www.smartcard.co.uk

SMART CARD NEWS

February 1993

Volume 2 Number 2

Rabobank Success in Electronic Banking

Dutch bank Rabobank has pioneered one of the more interesting and successful electronic banking systems for business customers in Europe based on the security of Smart Cards.

Rabo Telebanking has attracted corporate customers since the system was introduced in 1989. Not only has there been a healthy growth in the number of clients adopting the system, there have been substantial increases in the number of electronic transactions and account information inquiries.

Continued on page 23

The ORGA Datentechnik prototype card for the German Insurance card scheme.

Delegates at the Smart Card 93 Conference in London this month.

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
Managing Director
Orga Card Systems (UK) Ltd

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 7 - Inter-industry Commands for Interchange

Smart Cards in The Netherlands

CONTENTS

Rabobank Success

Continued from page 21

The figures speak for themselves.

Growth

Year	No. of Companies
Jun 1989	Start
Dec 1989	100
Dec 1990	1,000
Dec 1991	4,500
Feb 1993	13,000
Plan end 1995	50,000

Usage

Year	No. of Payments	Information
1991	2 million	10 million
1992	7 million	24 million

The system is aimed at the business market, and Telebanking rates are low. There is a one-time entrance fee of dfl 100 and an annual charge of dfl 200. There is an information charge of dfl 0.20 per transaction. The charge for making electronic payments is dfl 0.20 compared with dfl 1.90 for paper-based payments.

Rabobank's tariff structure for payment services stimulates the use of efficient payment systems, because the fees are less for electronic products.

With 7 million payments now going through Telebanking, this represents 10 per cent of manual processed payments.

Companies can have more than one user authorised to send in payments and receive account information, but the Smart Card is required for all transactions. On an average day there are some 10,000 log-ons with the peak period between 8 and 9 in the morning.

Bert Willems, Manager, Electronic Services Business Market, said: "With a weekly increase of 200 companies on Telebanking, all using Smart Cards, we can say that Smart Card technology has gained a solid place in our infrastructure. By doing so, however, we are still the only bank in The Netherlands that applies this technology on this scale in electronic banking."

Rabobank think that about 50,000 companies will be using their Telebanking system by end 1995. Every customer on Rabo Telebanking, and the local bank branches, requires a Smart Card reader and a Smart Card to access the system. Readers used are the Philips PE 111 and 112 modules. The Smart Card used is the DI card produced by Philips Communication Systems TRT in France and supplied in The Netherlands through Digital Equipment Company.

However, the Philips TB100 multi-application card will be used to secure the 20,000 PC workplaces (with a diversity of applications and authorizations) within the local branches. As new applications are developed for the business market the TB100 will be used to secure the specific modules coming from various product groups within Rabobank, and it is planned to change over to the TB100 card in 1994 as the D1 card reaches the end of its life cycle.

The number of Smart Cards in use at the beginning of 1993 totalled 24,000 - 18,500 by companies and 5,500 by local bank branches.

Contact: Bert Willems, Manager, Electronic Services Business Market, Rabobank, The Netherlands - Tel: +31 40 34 65 10. Fax: +31 40 34 67 09.

Newspaper Dispenser

Inhabitants of Naestved, the Danish trial town for the Danmont prepaid cashcard, can now buy their daily newspaper by simply inserting their card in a dispensing machine which deducts the cost from the value stored on the card.

Called the News Box, is has been developed by the Berlingske publishing house who have made the dispenser available on ten sites.

Henning Jensen, Danmont Managing Director, said this was the first proof that new kinds of Danmont vending machines were on their way to the market making use of the advantages the card presented.

Contact: Henning Jensen, Danmont - Tel: Denmark +45 4344 9999.

SmartCrypt for Pay-TV

Schlumberger Technologies has announced SmartCrypt as an innovative alternative to subscription pay television which could open up new markets for broadcasters and provide better value viewing for customers.

The new encryption system involves twin Smart Cards that enable broadcasters to create new pricing, packing and distribution choices while providing high level security against fraud. For example, by using Smart Cards to pay for entitlements, new payment methods can be introduced such as pay-per-time as an alterative to the traditional subscription.

New markets can be opened by packaging programmes by theme or for special interest groups. New distribution channels for a "programme card" can be made available as the Smart Cards can be displayed and sold in retail outlets, used as gifts, or offered in partnership with major brand advertisers.

As the cards are purchased in advance, there is the attraction for broadcasters of "up front money" without the risk of collection problems.

Television encryption systems face the potential risk of losses from fraudulent decoders. In the United States, the National Cable Television Association estimated losses as high as $4.7 billion in 1991.

SmartCrypt meets the problems of fraud with an easily replaceable Smart Card for security and encryption.

The system includes the programme encryption encoder, the set-top decoder, and an administration system which gives the operator control of the system and the ability to authorize subscribers. The decoder has the unique feature of twin Smart Card readers. One card is used as a detachable security processor that is the key to the security. A second card can optionally be used for a wide variety of payment options. The system is addressable on-line, uses on-screen display, and is based on encryption technology.

While suitable for satellite and terrestrial broadcasters, Schlumberger says SmartCrypt is ideal for cable operators or other small community networks because the equipment required at the programme distribution points costs significantly less than other comparable systems.

Contact: Gerard Monnin, Director Television, Schlumberger - Tel: France +33 1 47 46 70 75. Fax: +33 1 47 46 63 67.

Bowater Launches New Company

The Bowater Group is to strengthen its position in the plastic card market with the launch of a new company, McCorquodale Card Technology Ltd.

The new Reigate-based company will combine the operations of McCorquodale Security Cards with those of McCorquodale Smart Card Systems.

Nevil Hewitt, Managing Director of the new company, says the integration of the businesses will enable Bowater to capitalise on the expanding market for Smart Cards by combining the technical, manufacturing and marketing operations of the two companies.

He added that details of a major investment programme to increase production capacity in the company's manufacturing plants at Reigate and Lewes will be unveiled soon.

Contact: Nevil Hewitt, McCorquodale Card Technology Ltd - Reigate, England - Tel: +44 (0)737 223373.

Cashcard Appoints Cardinal

Cashcard Systems have appointed Cardinal (UK) to provide the software management services for Cashcard applications in the leisure industry.

