www.smartcard.co.uk

SMART CARD NEWS

January 1993

Volume 2 Number 1

Smart Cards Being Used in Swiss Ski Resorts

A user-friendly Smart Card is being used in Swiss ski resorts to speed access for skiers to the lifts and avoid frustrating delays. Called the Nedap Ski Card, it is a contactless card which can be read in the skiers pocket and is therefore “hands free.”

The picture below was taken high on the slopes of the Matterhorn in a temperature of -5 degrees Centigrade. Because there is no electricity supply available at this altitude to operate the turnstile, power is provided by a diesel generator.

Continued on page 3

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 6 - Communication Protocols Continued.

Smart Card '93 Conference Report.

CONTENTS

Smart Lunch Cards 4

Smart Card Prototype ATMs 5

Bull/Gemplus Licence Agreement 5

Card Payment in Pubs 6

Student Smart Card 7

Case Study: Loreta Bills Over £1m a Month 8

Carte VITALE - Social Security Card 10

Cylink Advanced Card 12

New Vending System 12

New Fabrication Technology 13

DTI Proposes Smart Card Forum 13

Smart Card Diary 14

Smart Card Tutorial - Part 5 Communication Protocols 15

Schiphol Travel Pass 20

Nedap Ski Card

Continued from page 1

The Nedap system was installed last year in the Zermatt region of Switzerland after rigorous testing over two winter seasons (about 1,500,000 visitors each season). Now about 15,000 cards have been issued by the biggest ski company in the Zermatt area and discussions are being held with other companies operating there. In the Aletsch area about 50,000 cards have been issued by four companies fully equipped with the system.

Nedap are now ready to offer the system to other countries, and this month the ski card will be tested in Solden, Austria.

The Nedap contactless card is used mainly in a ski card system as an electronic ticket for skiers. It can be programmed at the ski area point of sale terminal as a day, week, season or multi-run pass etc. and can be read at up to 70 centimetres at the control gate providing “hands-free” access to the ski lifts.

Advantages for skiers are clear: it avoids the long waiting time for passes to be issued with passport photographs, and reduces the time taken to pass through the control gates to the ski lifts. Skiers no longer have to fumble with tickets or physically show passes while trying to hold onto their gloves and ski sticks. They do not even have to take the pass out of their pocket. The Smart Card is checked automatically when they stand in front of the turnstile and if it is valid a green arrow lights up and they can pass through the turnstile. If the card is not valid a red arrow lights up and the gate remains locked.

More than 800 people per hour can be checked passing through the control gate - about twice as many as at gates where each skier has to physically show a pass and then put it away.

At the point of sale terminals, which consist of a PC-cash register, a video camera and a machine to issue the card, the Smart Card is automatically programmed with all information, for example, type of user, time validity and area. The terminal can produce a photo of the user electronically in seconds and attach it to the card.

Sales data is stored twice in the PC-cash register and transferred to the system computer on a disk. Thus the cashiers’ reconciliations and the daily reconciliations are produced automatically.

Benefits for the system operator

Nedap has produced cost-comparison figures against the normal magnetic stripe card in such a system. Although the magnetic stripe card costs approximately $0.25 compared with the Nedap Ski Card at $15, it is thrown away at the end of the validity period.

The Nedap Card can be used for a guaranteed minimum of 5,000 times and, therefore, costs approximately $0.03 each time it is used, making it eight times cheaper than the magnetic card.

For season tickets with a passport photograph there is an additional charge of about $0.04 for the video ticket and the packing.

They say that a company that needs 500,000 magnetic cards would only need 35,000 Nedap Ski Cards. The Nedap card becomes viable after four years in operation and, after ten years the company has saved around $700,000.

Skiers normally pay a deposit of $15 for the card which is reimbursed at the refund machine or cash point on redemption of the card. If the card is lost or the customer does not return it, the company retain the deposit to purchase a replacement card.

It is possible to use the system in an area involving several companies, and make periodic reconciliations. For example, Company A sells a Nedap Ski Card valid for its area and also the area of Company B. The amount of money due by Company A to Company B can be calculated automatically, based on the number of transactions registered on the Ski Card. Similarly if B issues cards that can be used in A’s area, money can pass from B to A.

