for use in credit or identification systems. It describes the many hand-held terminals in use today with Smart Cards.

The third generation (USA 6/6/89) describes the multi-use Smart Card now being standardised by the International Standards Organisation.
Mr Dethloff has sold rights to his patents to leading firms in Europe, the United States and Canada and continues to patent a number of important concepts.

His latest United States invention patents a future generation of electronic devices to implement and control economic systems of the type which will arise from changes in eastern Europe and elsewhere.

Phonecard for Three Countries

Plans to introduce a special phonecard for use throughout Switzerland, Germany and The

Fast Check Out at Crest Hotels

International hotel group Forte Crest is planning to provide Smart Cards for business travellers in a fast check out and electronic payment system throughout their hotels in the UK.

The system will go on a three month trial at the Forte Crest hotel in Farnborough, Hampshire, England, starting in January and this will be followed by national roll-out.

Called "Fast Check", the system is a software package developed exclusively for Forte Crest by the Smart Payment company in association with the IT Department at Forte, and Southampton based systems integrator Euclid and is used with Smart

Netherlands in 1996 have been announced by the Ascom-Unisys consortium.

Following PTT Switzerland's decision to introduce chip cards for payphones in Switzerland, a Sfr. 30 million-plus contract has been awarded to the Ascom-Unisys consortium for a pilot project to be launched in April 1995.

In this first phase, users will be able to use the PTT's own POSTCARD for payphone calls and have the charges directly debited from their PTT accounts. In autumn 1995, a special chip card which does not require a PTT account will be introduced. Both cards will be in use throughout Switzerland by the end of 1995.

The contract involves retrofitting 5,100 existing payphones for chip card operation, supplying 2,400 new payphones, and networking the payphones via server with the PTT's computing centre. As the network is an open, scalable system based on international standards and offering customer-specific solutions, it can be extended to other countries and adapted to accept bank card payment.

The second stage will involve the introduction of a special phonecard for use in Switzerland, Germany and The Netherlands. It is planned to extend the single phonecard to other countries.

Contacts: Peter Wullschleger, Ascom Service Automation, Switzerland - Tel: +41 31 999 6724. Fax: +41 31 999 6208. Erich Helwin, Unisys (Schweiz) AG - Tel: +41 380 3700. Fax: +41 31 372 04 85.

Cards and reader pads.

The Smart Card, from GPT Card Technology, is used to record relevant guest information and credit card details upon check in. Any services used are charged directly on the card via electronic reader pads situated in the hotel.

Guests wishing to check out, simply place the card onto the pad and check that the details of their bill are correct before their credit card is automatically debited and they are free to leave the hotel. The check out point will be located near the hotel exit to allow for an easy and speedy departure.

Customer research

Keith Brown, Director of Sales and Marketing at Forte Crest, says: "Our customer research revealed that speed of check in and check out was one of the most critical factors among our business guests when choosing a hotel. Checking out under the Fast Check system will take less than one minute and enhance the service we offer our guests."

Operating under the business brand of Forte, Crest Hotels are located in city centre airports and key commercial locations and are represented in most major cities in the UK as well as in Amsterdam, The Netherlands; Hannover and Hamburg, Germany; and Milan, Italy.

Contact Sarah Molony, Public Relations Manager, Forte Crest - Tel +44 (01)71 836 7744.

Philips Opens Caen Facility

Philips has opened its new industrial centre for Smart Cards in Caen, Normandy, France which offers a potential production capacity of 80 million cards per year. Of the 5,500 square metre centre, 1,800 square metres are clean rooms.

Production capacity will be progressively made operational to meet the needs of key markets in telecard, GSM SIM cards, banking and electronic purse cards, pay-TV cards and health cards.

The centre has received confirmation of approval of GIE des Cartes Bancaires (CB), Visa and Europay. Philips says "This represents a major asset at the time when major credit card networks like Visa, MasterCard and Europay have agreed on the

New Products at CarteS '94

CarteS '94, the international forum for plastic card technologies held in Paris had another successful show last month and consolidated its position as the leading European event for the card market.

Figures showed that visitors and delegates represented 55 countries, excluding France, as against 41 in 1993. There were 4,876 visitors, an increase of 20%, of whom 84% were from France and 16% from abroad. This increase was due to an increase of 129% in foreign participants.

Conference delegates amounted to 739 compared with 480 last year, with 27% from abroad. Six hundred professionals took part in workshops organised by the exhibitors (205 in 1993).

interoperability specifications of their cards which should lead to the generalisation of the Smart Card in the banking environment."