Argentine Order

Schlumberger Technologies, France, are to supply 17 million F256 Smart Cards and 9,000 Smart Card payphones to Argentina in an order worth around 150 million French francs.

Smart Cards: The Growth and The Challenge

This year's Smart Card 93 Conference in London in February attracted a record breaking number of delegates and exhibitors and evidenced the growth in Smart Card developments world-wide.

There was a general consensus that not only has the year seen an increase in the number of Smart Card trials and applications in many countries, but the emergence of new technology and potentially huge markets for cards and associated software and hardware.

In health care applications, for example, Germany and France are to issue health cards to all their citizens. GSM, the Smart Card based Global System for Mobile Communications, is starting to roll out throughout Europe and in other countries. Subscription and pay-TV services is another large and growing market using Smart Cards as the means of unscrambling the picture. In public transport there is likely to be wide-spread use of contactless cards in prepaid ticketing applications and also in automatic road tolling and road pricing schemes. In the financial sector there is more evidence that the banks are looking hard at Smart Cards. The French banks are leading by issuing Smart Cards to all their 20 million plus cardholders, and in Taiwan the banks are expected to launch a nationwide Smart Bank Card this year. And in Denmark trials are underway for what is intended to be the world's first country-wide pre-paid card.

That was the encouraging side of the conference, but there was concern about the painfully slow development of international standards with the recognition that applications, regional and even national schemes need global standards to achieve the maximum benefits of cost-effectiveness and security.

In the next few years, however, it is likely that customers will be faced with a bewildering array of Smart Cards for various purposes when what they would prefer is one multi-purpose card that could be used everywhere.

"Serious" issues were raised about the current processing time of Smart Cards in high speed road tolling and pricing.

Need for global standards

The need for global ICC standards was emphasised by Jean McKenna, of Visa International, the world's largest payment system with 281 million Visa cards in use in 1991. Addressing the Conference, she said that compliance with international standards was essential for the success of any global payment system, and they were keenly interested in the development of ICC standards at the ISO (International Organisation for Standardisation).

"You can well imagine the chaos that could result for cardholders if global payment systems had to implement standards that were developed to address specific needs in multiple national or regional markets," she said.

"Unfortunately, there is a high level of probability that some of this chaos may emerge. The development of international standards of ICCs has been painfully slow. Many of the problems occur when countries or experts try to ensure that existing applications are accommodated in emerging standards.

"Today, those intending to develop specifications to support ICC implementations must choose from these many options and hope that they have made the right choice."

Mobile communications

The two most important new features of GSM (the Global System for Mobile Communications) were security and personal mobility, said Alan Cox, of Vodafone UK.

Authentication was essential to guarantee that the user was genuine and that the card was not a fraudulent copy or had been reported stolen. On GSM, this security was built into the Smart Card. GSM also encrypted all conversations to a high degree of security, and the keys for this were generated by the Smart Card.

Personal mobility was also provided by the Smart Card. When placed inside a GSM phone, the phone authenticated itself with the home network, establishing the location of that subscriber on the

basis of the subscription in the Smart Card, not the particular mobile phone.

Experience of the GSM Smart Card in the market seemed favourable, but one area of concern was the size of the card. Although world standard "credit card" size it was too large to fit inside many of the new hand-held phones. Vodafone had, therefore, developed a small size which they called "plug in" and not much bigger than the contact area round the chip. Although electrically identical to its "big brother" there were now two standards.

Vision for the Future

Antony Watts, SGS-Thomson Microelectronics, said that the Smart Card answered two key needs: to satisfy consumer demand for an intelligent card product, and to prevent fraud associated with existing magnetic stripe cards.

There was no doubt that the Smart Card would take over from the magnetic stripe and would win against any other sort of non-intelligent solution, it was only a question of when, he said. Differentiation between Smart Cards and other card technologies could be expressed in two words "additional services."

Today's Market

Today's market was dominated by phone cards, banking and pay TV, but significant new markets were emerging, notably multi-service, electronic tags, mobile phone and health.

There was a strong customer preference to have one card that could be used everywhere. The temptation by issuers to differentiate their own application at the card level in order to maintain market control had lead to users carrying dozens of different cards around in their wallets. This problem had to be tackled, using intelligent IC based cards the differentiation for issuers could be built into a multipurpose single card.

Progress in contactless cards was restrained by a lack of standards for communication. In fact the situation was rapidly getting out of hand with important public domain projects, like highway tolls, being implemented with different standards. This lack of standards had forced IC manufacturers into a "waiting" phase as they did not know which types of circuits to design for the market or which technologies would be preferable.

Shortcomings

Serious issues had been raised as to the suitability of currently available Smart Card and associated masks to meet the requirements of the various European Commission DRIVE projects, said R Libbrecht, ERTICO

He said here were a number of short-comings and question marks over the suitability of currently available Smart Cards in respect of - the current processing time of Smart Cards (crucial for high speed tolling and road pricing applications); the processing time and capabilities of current Smart Cards to provide adequate data security in an integrated payment scenario; the definition of a "transport purse" to meet the specific need of banking organisations and the operators of public transport, ferry, car parks, tolling and road pricing systems.

He said that a study had been proposed to DRIVE to determine whether the current Smart Card masks could meet all the requirements or whether there was a real need to specify a new mask for a high performance Smart Card for surface transport applications.

Pre-payment for Gifts

French company, Finance et Monetique, are to use the electronic purse application of the JerseyCard Smart Card in the Channel Islands to give conference delegates and other groups of visitors to the Islands the facility to pre-pay for gift purchases.

Christian Lalanne, of Finance et Monetique, says they chose the JerseyCard application because of their practical experience in the field with a live system and a proven infrastructure.

Contact: Chris Parlett, JerseyCard Ltd, St. Helier, Jersey - Tel: +44 (0)534 37713. Fax: +44 (0)534 89665.

London Transport Tender

London Transport has awarded contracts in its contactless Smart Card Stored Value Ticketing scheme to AES Scanpoint (UK) and Westinghouse Cubic. GEC Card Technology will supply the contactless cards and Wayfarer Transit Systems will provide Smart Card readers.

The trial in the Harrow area will involve a network of 19 bus routes operated for London Transport by five companies using around 180 buses. It will start in early summer and run for about 18 months.