Card details:
Type:Contactless
Fabricator:Nedap
Dimensions:84.5 x 54.5 x 3.5 mm
Contact location:N/A
Chip manufacturer:Hughes
Chip type:CPU

Memory type:EEPROM
Memory capacity:128 bits
Comms protocol:Patented by Nedap
Security:Proprietary

Contact: K van Raay, Manager Ski Card System, Nedap NV, Postbus 6, 7140 Groenlo, The Netherlands. Tel: +31 5440 71111. Fax: +31 5440 62745.

Smart Lunch Cards

SOLAIC, the Smart Card manufacturing subsidiary of French computer engineering company SLIGOS, has been awarded a contract by the city of Montpellier, France, to supply 10,000 MIDI integrated circuit cards for use in school lunchrooms.

The cards have been under test in two lunchrooms since last May and will be gradually extended to over 100 establishments managed by the city's central kitchen.

The card will eventually allow schoolchildren to pay swimming pool fees and school bus fares.

Card details:

Type:	Contact
Fabricator:	SOLAIC
Dimensions:	ISO ID1 size
Contact location:	ISO or AFNOR
Chip Ref No.:	E3744
Chip Type:	Memory
Memory type:	EEPROM
EEPROM	3744 bits
Standards:	ISO 7816-1, 2, 3
Security:	PIN (four digit)

Contact: Charles Juster, Corporate Communication, Groupe SLIGOS - Tel: France +33 1 49 00 96 33.

DataCard Reorganises

DataCard Corporation announced last month that it was reorganising the company into three global operating groups that will report to Glenn W Highland, DataCard's President and Chief Executive Officer.

The Plastic Cards Group will consist of DataCard's four plastic card manufacturing plants located in the United States, United Kingdom, Germany and The Netherlands. Franz Hanlel, Corporate Vice President, European Sales, has been appointed acting General Manager.

The Card Personalization Group will comprise all products the company manufactures for personalizing credit, debit, identification and promotional cards. Jim Moar has been appointed Corporate Vice President and General Manager.

Three business units - Datatrol Transaction Terminals, Addressograph Imprinters and Smart Cards and Systems will be consolidated in the Transactions System Group, with CEO Glenn Highland acting as General Manager.

Contact: Mark Iverson, DataCard Director of Communications - Tel: USA +1 612 931 1763. Fax: +1 612 931 0418.

Smart Card Club Launched

The Smart Card Club was officially launched at an inaugural meeting in England this month which attracted 95 attendees from more than 60 companies.

"We see the Smart Card Club as the premier forum for every UK company involved in Smart cards," says founder, Richard Poynder. "Already the sector's major players have agreed to join and the final mix of members is in line with our target split of 50:50 vendors and scheme operators." He said the club had exceeded its original targets with a membership now set to exceed 35 major organisations.

Membership, which costs £5,000 for full membership and £2,500 for associate membership, is open to any company actively involved in developing or using Smart Card schemes and is based around a series of monthly meetings during 1993.

Contact: Richard Poynder -Tel: England +44 (0)753 83083. Fax: +44 (0)753 831113.

Smart Card Prototype ATMs

Prototypes of a new generation of Automated Teller Machines (ATMs) that will use contactless Smart Cards were demonstrated, along with potential applications, at the Retail Delivery Systems Conference in San Antonio, Texas, last month.

Developed by NCR Corporation and AT&T Smart Cards, the units are designed to offer customers additional services, such as a security system that works by verifying the cardholder's voice print. Unless this matches the one stored on the card, access to the account is denied.

Although there has been great interest in the use of voice prints as a means of positively identifying the cardholder as the rightful owner of the card, the technology has not yet advanced sufficiently to ensure an accuracy for mass market use, for example, at points of sale where high false rejection rates would be unacceptable. The most likely use of this technology is for telephone home banking applications.

Perhaps more significant is that AT&T's Smart Card readers can be connected to NCR's point of sale terminals, and they plan to begin working with banks to develop new Smart Card-based applications that will run on both ATM and point of sale machines.

The readers can also be connected to a cellular or wired telephone, personal computer, car (for electronic toll collection), and other devices.

"Our Smart Card can be viewed as a secure, portable, personal database that will provide banking customers with enhanced security and a broad spectrum of new services," says Diane Wetherington, President of AT&T Smart Cards.

"Most people have come to think of ATMs mainly as cash machines," says Jim Adamson, Vice-President of NCR Self-Service and Financial Systems Division, in Dundee, Scotland. "But the integration of Smart Card readers can transform the familiar ATM into a new kind of Financial transaction station."