Philips has already supplied over 25 million Smart Cards to the French banks and with their new production capacity plan to "aggressively address the volume markets like telecard."

TLP Version of PE112 Reader

Philips has announced the availability on its PE112 Smart Card reader of a TLP224 compatible communication protocol.

This general purpose reader is aimed at equipping application machines like Personal Computers with a Smart Card reading/encoding feature. It accepts a large variety of card protocols complying with ISO 7816 be they asynchronous (T=0) or synchronous (S=10, I²C ST1200, 4418).

Two versions of the new PE112 TLP are available - PE112-224, external version, connected to the serial V24 port of a PC; and the PE112-324, PC-integrated version mounted in place of a floppy disk drive. This model has been selected for installation on PCs supplied to CNAM-TS, the French medical insurance body, by Olivetti and CMG, the Hewlett Packard dealer. CNAM-TS will equip the 20,000 PCs it needs to install over the next three years with the reader.

Contact: A J Selezneff, Philips - Tel: +33 1 41 28 55 84. Fax: +33 1 41 28 79 68.

Best Technical Innovation Award

TOPCARD Monétique was awarded the prize for the Best Technical Innovation for its PCCR 100 pocket contactless card reader.

The device enables information transmission and reception between a Smart Card and fixed

equipment for applications such as multi-service payment systems (bus, train, metro, parking, tunnel tolls), electronic wallet, dynamic identification and access control.

Transmission technology is bi-directional infra-red. Unit dimensions: 101 x 62 x 8.5 mm, weight: 35 g (without batteries).

A PCCR 200 model has a 10 character LCD display.

Contact: Jean Marc Mathieu, General Manager, TOPCARD Monétique, France: +33 42 58 61 62. Fax: +33 42 58 69 96.

SecureLINK Card Reader

A new family of card readers for PCs and particularly portables, called SecureLINK, was shown by Bull CP8. The reader is connected to the microcomputer's PCMCIA (PC Memory Card International Association) slot and can be used to

PROTON Card Indoor Phone

A new indoor payphone has been developed jointly by French company Mecelec Electronique and Banksys operator of the Belgian network

authenticate a user and ensure the confidentiality of data stored on disk or exchanged over the network or via a modem.

SecureLINK incorporates a PCMCIA card which is inserted in a Type II PCMCIA slot. The CP8 connector, to which a chip card is connected, is attached to the PCMCIA card via a 15-way lead.

There are four versions of the reader: a PCMCIA card with integrated circuit for using the functions of a SPOM (Self Programmable One-Chip Microcomputer); MicroSIM connector for simple replacement of a SPOM; CP8 connector dedicated to the credit card format for handling cards in accordance with ISO 7816-1/2/3 standards and combining these three variants (SPOM, Micro-SIM and CP8 connector).

Percam System

Bull was also showing Percam, a combination of hardware and software for personalising CP8 cards. This can be electrical (encoding the IC), magnetic (encoding the ISO tracks), physical (stamping and engraving characters) or graphic (colour printing of photographs and text).

Running under Windows, Percam software is installed on a PC 486 DX2/50 Hz (12 Mb of RAM, 340 Mb hard disk) set up to perform all personalisation operations. Access to the PC is protected by a card reader and CP8-Log software. Bancontact/MisterCash and developer of PROTON, the national electronic purse.

On display at CarteS 94, the new phone called PI75 PROTON will initially be commercialised in Belgium in the pilot cities of Leuven and Wavre.

Contact: Andre Kauter, Mecelec, France - Tel: +33 75 07 88 00. Fax: +33 75 07 88 24.

Multi-Function Card

IBM was exhibiting the Multi Function Card (see front page) developed jointly by IBM Deutschland Entwicklung GmbH in Böblingen, Germany; DBP Telekom, and GAD (Gesellschaft für automatische Datenverarbeitung eG). the Society for Automatic Data Processing in Muenster, Germany.

According to IBM it is expected that in the next five years, around 50 million eurocheque and bank cards will be issued in Germany with a multi-function chip. Considerable interest shown in China for chip cards in payment systems and health and personal identification also meant that the market potential was not limited to Germany and Europe.

Contact: Heike Odermatt, Communications, IBM Deutschland - Tel: +49 7031 16-2970. Fax: +49 7031 16-2898.

Electricity Distribution Terminal

A retractable Electricity Distribution Terminal which makes electrical energy available to the itinerant user was shown by Innovatron.

The retractable device with a pivoting cylindrical system can be set in the ground or on the wall. It is activated manually using a standard jack system. The regulating system is separate for safety reasons and ease of maintenance and can be used to manage several terminals and can be connected to a Smart Card payment module. Still at the experimental stage, it is aimed at markets, lay-bys, campsites and harbours.