Initially groups of regular passengers will be approached and their current tickets supplemented or replaced with a Smart Card. Suitable groups include longer-period Travelcard or Bus Pass holders, school children via their schools, elderly and disabled passengers and London Transport staff.

After a few weeks, a local farecard will be introduced to evaluate alternative stored value fare products and the most suitable pricing structure, test the attractiveness of various charging options to passengers, confirm the reliability of the equipment, and centrally monitor the equipment and use of tickets to assess its operation.

In parallel with this bus work, London Underground is also examining the case for SVT and contactless ticketing. Although a stand-alone bus farecard is feasible, one which is also valid on the Underground and British Rail will be much more attractive to passengers, particularly in inner London.

Contact: Luke Howard, London Transport - Tel: +44 (0)71 222 5600.

Contactless Cards Strategy

Concern about the random development of contactless Smart Cards, which is a new growth area particularly in the field of transportation for fare ticketing and road tolling, resulted in a meeting in Germany this month to obtain agreement on a joint strategy for the European market.

The meeting was at the invitation of ADE (Angewandte Digital Elektronik GmbH) in collaboration with GEC. Other major companies who attended included Amphenol, Autokomp Bull, Detecon, GAO, Gemplus, Hengstler, Kodak, McCorquodale, Mikron, Philips, Schlumberger and Siemens.

ADE and GEC announced plans to produce a common reader ECCR1 (European Chip Card Reader) which is PIN-compatible with ISO 7816 - the standard for contact chips cards. This will enable a customer who does not wish to be tied exclusively to one type of card to use both types of cards.

When the full ISO standard is agreed, the ECCR1 will be modified to incorporate the additional features from the standard. This will allow the customer to use a GEC card or an ADE card, or a new card defined by the ISO standards, all in the same reader.

ADE Manager, H D Kreft, said that the European chip card market was now at the beginning of a new growth phase and producers and suppliers needed to give their major customers clear signals about the future European chip card technology.

Contact: H D Kreft, ADE, Brunstorf, Germany - Tel: +49 41 51 8891 32

Orga to Supply Mercury

ORGA Card Systems (UK) has been awarded a contract to supply Mercury Personal Communications with Smart Cards for its new mobile phone service to be launched in the London area this summer.

In addition to supplying the cards, ORGA has also developed the operating system which resides on the card and the equipment for personalising the card.

The Smart Cards, known as Subscriber Identity Modules, will be manufactured and personalised in the company’s new factory in Paderborn, Northern Germany.

Contact: Paul Hill, Marketing Manager Orga Card Systems (UK) - Tel: +44 (0)491 410997.

Franco Swedish Patient Card

France and Sweden are to co-operate in developing a prescription card which, it is hoped, will lead to a European standard in this field. Sweden has already successfully piloted a prescription card, and France wants to add this application to its Santal Patient Card.

The Santal project

The Santal Patient Card Project is regarded as the most advanced of its kind in France. Centred in the St. Nazaire (population 250,000) area in northern France, it involves 10 hospitals, 12 laboratories, 50 medical practitioners and some 36,000 cards have been issued during the five-year test period 1988-1992.

The Bull 8K byte EEPROM card is offered free of charge to hospital patients when they are admitted and when they consult town practitioners.

It has three "sealed " areas - an administrative area which contains personal information such as the patient's GP, next of kin, and health insurance cover; a blood group information area; and a medical area containing a limited amount of essential information, for example, medical and surgical history, hospital stays, treatments or medical consultations, and medical examinations of particular significance. This is the area read and, if necessary, printed out on arrival in a medical ward. Additional information can also be entered on the card at the end of the medical consultation or hospital stay.

French prescription card project

The Santal prescription card project will start in a part of the Santal local area (17,000 inhabitants) and all the general practitioners and pharmacists in the area will be involved and benefit from the informatic systems communicating with SANTAL applications.

The pharmaceutical follow-up should supply doctors and pharmacists with the tools necessary for using the card as a medical and prescription information support. Doctors will be able to consult and update medical information contained on the cards as well as writing prescriptions on the card.

Swedish Prescription Card

The Swedish Prescription Card project is a joint project between Infocard, The National Pharmacy Corporation of Sweden and the island of Tjirn, Bohuslan, where the project is taking place.

The focus is on providing better information for prescribing doctors by collecting all information on prescriptions on a patient card. The card also carries a total medication history, important diagnoses and hypersensitivity indication.

The first small trial began in 1989 involving only one pharmacy and one health care centre and provided technical experience of handling computerised prescriptions on microprocessor cards and the reactions of patients and physicians.

It used 8K byte EEPROM cards and MSDOS personal computers with three databases providing information on all available drugs with brand names, form, strength, pricing etc; pharmaceutical information on the drugs, for example, appropriate dosage, side effects etc; and information on the possible drug treatments of common diseases.

Sweden/France co-operation

The two national health authorities - Santal on behalf of the French Ministry of Health, and Apoteksbolaget (Pharmacy National Institution) for Sweden, are co-operating to achieve a multinational approach to the use of a medical card allowing a prescription application.

The project specification is expected to be completed soon and trials will run in both countries. It is hoped that this work will lead to a European standard and possibly future European co-operation on Smart Card health applications.

Contacts: Philippe Cirre, Centre Hospitalier St. Nazaire - Tel: France +33 40 90 60 11; and Dr Gunnar Klein, Gunnar Klein AB, Sweden - Tel: +46 8 80 80 00.

German Medical Insurance Card

Germany is starting to place substantial orders for its medical insurance card scheme. The first contract has been awarded to Siemens to supply 50 million chips. The first part of the order will be SLE 4418 M2 1K byte chips to be followed about mid-1993 by SLE 4432 M4 2K byte EEPROM chips.

The Federal Association of General Practitioners and ORGA Datentechnik GmbH in Paderborn, have been working together on the medical insurance card scheme.

The medical insurance card will contain personal details and information about insurance and is intended to make administration easier for doctors, insurance companies and government departments, saving time which will be to the benefit of patients.

The card should not be confused with the patient card which will contain the patient's health information and medical history.

The insurance card will store the holder's name, date of birth and address of the insured party as well as his insurance company and all the required organisational data.

A reading device developed by ORGA Bond-Technik reads the chip card when the patient registers with a practice.