One obvious benefit of Smart ATM Cards is increased security, and a single card can be used as an ATM card, an insurance information card, and a debit card for making purchases in a store, placing phone calls, paying highway, bridge and tunnel tolls, mass transit fares and even making purchases from vending machines. Funds for each of these uses can be transferred at any ATM from the customer's bank account to the debit portion of the card.

"Smart Cards make it possible for ATMs to expand beyond mere banking functions," said Mr Adamson. For example, "electronic tickets" for airline travel, sporting events, plays or concerts could be purchased at an ATM and loaded onto the Smart Card. The card would then be accessed at the airport, stadium, theatre or concert hall.

AT&T plans to make the Smart Card interface available to other terminal developers.

Contact: Michael Jacobs, AT&T Smart Cards, USA - Tel: +1 (201) 564 3836. Jim Mazzola, NCR Corporation, USA - Tel: +1 (513) 445 6148.

Bull/Gemplus Licence Agreement

Two of the major players in Smart Card Technology, Bull CP8 and Gemplus, have confirmed an agreement whereby Bull CP8 has licensed Gemplus for the use of Bull CP8 patents related to Smart Cards.

The patents are used for the development of the most important part of the microprocessor cards - the operating system or "mask" used to provide the level of security required for the various functions of the card, and internal operations which allow the card to be used in a wide variety of applications, for example, payment systems, health cards, pay-TV, telecommunications, transport systems, personal files, etc.

Bull says the agreement is part of its policy to provide access to its patent portfolio in this domain. At the same time the move will strengthen the position of both companies in the Smart Card field.

Contacts: Marc Lassus, Gemplus Chairman and CEO - Tel: France +33 1 42 32 50 01; and Jean-Louis Coulon, Bull CP8 Chairman and CEO - Tel: France +33 1 39 02 44 00.

Card Payment in Pubs

Regulars at 12 Whitbread managed public houses are able to pay for drinks and machine games using Smart Cards in a trial scheme which will run for six months.

Whitbread's are using a system from Cashcard Systems, based in Newark, Nottinghamshire, England; and Smart Cards from Schlumberger Technologies, France, who are Cashcard's development partner and a leading producer of Smart Cards, systems and software.

The pre-payment Smart Cards are proving popular with customers at the test pubs. At The Hendon, in North West London, Manager John Hyde said: "The trial is going well. It's a good concept and in just over two months we have issued over 1,000 cards."

All of the pub's amusement machines are now card operated and if customers want to play them they have to have a card. The trend now is to use the card as a "piggy bank" and to buy drinks with it.

Customers who use machines frequently gain points which are added to their cards. For every 100 points they earn a free pint.

Most regulars now have cards, said Mr Hyde. Among the benefits are that it saves giving and holding change, and the machines do not hold cash.

There is no charge for the card and it is easy to operate. In the weeks before Christmas some customers were putting £2 a day on their cards and at Chritsmas Eve or New Year's Eve they had between £80 and £90 to spend.

In another test pub, The Portsbridge, at Cosham, Potsmouth, the trial was described as a "huge success" by licensee Dave Milner. Many customers now deposited enough money on their cards to last them through the week, he said. Recently he issued over 130 cards to customers in one week. The cards saved hassle in supplying loose change.

From Whitbread's point of view there is less cash on the premises and, where amusement machines are card operated only, there is no cash stored in them and no need for them to be emptied. The card, of course, also encourages customer loyalty.

The customer chooses the value he or she wants put on the card at a validator unit sited at the point of sale where the cards are encoded with the credit. The cards are then usable, in the majority of cases, for the normal cash transactions across the bar and at pinball machines, juke boxes, and pool tables etc.

Users simply insert the card in an acceptor unit fitted to machines or equipment. The amount of credit on the card is shown on an LCD unit. The unit then shows the appropriate price, for example, of a drink or a game of pool and this amount is debited from the card.

As it debits the card, the acceptor can also be programmed to write incentive points back onto the card, perhaps entitling the customer to a free drink after so many points have been accumulated.

At present use of the card is restricted to the pub where it is issued, but eventually it could operate across a chain of leisure outlets.
Card details:

TypeContact
FabricatorSchlumberger
Dimensions85.6 x 54.0 x 0.80mm
Contact locationFront (either top or centre)
Chip manufacturerSchlumberger
Chip reference no.SE416
Chip typeMemory + logic
Memory typeEEPROM
Memory capacity416 bits
Comms protocolSychronous
SecurityPIN (16 bits)
CryptographyDES

Cashcard Systems are currently in discussion with seven national pub retailers, four bowling operators, two bingo operators, a cinema chain, a brewery and a family entertainment centre.