Portable Parking Meter

Innovatron Systemes Urbains was demonstrating a portable parking meter which uses rechargeable

Hitachi Announces New Chip

Hitachi has announced the H8/3102 chip developed especially for Smart Card applications and which has 8K bytes of on-chip EEPROM, 16K bytes of ROM and 512 bytes of RAM.

The core CPU is based on Hitachi's successful H8/300 architecture which features a 16-bit internal bus structure and a general purpose register array which can be used as 8 x 16-bit registers or 16 x 8 bit registers.

Hitachi says its architecture lends itself to efficient software development using high level language compilers, and this is supported by the H8/300's powerful and flexible address modes.

The instruction set implements register based arithmetic, logic operations and data transfer commands, including 8 x 8 bit multiply and 16 ÷ 8

microprocessor cards designed to be integrated in a multi-service multi-operator system.

The meter was developed by Mikrokit based on specifications by the city of Helsinki, Finland which has ordered 40,000 units. Some 20,000 have already been distributed and the remainder will be delivered by the end of 1994.

Innovatron Systeme Urbains took over the Finnish company Mikrokit and now includes the meter in its catalogue as a complementary system to the Piaf parking meter which is in use in about 80 towns and cities in France and other countries.

Contact: Geneviève Boeuf, Groupe Innovatron, France - Tel: +33 40 13 39 42. Fax: +33

Card Production

FMN Holding Group was showing its new high speed ID card personalisation printer (720 cards/hour) targeted at government services, banks and card manufacturers. Cybernetix demonstrated its MSX 3000 machines for micromodules cutting and sorting as well as their insertion in plastic supports. It is aimed at the Smart Card mass production market. The latest developments from Muhlbauer GmbH were its Card Puncher CP2000 and Card Inspection CI2100 designed for card manufacturers.

bit division, as well as bit level instructions.

The new device will operate in both 3V and 5V reader systems and incorporates a power saving sleep mode.

Die size

Hitachi says its new IC chip fabricated in their 0.8 micro CMO process "features the smallest die size in the industry" at only 3.47 x 5.21 mm (18.08 mm²) pointing out that die size is a critical factor in Smart Card design as a small die size reduces the risk of mechanical stress and contributes to improved reliability.

This claim is difficult to check as for commercial reasons most chip manufacturers do not reveal die size except under strict non-disclosure agreements which prevent *Smart Card News* from publishing this information. An exception is Motorola and at

least three of its chips are smaller than the new Hitachi device but contain less memory.

In the Motorola MC68HC05xxx series the SC21 has a die size of 2.9 x 5.1mm (14.8mm²); the SC24 is 3.4mm x 4.1mm (13.9mm²) and the SC26 is 4.2mm x 2.83mm (11.89mm²).

However, compared with the Hitachi chip which has 8K bytes of on-chip EEPROM, 16K bytes of ROM and 512 bytes of RAM, The Motorola SC21 has 3K bytes EEPROM, 6K bytes ROM and 128 bytes RAM; the SC24 has 1K bytes EEPROM, 3K bytes ROM and 128 bytes RAM; and the SC26 IK bytes EEPROM, 6K bytes ROM and 128 bytes RAM. Motorola's SC28 has 8K bytes EEPROM, 12K bytes ROM and 256 bytes of RAM but the die size is not published.

According to Hitachi, its new device is ideally suited to second generation Smart Card applications, for example, digital cellular telephone systems, financial systems and others where security is a prime consideration, and for multi-application cards.

The H8/3102 is available as a base chip, complete wafer or packaged as a Chip On Board (COB) assembly ready for incorporation into a card.

Devices will be sampling early in 1995. C-compiler and emulation tools are also available.

Contact: Vince Pitt, Hitachi Europe, Electronics Components Group, UK - Tel: +44 (0) 1628 585000. Fax: +44 (0) 1628 778322.

Smart Card Diary

Smart Cards & Plastic Cards Conference, 21/22 November, Sandton Holiday Inn, Johannesburg, South Africa.

Conference includes the latest information on the Interbank Smart Card pilot study, applications in the main sectors, developments in technology, local and international manufacturing, security and the Bloemfontein Taxi Smart Card pilot study. Contact: AIC Conferences, South Africa - Tel: +27 11 463 2802. Fax: +27 11 463 6000.

Global Smart Cards 1994: Exploiting the Commercial Opportunities, The Mount Royal Hotel, London, 23/24 November.