The connected printer produces a registration form, patient record sheet and, if necessary, prepares prescription forms. This minimum configuration of reader and printer costs DM 800.

However, if the doctor already has a computer in his surgery he can make the information on the card available for electronic data processing and form the basis for all further processing, from issuing prescriptions and maintaining a patient file, to private payment and invoicing the responsible insurance company.

Contact: Paul Hill, Marketing Director, Orga Card Systems UK - Tel: +44 (0)491 410997.

Leisure Industry Smart Cards

The leisure industry needed a solution to cash handling, John Kelly, of Cashcard Systems, told the Smart Card 93 Conference in London, and, as an example, he said a large bowling centre could handle 3.5 tons of coins which had to be counted, bagged and transported.

Britain had some 70,000 pubs, 150 bowling centres, 500 premium outlets such as nightclubs, one hundred plus holiday centres, as well as theme parks, restaurant chains, family entertainment centres (with up to 400 amusement machines) etc.

Pre-payment Smart Cards, he said, could assist cashflow with money up front, operating cost benefits, downtime reduction, flexible pricing, unused credit, security and marketing opportunities.

Whitbread Trial

Cashcard are currently running a trial with 11 Whitbread managed public houses involving the use of Schlumberger pre-paid Smart Cards to enable customers to pay for drinks and machine games. (SCN Vol 2. No.1).

Whitbread are expected to decide soon whether or not to extend the scheme.

Cashcard Systems say discussions are currently underway with seven national pub retailers, four bowling operators, two bingo operators, a cinema chain, and a family entertainment centre.

Contact: John Kelly, Chief Executive, Cashcard Systems Ltd, England - Tel: +44 (0)636 610022. Fax: +44 (0) 636 610122.

Social Security Cards

Philips are to supply five million D2000 2K bit EEPROM cards for the German Social Security ID card system.

VideoCrypt "S" for BBC Select

BBC Select is a highly sophisticated UK subscription television service offering specialist programmes which are recorded on our home or office television sets when most of us are asleep. The service, launched last summer, makes use of the period 2am-6am when BBC1 and BBC2 are closed down, and all the subscriber has to do is to remember to insert a Smart Card (the Viewing Card) in the decoder and put a blank tape cassette in the video recorder and leave it in the standby mode.

Viewing of subscription programmes is only possible through a decoder (the BBC Selector), which works in conjunction with a Smart Card to unscramble the programmes. The Selector is designed to enable the recording of programmes automatically for most VCR models by sending an infra-red (IR) message to the VCR telling it which channel to turn to and when to start and stop recordings.

As a large number of people have difficulty in setting their VCR timers, it was a requirement that the process of recording the descrambled programmes overnight should be automated, and that the customers VCR be operated under the control of the BBC Selector.

The system provides a neat solution to making the large number of VCRs with their own IR codes respond to automatic recording. Data representing the various VCR codes are compressed into a file and programmed onto Smart Cards. These cards, known as Installer Cards, are used by engineers for the initial installation to perform the VCR customisation of the Selector. In operation the Selector literally floods the room with IR light causing the VCR to respond to the command sequence as if it had emanated from a normal IR handset.

The subscription services are primarily educational and training biased and offer both news and topic orientated programming.

The scrambling system is based upon VideoCrypt, a joint project by Thomson Consumer Electronics and News Datacom. The two companies worked with the BBC Research Department to produce VideoCrypt "S" to meet the particular requirements of the new broadcast system.

Videocrypt, as used in the British Sky Broadcasting subscription channels (see SCN September, 1992), was changed as the transmission parameters of a terrestrial system were different to those of a satellite system (BSkyB). The VideoCrypt scrambling method known as Line Cut and Rotate (LCR) was replaced by a Line Shuffling (LS) method which improves picture quality in the presence of multi-path echoes more likely to be encountered on terrestrial broadcasts than on cable or satellite, particularly in certain geographical areas.

In the LS method, the lines making up the television picture are "shuffled" rendering it unwatchable to the non-subscription viewer. Flexibility in the system allows intermediate levels of scrambling to be used whereby the picture is unpleasant to watch but considered a "tease" to attract a potential audience. There is also an optional audio scrambling feature.

The line shuffling process is activated by an Encoder, or Scrambler, at the Television Centre, and the re-ordering sequence is driven by a large (multi-byte) Control Word (CW).

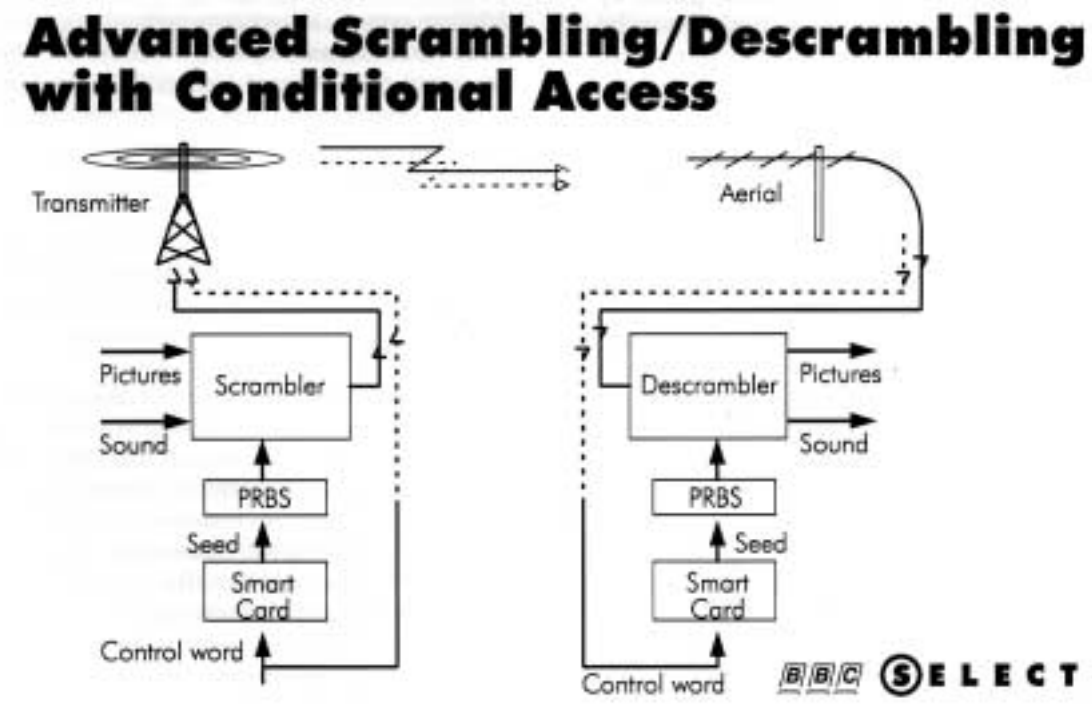
Security Encoder Computers (SECs) work in conjunction with an Encoder Smart Card. The SECs periodically pass a Control Word (CW) to the Encoder Smart Card which contains a cryptographic algorithm and software unique to BBC Select and converts the CW into a scrambling SEED. The SEED is then used to initialise a Pseudo Random Bit Stream (PRBS) generator, which in turn controls exactly how the television lines are shuffled within the encoder. The process of the SEC exchanging the CW with the Smart Card occurs so frequently that a would-be hacker has virtually no time at all before the way in which the lines making up the television images is fundamentally renewed.