Contact: Mike Bowen, Card Project Manager, Whitbread - Tel: England +44 (0)582 424200.

Smart Student Card

A Smart Student Card is being used by students at the University of Lille in Northern France. The use of a card - based portable file enables students to carry their own records in a safe way while allowing the university authority to access and update the files when required.

In addition to storing academic records, the multi-application card can also be used to pay for meals in the university restaurant, pay for the use of photocopiers and control access to libraries, laboratories and sporting and other university facilities.

Smart Cards offer the advantages of automating administration filing systems, a standard communication device, security to provide reliability of student records, payment functions to minimise the use of cash on the university premises, and a single device for multiple access.

Between 20,000 and 25,000 Philips TB100 multi-application Smart Cards have been issued in the project.

Card details:

TypeContact
FabricatorPhilips
DimensionsISO ID1
Contact locationBack
Chip manufacturerMotorola
Chip type68HC05
Memory typeEEPROM
Memory capacity
Mask ROM6 Kbytes
EEPROM3 Kbytes
RAM128 Bytes
StandardsISO 7816-1, 2, 3
SecurityPIN
CryptographyDES

Contact: Janice Ratcliffe, Philips Communication Systems - Tel: England +44 (0)223 444888.

Advanced Card Association

Plans are being made to launch an Advanced Card Association (ACA) as a professional association for the promotion and development of Advanced Cards, of every type, and to represent the interests of the advanced card industry to government bodies, standards organisations and to the various market sectors. It will also provide information to members, including a pan-European central information database.

A list of proposed objectives is available and the organisers are particularly interested in hearing from companies who would be prepared to act as a “key contact” for a particular country.

It is intended that the ACA will be a non-profit making organisation. If you or your company are interested in discussing your involvement in the joining and establishment of ACA, then contact: Simon Reed or Chris Stanford, c/o Charta Associates Ltd, The Court, FREEPOST, PO Box 301, Hemel Hempstead, Herts, HP1 1BR, England. Tel: +44 (0) 442 231844. Fax: +44 (0)442 236604.

Patient Data Card Pilot

Smart Card suppliers will be disappointed to learn that the National Health Service in Scotland has chosen an optical memory card for its Patient Data Card system pilot project to be set up in the Grampian area. Some 8,000 cards will be issued to patients this year and the pilot project will run until 1996.

The £750,000 contract has been awarded to EDS-Scicon. The card selected is an optical memory card which uses laser technology to read and write information on the card. The NHS card will have the capacity to hold between 800-1,200 A4 pages of information.

Health Care Conference

A major international conference on the use of card technology in health care to be held in France in September (See Diary on page 14) will feature top speakers from many countries.

France and Germany are to use Smart Cards in their national health programmes and plan to issue cards nation-wide by the mid-1990s, while in the United States there is strong interest in reform of the health services.

CASE STUDY

Loreta Bills Over £1m a Month

The Loreta (LOcal RETail Accounting) Smart card scheme for small garage businesses appears to be one of the most successful applications of Smart Card technology.

Last year Loreta was billing over £1 million a month but since then it has increased the number of terminals installed in garages from 250 to 350 and issued a further 15,000 cards bringing the total number of cards distributed to 35,000. Even in an economic recession which has hit small businesses hard, the Loreta scheme has increased its share of a highly competitive market.

After a pilot test, the scheme went "live" in October, 1990. It was devised by PHH Europe, based in Swindon, 140 kilometres west of London, England, and a subsidiary of the PHH Corporation headquartered in Maryland, USA. Few people have heard of PHH because it provides a range of services to other companies and does not deal directly with the public.

To understand the Loreta scheme it is helpful to look at another part of the company's business operations. In the UK, it has some 600,000 charge cards used regularly in a network of 20,000 filling stations and repair workshops. Among these is the AllStar Fuel Card (a magnetic stripe card) which is claimed to be a market leader with over 50 per cent of the served market. However, this card is normally used for fleets of over 100 vehicles because of the credit requirements. As a result, products like AllStar are only available to about one third of all company operated vehicles in the UK, whereas the bulk of the market is made up of small fleets of up to 10 vehicles. Market research also showed that many garages wished to offer credit accounts to local companies because it produced repeat business.

Market Opportunity

Here was a market opportunity - a substantial unserved market of small fleets of company operated vehicles, a majority of garages wishing to offer credit facilities to the same market but unable to do so due to the credit risks involved.