The conference will highlight the major benefits to organisations from around the world which have pursued innovative Smart Card systems. Organised in association with The Smart Card Club. Contact: AIC Conferences - Tel: +44 (0)171 827 5964. Fax: +44 (0)171 329 4442.

CardTech/SecurTech '94 West, Westin Hotel, Santa Clara Convention Center, California, USA, 30 November/1 December.

Conference designed to augment the larger East show held each Spring, will provide a general session on major industry trends followed by a developer track focusing on technical issues associated with integration of advanced card and security technology into hardware and software systems; and an applications track looking at the business justifications and strategies. Associated exhibition with over 40 booths. Contact: CTST - Tel: +1 301 881 3383. Fax: +1 301 881 2430.

Smart Card Europe, Royal Lancaster Hotel, London, 13/14 December.

The 2nd annual European conference focuses on security issues, particularly regarding electronic purse schemes, and examines the major applications in the rapidly developing fields of transport and telecommunications. New to the

The Disposable Telephone Card

conference is a tutorial on 12 December by Dr David Everett for those who want to get up to speed on Smart Card technology. Contact: IBC Technical Services - Tel: +44 (0)171 637 4383. Fax: +44 (0)171 631 3214.

Added Value Opportunities in Cards, Claridges, London, 14/15 December.

Exploring issues vital to the successful planning, implementation and management of the latest payment card products, topics cover strategic partnerships, retaining customer loyalty, new market segments and the impact on traditional card activity of debit and prepayment cards. Contact: Kate Briscoe, Conference manager, AIC Conferences - Tel: +44 (0)171 242 2324. Fax: +44(0)171 242 2320.

MULTICARD '95, Grand Hotel Esplanade, Berlin, Germany, 11-13 January 1995.

International conference focusing on Smart Cards in health systems, as an element in modern transportation systems and their use in cashless transactions. Contact: inTime, Berlin - Tel: +49 30 892 9763. Fax: +49 30 893 2848.

Smart Card '95, Olympia 2, London, England, 14-16 February 1995.

The international advanced card exhibition and conference will target prepayment and finance, technology and marketing, transport, communications and advanced identification. Programme available from November. Contact: Conference Secretariat QMS Ltd, England - Tel: +44 (0)1733 394304. Fax: +44 (0)1733 390042.

Further PROTON Order for Bull

Banksys has increased its Bull CP8 card order from 50,000 to 110,000 CC (Cash Card) 60 cards for shipment between now and the end of 1994 for PROTON, the Belgian Electronic Purse. The card will be used to pay for low value purchases such as parking, ticketing machines, public transport, telephone calls and small retail purchases. Trials will take place in the towns of Leuven and Wavre. *by Michael Meyerstein, BT, Development & Procurement*

Introduction

By far the greatest number of IC cards issued to date has been for telephone use. BT has recently entered this Smart Card arena through two events: the announcement of Mondex - an initiative to introduce electronic cash - and the issuing of an Invitation To Tender (ITT) for disposable IC cards and Card Accepting Devices (CADs) for use in Payphones.

Our investigations have shown us that meeting the requirements of a payphone disposable card technology which will take us into the 21st century requires the adoption of the "Third Generation" concept. In this article we will explore these requirements and examine how this technology can meet our business needs.

The Commercial Requirements for Disposable IC Cards

The commercial requirements can be summarised as follows:

- Multiple, open sourcing of cards and CADs
- Technology suitable for public payphones, small low-cost payphones and domestic telephones
- Cards can be used for more than one prepayment application
- Acceptably low lifecycle costs of cards and payphones
- Future-proofing possibilities (eg. extra memory for the user)
- International acceptance in payphones
- Adequate security for international operation
- High-quality graphics possible on both sides of the card
- The payphone must not swallow the card, i.e. it must update any card if it was previously removed before the decrementing process was completed (this is known as "anti-tearing").

Some of these requirements need to covered in a little more detail:
Our studies showed us that the lifecycle cost of an IC card payphone would be much less than that of other types. Nevertheless, for a disposable IC card to be justifiable on cost grounds, the cost of the card would have to come down below that of today's EEPROM cards, even after taking into

Security

An adequate level of security is required to resist the following potential threats:

- Use of stolen, un-personalised cards or ICs
- Illicit re-loading of used cards
- Emulation of cards by other devices
- Counterfeiting or copying of cards
- Modification of cards, eg. to prevent decrementing or to alter the stored value
- Use of other cards not normally accepted for prepaid calls
- Tampering with a payphone to learn secrets of its operation or to modify its operation.