Control words are simultaneously transmitted over the air using the data channel within the vision signal, and broadcast to all Selectors in the field.

In the field, the Selector descrambles the images by re-ordering the shuffled lines. To do this it has to seed or initialise its internal PRBS generator to match that at the SEC in Television Centre. Since it does not have the SEED to perform this task, it must derive this from other encrypted information. Integral to the Selector is a Smart Card reader into which the customer inserts the BBC Select Smart Card (the viewing card). The Selector extracts the CW from the over-air data channel, and passes it to the Viewing Card. An algorithm, related to that in the Encoder Smart Cards, recovers the SEED from the CW data. By passing the SEED back to the PRBS generator in the Selector, the scrambling is unlocked and the television lines are unshuffled.

The Smart Cards used by BBC Select are supplied by US3, Inc., of Santa Clara, California, who are also suppliers of Smart Cards to British Sky Broadcasting.

Contact: Mike Walsh, BBC Select, BBC Subscription Television Ltd UK - Tel: +44 (0)81 576 2000. Fax: +44 (0)81 749 1647.



Swedish Road Toll Scheme

Swedish motorists are to be made to pay for new roads by paying tolls. Many of the bigger cities will soon start large building projects to improve roads and public transportation. In Stockholm alone over 30,000 million SKr (,3,000 million)is to be invested in new roads and public transportation with about half of this on road projects.

The city recently decided that money collected by road tolls should finance the new roads. Until now building and maintenance of roads has been financed through taxation.

The Swedish National Road Administration (SNRA) has therefore initiated a Swedish road toll test scheme called ADSW - Automatic Debiting System for Sweden. The test site is one of five test pilots in the European Commission's ADEPT project.

Introducing the project at Smart Card 93 in London, Ulf Baggstrom, of Au-System Communication, pointed out some of the advantages of an automatic system compared to a manual system.

As vehicles were charged "on the fly," studies had shown a saving of up to 10 pence by motorists and up to 50 pence by truck drivers by eliminating the need for the vehicle to stop. Antennas could be placed in the existing traffic environment and the use of land in conjunction with the toll stations was minimised. Staff could be reduced. Security could be improved by reducing cash handling. Automatic toll collection systems caused less or no delay, and maximum capacity was, in theory, only limited by the road's capacity.

The ADSW system

The ADSW system is meant to be a general communication link between a vehicle and a roadside system, but it is not regarded as a final solution, more a platform for future development and experiments.

International, European and industry standards have been used as far as possible, and by using a standardised Smart Card there is also a possibility to interact with other, non RTI (Road Traffic Informatics) applications such as parking, public transportation and telephone.

The system

The system is being developed by two Swedish companies, AU-System and SAAB Combitech, together with the Norwegian company Micro Design A/S, with the Swedish Transport Research Institute providing administrative project management.

The site is an urban arterial road south-west of Gothenburg with a speed limit of 70/90 km/h and two lanes for traffic in each direction. The test site is equipped with two gantries approximately 200 meters apart. Two antennas are mounted above the carriageway on each gantry. The road-side detection covers the entire road width and a video camera is mounted in conjunction with one of the gantries.

The control centre is located at the SNRA regional office in Gothenburg and communication between the roadside system and the control centre is done over ISDN.

SAAB Combitech has developed the microwave link, the transponder, antenna and the link controller. Micro Design has developed the debiting system, the system controller and the video enforcement system. AU-System has developed the On-board Unit (OBU), the Card Service System (CSS), and security mechanism.

Smart Cards

The Smart Cards chosen for the project are Gemplus MCOS 2K byte EEPROM cards with built-in functions for DES encryption. The card complies with ISO 7816-1/2/3 standards.

There are two different types of Smart Cards involved in the system. The OBU card is a "vehicle" card used to initiate the OBU with vehicle data, typically vehicle licence number, vehicle classification, environmental classification etc. Before this card will function, the user must present a PIN code, and the OBU cannot function until it has been initiated with the card.

The other card is the "driver" card which contains

information about the driver and what services he is allowed to use in the system.

Payment methods

Two payment methods are available in the ADSW - pre-payment in which the driver loads the card with electronic cash and uses this to pay the toll, and post-payment in which the identity of the card is transmitted to the debiting system and the card owner's account is charged with the toll fee.

In pre-payment mode the transaction is carried out without revealing the identity of the driver or the card. If the card does not contain enough value to pay the toll, the payment mode is automatically switched over to post-payment.

Security

The OBU - about the size of a car radio - is larger than many other OBUs in use in other road projects, but in this case it also functions as a mobile encryption/decryption unit.

The DES algorithm is used to provide three levels of security - protection against false cards, transaction replay and data manipulation.

The roadside system authenticates the card by means of a challenge and response system on the move. It sends out a random number to the OBU which encrypts the number with a secret key and returns the result to the roadside system which decrypts the result and compares it with the number that was sent out. If they correspond the card is authentic.

To protect against transaction replay, every transaction is marked with a unique certificate which varies for every transaction.

The certificate is calculated from the contents of the transaction and protects the transaction against manipulation. If data is modified during transmission, the certificate will not be correct.

The video enforcement system takes pictures of vehicles not accepted by the system and shows the vehicle licence plate, date and time, location and cause of picture for transmission to the debiting system for post processing via ISDN.