As a result of their research, PHH decided that Smart Cards provided the means to manage credit risk along with the ability to handle a wide range of end user requirements cost-effectively.

They selected Schlumberger's Smart Card division in The Netherlands as their main partner and they supplied the Smart Cards and terminals and developed a large part of the software for a small scale pilot.

The concept

The concept devised by PHH was that the retailer would "own" the product and use it to promote account business at his garage in competition with other garages in the area, thus PHH was to accept the full credit risk for the retailer.

The products would be branded to the retailer's requirements and they would be provided with a marketing package to help the retailer sell the product.

Thirdly, PHH would provide a regular cash flow to the retailer by paying him weekly, although the card users would be invoiced less frequently.

Then the card had to be able to support any pricing structure - discounts and surcharges - required by the retailer on the range of products offered for sale via the card.

Attraction for Garages

An attraction for garages is that they can have their customer cards specially branded. Some companies, typically multi-
national oil corporations such as Esso, BP and Elf, choose to have a unique design. However, smaller garage chains may adopt a variation of the standard Loreta card, the retailer making his choice depending upon his particular marketing strategy.

Both types of card used in the Loreta system are Schlumberger M64 microprocessor cards, using the A2 mask. The retailer card is located inside the PIN pad and includes files containing details of products such as fuel, shop goods and cash, and sub-products, for example, diesel or unleaded petrol as types of fuel.

The customer card, which has the capacity for over 800 transactions, includes the transaction directory where records of purchases against the purse (or credit line) and mileage for each permitted Vehicle Registration Number (VRN) are stored; and the parameter directory where attributes relating to the purse (such as value), VRN's and terminals are stored. This file can be modified by card parameter change records without the card being recalled from the user.

PHH have installed an IBM RS/6000 processor at their headquarters at Swindon (this replaces PCs used in the pilot test) to handle data transfer, normally during the night. It sends records to the point of sale terminals and collects the customer card sales transactions and confirmation that card parameter changes have been applied to the cards. If required, blacklisted card numbers and marketing messages can be downloaded to the terminals.

When a user presents his customer card at a garage, the transaction time is about 30-40 seconds - about the same time required to process a magnetic stripe fuel card transaction.

Managing the risk

The Smart Card is seen as a key element in minimising the company's exposure to bad debt. If an account becomes bad, the company's exposure can be controlled either by reducing the purse values, or by blacklisting the card and blocking it the next time it is inserted into a terminal.

When spending limits have been established in line with expected card usage, the agreed spending power is distributed across the cards making allowance for the number of vehicles involved and the type of products to be purchased. For example, a card may be used only for frequent purchases of fuel, or perhaps infrequent but high-value servicing may be required. Depending on the pattern as many as 48 electronic purses can be established in the card, ie up to one purse per separate product that Loreta allows.

During transactions, the appropriate purse is decremented by the value of the item. As customer invoices are produced twice a month, each customer card is automatically revalued at the point of sale, back to the agreed purse limits, unless the customer is on the black list.

Key Aspect

Another key aspect of the system is end user flexibility. A garage manager, for example, does not want his account customers to use their cards at other garages in the same chain in the area, but he would want the card to be used in his company's chain if the vehicle goes out of the area. PHH have developed a technique which allows this flexibility of control and also pricing flexibility, for example, if a garage wants to offer big spending customers a discount on car wash only, or on the other hand add one pence per litre to pump prices for others, this can be achieved utilising the relational file system operating on the IBM RS/6000.

Conclusion

The success of the Loreta scheme lies firstly in recognising a new business opportunity and then conducting extensive market research into customer requirements and managing the credit risk. To have used magnetic stripe technology would have required on-line authorisation of each transaction and profit margins would not support the high costs involved. PHH, therefore, decided that they could only offer this service profitably by using Smart Card technology.

Secondly, after pilot testing, they invested in a central computer system with over 100 relational databases and about 200 programs. PHH believe that it is only by combining the powerful applications of the Smart Card with complex transaction processing systems that the real value of the Smart Card can be exploited.

Not only has the Loreta Smart Card system helped PHH to break into a new market, it can also boast that its clients include film stars, sports personalities and members of the Royal Family.

Contact: Simon Reed, Charta Associates Ltd - Tel: England +44 (0)442 231844. Fax: +44 (0)442 236604.