In a situation where the same cards were accepted by many major Public Telecomm Operators (PTOs) for international use, the potential rewards for attackers would be much greater than if a fraudulent card could be used against only one PTO. One may assume that attackers might have access to significant skills, funds and manufacturing facilities. Therefore the security has to be much more sophisticated, especially against the threats of copying or counterfeiting cards.

We believe that if we were to adopt disposable IC cards then we must have a transport locking feature and an active cryptographic authentication method on the card. (The Transport Locking Code provides a means of disabling the IC or card when in transit between, eg. IC supplier and card supplier. This prevents stolen devices from being programmed for use in a payphone).

Costs

Costs which affect the decision on which technology to adopt include the following:

- Capital cost of the payphone
- Maintenance costs of the payphone
- Expected lifetime of the payphone
- Cost of cards

account the revenue from advertising and promotions.

This implies a variant of the Third Generation solution (described later in this article), where the high production volumes and competitive sourcing

will drive down the cost of the product.

Future-Proofing

This includes a migration path towards the following:

- Multi-application disposable prepayment cards
- Multifunction, inter-network, telecomms cards incorporating secure access, personal utilities and a choice of payment methods.
- Inter-sector joint applications
- General-purpose electronic purse
- Tele-services and tele-payment applications

It is becoming clear that the Smart Card will act as a bridge between telecomms networks and between applications in consumer finance and telecomms.

Today's Technology Choices

The table below shows how today's choices of disposable card technology compare with the specific requirements of BT as explored in the previous section. It is not an exhaustive survey of all technology types, since some are obviously not suitable due eg. to inadequate security.

The magnetic card's chief disavantages are its proprietary nature and its comparitive insecurity. EPROM IC cards do not provide a large unit count or user-definable memory. EEPROM IC cards are currently too expensive. The authentication methods of neither the EPROM nor the EEPROM cards would be strong enough for pan-European use.

The conclusion here is that none of the disposable card technologies in use today would be capable of meeting BT's requirements for a technology to replace the optical cards currently used by BT.

France Telecom and Deutsche Bundespost Telekom (at separate meetings) announced a new type of disposable IC telephone card, called the "Third Generation" concept which is capable of meeting all of BT's requirements. This is described later in this report.

Contact vs Contactless IC Cards

There is a variety of contactless cards on the market now and they appear to be gaining favour with some (not all) transportation applications. This technology was rejected by BT Payphones for the following reasons:

- Contactless technology does not currently provide a low-cost, disposable card
- Interoperability with other European operators would not be possible, since none uses contactless cards

Disposable Telephone Cards: Comparison of Non-Optical Technologies

CHARACTERISTIC	HI-CO MAGNETIC[2]	EPROM (1ST GEN.)	EEPROM (2ND GEN.)	EEPROM (3RD GEN.)
Open sourcing	Partly	Yes	Yes	Yes
Small low-cost phones	?	Yes	Yes	Yes
Multi-payment applications	Infeasible	Infeasible	Infeasible	Yes
Low card costs	Yes	Partly	No	Yes
Low reader costs (lifetime)	No	Yes	Yes	Yes
Future proofing	Partly	Partly	Yes	Yes
Pan-European use	No	No	Partly	Yes
Security[1]	No	No	Partly	Yes
Anti-tearing	not needed	not needed	No	Yes
Good graphics 2 sides	No	Yes	Yes	Yes

[1] Security needs to be sufficient for international use of BT cards

2
The magnetic cards referred to are the proprietary, high-coercivity type as used in many payphones throughout the world.

- A payphone needs to communicate with the card for the duration of a call and so we cannot take advantage of contactless (ie. no slot) operation
- Open sourcing of compatible contactless cards and payphones does not appear to be possible at this time.
- Important telecomms Smart Card standards (eg GSM, TE9, DECT) are based on ISO-standard contact cards.

The Third Generation Solution

The Concept

Third Generation is basically an EEPROM telephone-card IC (ie. it has a counting capacity of many thousands of units) with the addition of active cryptographic authentication and extra, user-definable, memory.

All Third Generation designs have the following features in common:

- Security logic to control read/write memory access, counter operation and addressing of memory
- First 104 memory addresses compatible with today's EEPROM cards (ie. 64 bits IC/card ID, 1 bit personalisation flag, 39 bits secure EEPROM counter)
- Cryptographic process to authenticate the card and to protect the decrementing operations. Process uses hard-wired one way crypto function and stored secret key.
- Extra, protected memory for the storage of user-data for future applications.

The Third Generation concept was developed by European PTOs, card suppliers and IC manufacturers. The idea is to have a card which is sufficiently secure and has enough features for it to be used by all European PTOs. This concept would produce lower card prices and would pave the way to inter-operability.