Experience to date

The time required to process a complete toll transaction is approximately 100-200 ms, depending on the speed of the vehicle. The Smart Card is relatively slow in communication and updating, which means that the use of the card during the session has to be minimised.

This problem was solved by letting the card do the main part of its work before and after the session. Only the most vital parts of the data are updated during the session, the rest of the updates being done afterwards.

This means that the OBU has to do the most processing during a session - encryption and decryption, for example are done in the OBU. Consequently, the OBU itself has to be secure.

A better solution is seen to have all the security mechanisms handled in the Smart Card so that the OBU device, built on an open architecture, can be manufactured, distributed and used without considering security problems.

Benefits

The test has shown many benefits in using a Smart Card as a component in an automatic road toll system, such as:

The driver has his own card and uses it in different ways, as an identification card or as an electronic purse. Debiting is always connected to the card owner, not to the vehicle.

It is a secure device with secret keys, electronic cash and user data protected from fraud.

It is portable and the card owner can use his card in several applications, such as parking, public transportation, telephone, etc.

The Smart Card is standardised and the operator is not tied to follow a custom-made technique.

Contact: Ulf Baggstrom, AU-System Communication AB, Sweden - Tel: +46 8 726 7500. Fax: +46 8 19 3322.

Smart Card Diary

Card Technology Asia 93, York Hotel, Singapore, 15/16 April.

The conference will cover some of the latest applications and developments in Smart Cards and prepaid cards. Speakers include representatives from U Card Inc (Japan), BankExim (Indonesia), The Schuler Consultancy (USA), ACE (USA), Barclays Bank (UK), Gemplus Technologies Asia, and Transit Link (Singapore). Contact: Centre for Management Technology, Singapore - Tel: +65 345 7322, Fax: +65 345 5928.

CardTech/SecurTech/ISSA '93 Conference and Exhibition, Hyatt Regency Hotel, Crystal City, Virginia, USA, 18-21 April.

Ten concurrent seminars will be held throughout the three main days of the conference - CardTech tracks stressing applications of advanced card technologies, SecurTech tracks addressing specific applications, and ISSA (Information Systems Security Association) tracks focusing on security. A major exhibition is being run in conjunction with the conference. Contact: Ben Miller (CTST) Tel: +1 301 881 3383.

European Financial Self-service '93, Sheraton Hotel, Edinburgh, Scotland, 18/19 May.

Now in its seventh year the conference and exhibition focuses on unattended financial services and is preceded on 17 May with a tutorial on card authentication methods and cardholder verification techniques. Contact: Paula Biagioni, SETG, Glasgow, Scotland - Tel: +44 (0)41 553 1930.

European Smart Card Conference 93, Helsinki, Finland, 1-3 September.

Contact: Eija Ohrnberg - Tel: Finland +358-0-752 0711. Fax: 358-0-752 0899.

The Role of Card Systems in Health Care: Facts and the Future, Pharo Gardens, Marseilles, France, 22-24 September.

A major international conference on the use of card technology in health care featuring speakers from many countries, the conference is being hosted by the French Ministry and Social Affairs, Ministry of Health, and the International Institute of Robotics and Artificial Intelligence. Contact: Elsbeth Monod, French Ministry of Health - Tel: +33 1 40 56 66 93. Fax: +33 1 40 56 64 82.

SX Card from Solaic

SX, the new memory Smart Card from Solaic, the Smart Card manufacturing subsidiary of Sligos, has been developed for multiple applications and multiple service providers.

According to the company it is well adapted to applications with on-card data files (such as in health care and education), security (access control, banking, government offices etc) and electronic payment.

Features include an EEPROM memory that can be loaded with an additional program to expand the functions of the card, a secure operating system that assigns individual protection to each file on the card, while passive security is provided by PIN. Cryptographic functions are based on the DES algorithm contained in the ROM memory.

Contact: Charles Juster, Sligos, France -Tel: +33 1 49 00 96 33.

Deutsche Telekom Order

Solaic, has been awarded a contract to supply Deutsche Telekom with 12 million phonecards in 1993.

This contract follows orders for seven million phonecards in 1991 and 1992, making the company one of the biggest card suppliers to the German communications authority.

Smart Card Tutorial

Part 6 - The T = 1 Comms Protocol

The T = 1 communication is an asynchronous half duplex block transmission protocol. In terms of the OSI model this protocol operates at layer 2, the data link layer. The physical layer (layer 1) operates in the same way as for the T = 0 protocol except for the error detection and correction. In essence this protocol puts an envelope around a block of characters which allows,

flow control
block chaining
error correction.

The choice of communication protocol for the ICC is still a hot topic and one has to consider what advantages can be offered by the block protocol and then to examine the price that must be paid.

The most obvious advantage of the T = 1 protocol is the ability to manage data flow in both directions. In our discussion of the T = 0 protocol it was shown that for a particular command that the data is either sent to or received from the ICC. This limitation was really due to the use of a single byte for defining the length of the data related to the command.

The T = 1 protocol also removes the T = 0 restriction of the master slave relationship where the interface device (IFD) always initiates a command to which the ICC responds. For this block protocol a command may be initiated by either the IFD or the ICC albeit within the restrictions of the protocol.

A further advantage of the T = 1 protocol is the ability to chain the blocks of data such that an arbitrarily large block of data may be transferred as the result of a single command by the transmission of the appropriate number of frames chained in sequence.

The block protocol also has a more sophisticated error management system. This allows the use of a block error detection code (EDC) and the ability to re-transmit blocks that are subject to some error condition. By comparison the T = 0 protocol has a primitive character error detection and correction scheme as described previously in the tutorial (part 4).

Clearly there is a price to be paid for this higher layer protocol. Apart from the more complex software in both the ICC and the IFD the protocol is more demanding on the RAM memory of the ICC which needs to maintain the last sent block in case retransmission is required. In general the T = 1 protocol offers advantages where the application is managing large blocks of data, particularly when it is required to pass data in both directions as part of a particular command. The efficiency of the protocol is only really apparent for larger data transmissions since the underlying physical layer is still operating in character mode as for the T = 0 protocol. The reduction of the character frame to 11 etu (elementary time units) compared with the 12 etu demanded by T = 0 has to be balanced against the administrative overhead of the frame structure which has both a prologue and epilogue.