Recently, the concepts have been realised and designs which have been committed to silicon and pre-production samples are expected at any time now. At least two different designs are currently vying for the title of Third Generation. These have been announced to European PTOs by France

Telecom in Paris and Deutsche Bundespost Telekom in Munich, using ICs produced by SGS-Thomson and Siemens, respectively.

The Authentication Process

All Third Generation designs use the principle of a crypto function which is embedded in the hardware of the IC, coupled with a unique secret key which is put into the card as part of the personalisation process.

The card is authenticated by a security module (which in BT's case will be in the payphone) which presents it with with a random-number "challenge". The card uses its crypto capability to transform the challenge into a "response". The security module checks to see if the response is what it was expecting to get.

Calculating the response requires use of the card's unique secret key, but this can be used only by the card's internal logic and cannot be read by the payphone. Therefore, the security module has to synthesise the card's secret key using the same process as was used during personalisation of the card.

This is easier to understand using the diagrams shown over:

Inter-Operability of Third Generation

Deutsche Bundespost Telekom (DBT) and the Netherlands PTT have recently announced a scheme to use the same card type of card, initially a 104-bit EEPROM device but migrating to the Third Generation solution soon. France Telecom (FT) is trialling an advanced EEPROM card (called the T2G) and is expected to go over to a true Third Generation soon. DBT and FT have announced that they will achieve inter-operability of Third Generation cards by 1996.

The various Third Generation designs are not fully compatible, in that they use different crypto functions and key lengths and different methods of presenting the response. Inter-operability and multi-sourcing might therefore require the BT payphone to be able to recognise these different types and to invoke the appropriate suite of software. The security module might likewise have to be capable

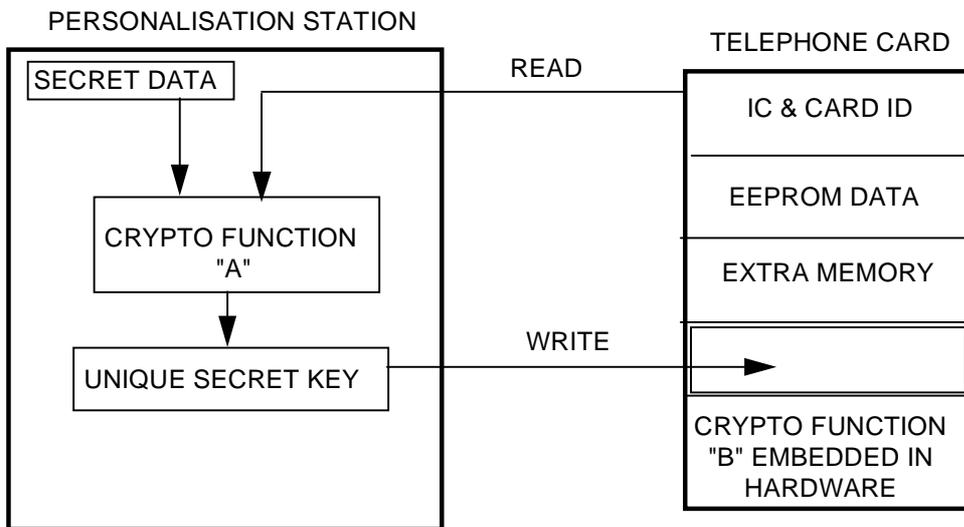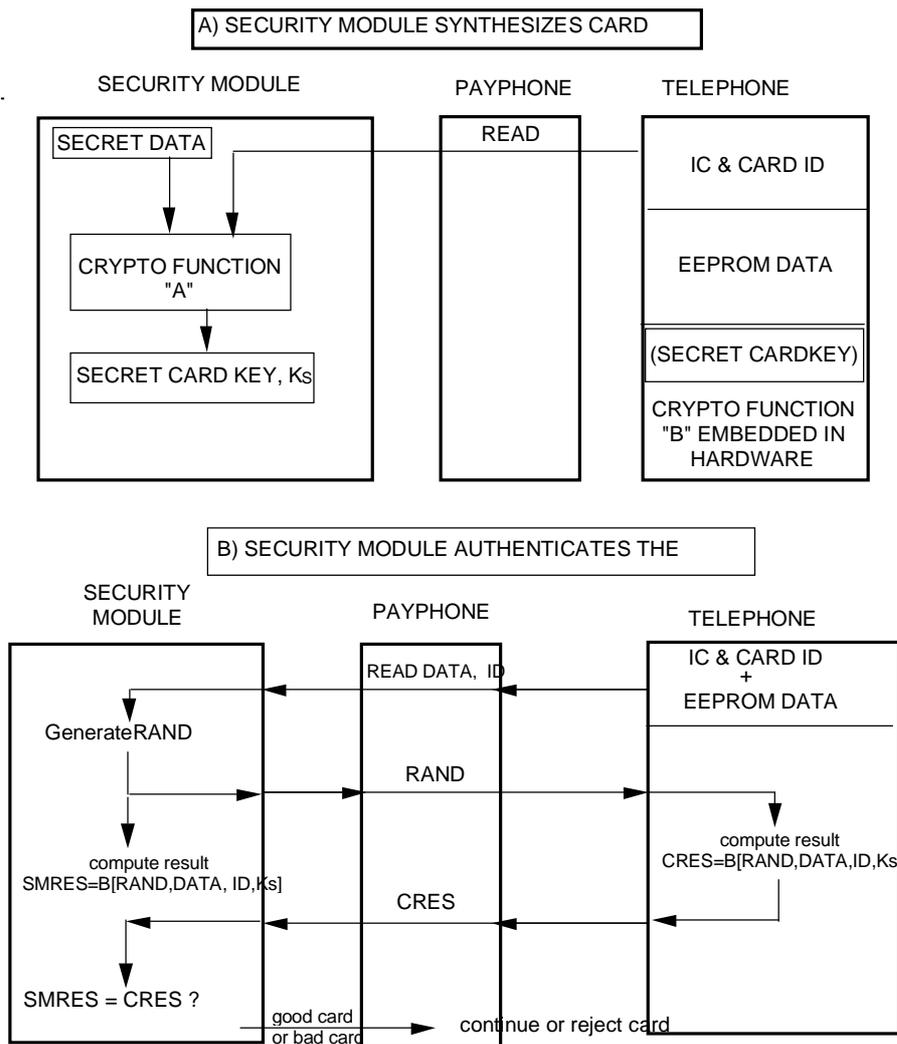## Figure 1: Generation of Secret CardKey at Time of Personalisation

PERSONALISATION STATION

TELEPHONE CARD

SECRET DATA	IC & CARD ID
	EEPROM DATA
CRYPTO FUNCTION "A"	EXTRA MEMORY
UNIQUE SECRET KEY	
	CRYPTO FUNCTION "B" EMBEDDED IN HARDWARE

READ

WRITE

Figure 2: Authentication Method for Third Generation Telephone Card

A) SECURITY MODULE SYNTHESIZES CARD

SECURITY MODULE   PAYPHONE   TELEPHONE

READ

SECRET DATA		IC & CARD ID
		EEPROM DATA
CRYPTO FUNCTION "A"		(SECRET CARDKEY)
SECRET CARD KEY, K_S		CRYPTO FUNCTION "B" EMBEDDED IN HARDWARE

B) SECURITY MODULE AUTHENTICATES THE

SECURITY MODULE   PAYPHONE   TELEPHONE

READ DATA, ID

IC & CARD ID
+
EEPROM DATA

GenerateRAND

RAND

compute result
$SMRES=B[RAND,DATA, ID,K_S]$

compute result
$CRES=B[RAND,DATA,ID,K_S]$

CRES

SMRES = CRES ?

good card
or bad card   continue or reject card

of running different crypto functions for key-   generation and authentication. The sharing of secret

©1994 Smart Card News Ltd

data between different payphone operating companies in a deregulated international market is an issue which needs to be resolved.

Technical Requirements

The card technical requirements are summarised below:

- An EEPROM IC Card (ICC) with internal programming-voltage generation
- Contact layout and command set compatible with ICCs currently in use by Deutsche Bundespost Telekom, i.e. 5 active contacts, to the IS7816-1 & 2 standard
- EEPROM secure "abacus" counter with around 32,000 unit capacity
- First 104 addresses compatible with existing EEPROM ICs
- Cryptographic challenge/response authentication using unique secret key stored on the ICC and authentication algorithm embedded in the ICC hardware
- Computational complexity of the authentication process sufficient to obviate the need for secrecy of the authentication algorithm
- Extra memory for user applications, programmable in Issuer or User configurations. Alternatively this memory can be used for a second secret key, programmable in Issuer configuration only and not readable by the outside world;
- Anti-"tearing" protection
- Extra memory for optional use of activation certificate
- Transport Locking Code protection in Issuer configuration
- High level of physical security embedded in the IC
- Uses non-toxic, environmentally compatible plastics.