There can be no doubt that the error control is significantly improved over the T = 0 protocol but at the lower speed of 9600 bit/second operated by many ICC's over very short transmission paths the probability of communication errors is much reduced. However it is clear that there is a move towards the use of the T = 1 protocol and it seems highly likely that this will become the predominant protocol of the future. We should not however dismiss the use of the T = 0 protocol which in some situations may well offer a more optimum technical solution. The T = 1 protocol is specified in the ISO standard ISO 7816 - 3 / AMD.1

The block frame

The frame consists of three fields,

- prologue field
- information field (optional)
- epilogue field

as shown over.

Prologue Field			Information Field	Epilogue Field
Node Address NAD	Protocol Control Byte PCB	Length LEN	Optional INF	Error Detection LRC or CRC EDC
1 Byte	1 Byte	1 Byte	0-254 Bytes	1/2 Bytes

The prologue field consists of three bytes,

- NAD the node address
- PCB protocol control byte
- LEN the data length

The NAD byte uses bits 3 -1 to identify the source address and bits 7 - 5 to identify the destination address. The bits 4 and 8 are used for Vpp control which will not be discussed further here. The node address byte allows the use of multiple logical channels where required otherwise both addresses should be set to zero.

The PCB byte allows the identification of three types of block frame,

- An information block (I - block)
- A receive ready block (R - block)
- A supervisory block (S - block)

The information block is the frame which is used to transmit application commands and data between the ICC and the IFD. The receive - ready block is used as an acknowledgment when the protocol is sending data as a sequence of chained blocks. The supervising block is used to establish control parameters and to effect a resynchronisation or abort status as the result of some error condition. The information block also acts as an acknowledgement byte in the non chaining mode.

The LEN byte indicates the number of bytes (if any) in the information field of the frame. Its allowed range of values are from 00 - FE_{hex}. This allows a maximum information field of 254 bytes.

The information field is used to convey the application commands and data which we will discuss in the next part of the tutorial.

The epilogue field contains the block error detection code which may be either an LRC (longitudinal redundancy check) or a CRC (cyclic redundancy check). The LRC is 1 byte whilst the CRC occupies 2 bytes. This option is defined by the specific interface characters.

Specific Interface Characters.

In a previous part of the tutorial (part 4) we discussed the specific interface characters given by the answer to reset (ATR). The T = 1 protocol uses three of these characters to establish the necessary options before communication can take place. These bytes are assigned as follows (where i > 2),

TAi	=	IFSC	(default = 32)
TBi			
(bit 4 - 1)	=	CWI	(default = 13)
(bit 8 - 5)	=	BWI	(default = 4)
TCi			
(bit 1 = 1)	=	CRC	option
(bit 1 = 0)	=	LRC	option (default)

The IFSC is the information field size for the card. There is also an IFSD which is the information field size for the interface device. This has a default value of 32 bytes and can only be changed by means of an S - block request from the IFD to the ICC.

Waiting Times

The T = 1 protocol uses two waiting time parameters to help flow control,

- Character Waiting Time (CWT)
- Block Waiting Time (BWT)

The character waiting time is the maximum time between successive characters in a block whilst the block waiting time is the maximum time between the leading edge of the last character in a block sent be the IFD and the leading character of the next block sent by the card.

The character waiting time may be used to detect an error in the length of a block whilst the block waiting time may be used to detect an unresponsive card. There is also a block guard time (BGT) which is defined as the minimum time between the leading edge of the last character of one block and the leading edge of the first character in the new block to be sent in the alternative direction. The CWT and BWT are calculated from the values of CWI and BWI coded as shown previously in the specific interface bytes by means of the following equations,

$CWT = (2^{BWI} + 11)$ etu

$BWT = (2^{BWI} \times 960 \times 372 / f)$ Sec + 11 etu

Where f is the clock frequency.

The minimum value for the BWT is 100 mS + 11 etu when the card operates with the default frequency of 3.58 MHz. The block guard time has a value of 22 etu such that the delay between the start of the last character of a received block and the start of a transmitted block is greater than BGT but less than BWT. Accordingly the minimum inter block time is 11 etu which is equal to one character time.

Protocol Control Byte

The protocol control byte identifies the different types of block and carries some control information including a single bit sequence number (N) and a block chaining bit (M). Other bits are used to identify transmission errors. The PCB is coded as follows.

Type	PCB (bits 8-1)								Function
I	0	N	0	0	0	0	0	0	Standard I Block
I	0	N	1	0	0	0	0	0	Chain bit set
R	1	0	0	N	0	0	0	0	No errors
R	1	0	0	N	0	0	0	1	EDC / Parity error
R	1	0	0	N	0	0	1	0	Other errors
S	1	1	0	0	0	0	0	0	Resynch request
S	1	1	1	0	0	0	0	0	Resynch response
S	1	1	0	0	0	0	0	1	IFS request
S	1	1	1	0	0	0	0	1	IFS response
S	1	1	0	0	0	0	1	0	Abort request
S	1	1	1	0	0	0	1	0	Abort response
S	1	1	0	0	0	0	1	1	WTX request
S	1	1	1	0	0	0	1	1	WTX response

The I blocks can occur as independant blocks or as part of a chain. The 'More' bit is set to indicate that further blocks are to follow. The sequence number of the sender alternates between '0' and '1' starting with '0'.

The R blocks are used to acknowledge the successful or otherwise receipt of transmitted blocks. The sequence number N carries the value of the next expected value of N where the transmitter alternates the value as mentioned above. Whilst blocks transmitted as part of a chain must be acknowledged by an R block the receipt of a successful stand alone I block may be acknowledged by an I block response. The two correspondents manage the sequence numbers of their I blocks independently alternating between '0' and '1'. The R block has three possible states as shown in the table.

The S blocks are used to invoke four control states as shown in the table. The resynch request is used by the IFD (only) to force a reset of the block transmission parameters to their initial values. A chain may be aborted by either the IFD or ICC perhaps due to some physical error such as memory corruption. The ICC may send an IFS request to invoke a change in the IFSC it can support. Similarly the IFD may send an IFS request to indicate a new IFSD it can support. The S block control also allows the ICC to request an extension to the block waiting time (BWT) that may be necessary to execute a command received in an I block. The INF field in this block contains a single byte integer value which is to be calculated as a multiple of the BWT value. In all cases the receiver of an S block should send the appropriate response block.

The T = 1 Protocol in Operation

Using the notation of the ISO 7816 standard we can show the basic operation of the protocol. A more complete definition can be obtained from the standard.

I Blocks; I (N,M)

Where N = Sequence number (alternately`0' and `1')

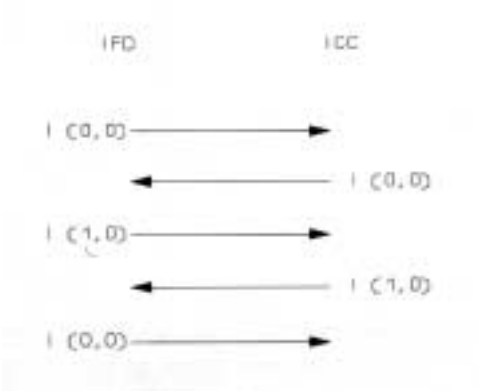
M = More data bit

The More data bit is set when an additional I block is to follow in the chain

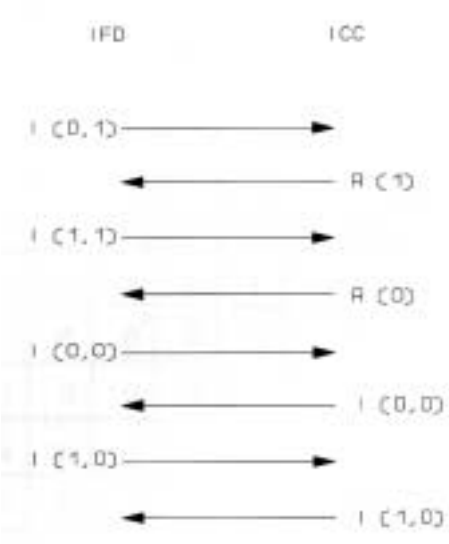
R Block; R (N)

Where N = Sequence number of next expected block

The protocol defines that the IFD and the ICC each have the right to transmit in turn where communication commences with transmission of a block by the IFD.

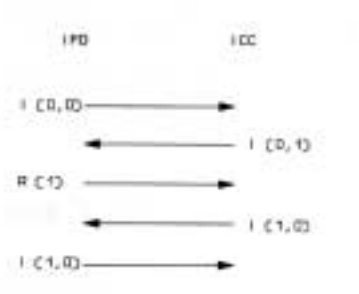


Normal I block transmission



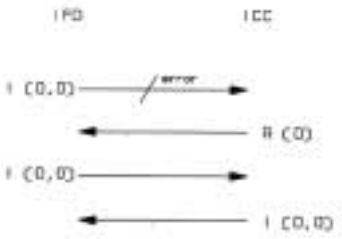
I Block Transmission With Chaining

note that an I block was used by the ICC to acknowledge the last block in the chain sent by the IFD. The ICC may send chained blocks in the same way as shown for the IFD.

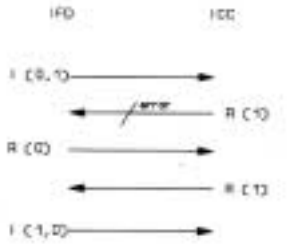


Error Handling in I Block Transmission

Error in I block receipt



Error in I block chain response



In both cases the transmitter is notified to retransmit the block received in error. There are of course a large number of possible error scenarios but they are all based on the simple concepts shown above.

Next month we will look at the proposed Inter-Industry commands.

David Everett

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

Name_____

Position_____

Company_____

Address_____

_____

Tel._____

Fax._____

Name_____

Address_____

_____

Card No._____

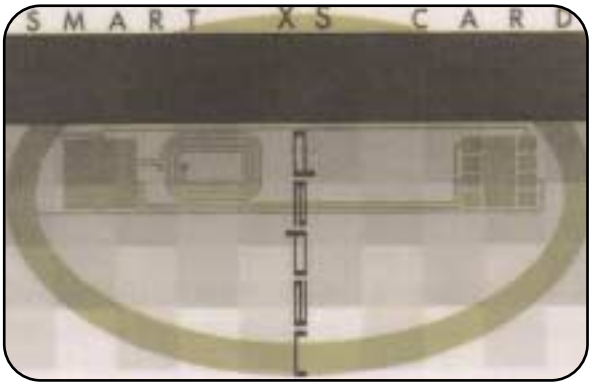
Expiry date_____

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.

Dutch Railways Trial



Field Trials with contactless cards on Dutch Railways are expected to lead to a much bigger trial later this year.

Over 300 employees of Dutch Rail took part in the trials, registering their travelling between Utrecht and the cities of Tiel and Maarssen over a two month period. Some 31,800 valid registrations were made during the trial which ended last November.

The system, which was developed by Dutch Railways, Nedap and Digital, consisted of a registration unit with receiver/transmitter and an LCD display to indicate the train number, platform and departure time together with an "open" registration unit capable of reading contactless cards at a distance of 70 cms. The cards used were standard Nedap contactless cards with EEPROM memory.

Contact: Johan Hogen Esch, Manager Research and Development, Nedap NV, Postbus 6, 7140 Groenlo, The Netherlands - Tel: +31 5440 71111. Fax: +31 5440 62745.

Misubishi Contactless Card

A new contactless Smart Card has been announced by Mitsubishi and is designed for mass user systems ranging from ticketing to automatic warehousing and even production control, providing authorisation and proof of payment functions.

Based on principles of electromagnetic inductance, the card operates at communication distances of up to 50 cms. Two versions are available, one measures 54 x 85.5 x 2.5mm and incorporates a five year life battery, while the other is 1.4mm thick and has a battery life of three years.

Contact: Christine Warren, Semiconductor Division, Mitsubishi Electric UK - Tel: +44 (0)707 276100. Fax: +44 0707 278692.

Pakistan Phone Card Order

Schlumberger Technologies, France, are to deliver one million Smart Cards to Pakistan for the Telecard Company as well as 3,500 Smart Card Payphones, a supervision centre and 700 residential Smart Card telephones.

Contact: Abdellah Nasredine, Schlumberger Technologies - Tel: France +33 1 47 46 66 67.