Benefits to the User

For any Smart Card scheme to be successful, the user must perceive that he/she is getting something which is useful, good value-for-money and easy to use.
The potential benefits of disposable IC cards to BT's customers are:

- Pan-European use of BT Phonecards
- Applications using the extra memory
- Greater collectability of cards due to better graphics
- Greater availability of payphones due to improved reliability
- Access to a wide range of services from payphones

Michael Meyerstein

ORGA Expands in US

ORGA Kartensysteme GmbH in Paderborn, Germany, plans to expand its activities in the American market as well as Canada, middle and south America by setting up a company in Paoli, Pennsylvania.

It is forming ORGA Card Systems, Inc., and intends to take over Paoli-based ADE Applied Digital Electronics which will add contactless chip card technology to ORGA's range of products and the authorisation to exclusively market the extensive licensing of ADE in the American markets.

The deal is being negotiated by Holger Mackenthun of ADE who will head the new operation in the US.

ORGA Card Systems Inc. is offering consultancy, product development, card production and card equipment.

ORGA's manufacturing capacity is 40 million phone cards a year and five million microprocessor cards which are used mainly in GSM applications. It also manufactures Smart Card modules for phone cards and microprocessor cards for other card companies.

Contacts: Bernd Schaefers-Maiwald, Germany - Tel: +49 5254 991-0. Fax: +49 5254 991 196. Holger Mackenthun, in USA - Tel +1 610 993 9810. Fax: +1` 610 993 8641.

PC Security Card

Personal Computer Card Corporation has announced in the United States the release of PCSS (Personal Computer Security System) Plus, its second generation security system for DOS/Windows based desktop PCs.

User identification takes place during boot-up when a 2K bytes EEPROM Smart Card is inserted into a card reader included with PCSS Plus. The user enters a unique PIN at the keyboard and the PCSS Plus software compares this PIN to the card.

The device can also force users to periodically change their PIN, display messages in the user's native language, ask challenge/response questions, and expire a card on a specific date.

In addition to the security advantages, the access card can store a user's Novell network ID and password, automatically logging on for them when prompted.

By storing the user's network password in the card's protected memory, network administrators no longer need to tell users their password to the company's LAN.

They may also assign complex and random IDs (up to 64 characters in length) and passwords (up to 14 characters in length), thus increasing network security.

Contact: Kip Wheeler, Vice President of Technology, Personal Computer Card Corporation - Tel: +1 813 644 5026. Fax: +1 813 644 1933.

I wish to subscribe to **Smart Card News** for 1 year i.e. 12 monthly issues at:

☐ UK £375

☐ International £395

☐ Please invoice my Company

☐ Cheque enclosed

☐ Please charge my credit card
    Visa/Mastercard/Eurocard/Access/Amex

Name_____

Position_____

Company_____

Address_____

_____

Tel._____

Fax._____

Name_____

Address_____

_____

Card No._____

Expiry date_____

Signature_____

Please return to: Smart Card News Ltd. PO Box 1383 Rottingdean, Brighton BN2 8WX, United Kingdom, or facsimile to + 44(0)273 300991.

Smart Card News carries an unconditional refund guarantee. Should you wish to cancel your subscription at any time then we will refund all unmailed issues.

Contactless on Paris Metro

©1994 Smart Card News Ltd

aim of encouraging the development of industry standards.

* Sizes are current badge dimensions before mass production.

Contact: Claudine Battaglia-Thfoin, Information Services, Innovatron Industries - Tel: +33 1 40 13 39 40. Fax: +33 1 40 13 39 49.

A contactless Smart Card ticketing system is being tested on the Paris Metro and on buses. Currently there are some 4,000 ticket holders and 400 terminals involved in the trial.

The contactless ticketing and access control system using high frequency induction communication has been developed by RATP (Régie autonome des transports) and Innovatron and is intended for use on the Paris Metro, bus and regional railway systems.

Field tests began in 1993 with the intention of progressively increasing the number of machines and cardholders, functions tested and conditions of use. Initially they covered access control for RATP employees when opening and closing Metro stations, control rooms and offices; and subsequently access to and payment for public transport.

A range of access and payment terminals have been developed for different modes of transport and a range of badges for passengers. The Monolithic badge (size* 96 x 55 x 5mm) provides basic access and payment functions on a subscription basis and/or via secure electronic purse payment. A Monolithic Badge with LCD (96 x 58 x 6mm) enables the user to check the details of his or her entitlements, and a Smart Card reader badge (108 x 62 x 7mm) has the potential for multi-service use for purposes other than just public transport (parking, vending machines etc.). The Smart Card can be taken out of the badge and used on standard terminals with contacts.

Next year, Innovatron will be making this system available under licence to public transport organisations and interested manufacturers with the