Carte VITALE - The French Social Security Card

Experiments with the Carte VITALE, the French Social Security Card, are being extended this year to three further sites, bringing the total to seven. In addition the card readers are being replaced with units with a greater memory capacity, and there will be a new version of the Bull CP8 card.

The objectives of the experiments are to streamline the administration and reimbursement procedures of the French Social Security services by:

* replacing claim forms

* eliminating the use of medication labels for reimbursement

* cut reimbursement time from weeks to under 48 hours

* make substantial savings in Social Security costs

* offer cardholders other services.

To give some indication of the size of this project, the Social Security system in France covers three main insurance schemes with 80,000 employees, 28 million members and about another 28 million dependants.

Each year over 800 million medical claim forms are filled out by medical practitioners and then by claimants, and some four billion labels are attached to them before they are processed.

The experiment began with project SESAM - pilot schemes each involving between 4,000 and 5,000 social security members and pharmacists in the towns of Boulogne-sur-
Mer, Bayonne, Charleville and Rennes.

This was followed by a full VITALE card project in Boulogne-sur-Mer, and more than 121,000 cartes VITALE have been issued.

Participating in the scheme, each with their own card, are CNAMTS, the French National Health Insurance Scheme for Salaried Workers; MSA, the Farmer's Mutual Insurance; and CANAM, Health Insurance for Non-Salaried Workers. They were joined at the end of last year by the railway employees and civil servants.

The practitioner's card (CPS) is issued to all medical practitioners - doctors, dentists, pharmacists, nurses, therapists, and laboratories. Some 666 practitioner's card readers (MPSs) have been installed for use by CPS cardholders in their surgeries, dispensaries and laboratories to authorise the type and cost of treatment.

There are 117 public terminals at which cardholders can read the information on their cards after treatment and have their cards updated if their entitlements change.

It is also possible for health professionals to read the history of settlements made.

How the system works

At the doctor's

When medication is being prescribed, the CPS card held by the doctor and the VITALE Card

held by the patient, are inserted simultaneously into the MPS. The treatment and cost are authenticated together with the patient's entitlements and then the doctor issues the prescription.

The treatment records stored in the MPS are polled each night to the Social Security processing centre so that the patient or the doctor, depending on who has borne the cost, is reimbursed with minimum delay.

At the pharmacist's

The patient takes his prescription to the pharmacist. His medication is bar coded so that the pharmacist can record the transaction immediately on his own MPS. The cost of the medicine is then authenticated by the simultaneous introduction of the pharmacists CPS card and the patient's VITALE card. When the data has been collected and processed, the pharmacist or patient is reimbursed.

Developments

This year sees the replacement of all MPSs with larger memory units and an extension of the experiment to three other sites which will study a new version of the Carte VITALE with the possibility of exchanging information with biologists and radiologists. The seven sites will evaluate their experiments at the end of 1994.

Present card details:
TypeContact
FabricatorBull CP8
DimensionsISO ID1 size
Contact locationFront
Chip typeMicroprocessor
Chip referenceM4
MemoryEPROM
Memory capacity1 Kbyte
StandardsISO 7816-3
Comms protocolT=0
SecurityPIN (4 digits)
CryptographyTelepass algorithm

Future card

The future VITALE card to be supplied will be an 8 Kbyte EPROM card, SCOT 20 using the DES algorithm.

Contact: Yves Girardot, Bull CP8 - Tel: France +33 1 39 02 44 63. Fax: +33 1 39 02 44 02.

Cylink Advanced Card

Cylink Corporation, a leading international supplier of commercial data encryption devices to financial institutions and multinational corporations has developed an Advanced Smart Card designed specifically to the meet the demands of the high-
security, public key cryptosystem marketplace. Based in Sunnyvale, California, the company says the card will be available in the first quarter of this year.

Field-programmable, the Smart Card is designed for system applications requiring high-security, distributed database access control, digital signatures, and key management. It uses an enhanced Intel 80C31 microcontroller and contains 16K bytes of non-volatile program and data storage memory.

The chip has a 512 bit public key maths coprocessor that can implement a 512 bit exponentiation in 1.5 sec. The device also contains a random number generator.

Card details:

TypeContact
FabricatorCylink
DimensionsISO ID-1
Contact locationFront
Chip typeMicrocontroller
Chip reference80C31
Memory typeEEPROM
Memory capacity
Mask ROM-
EEPROM16 Kbytes
RAM768 bytes
StandardsISO 7816-1, 2, 3
CryptographySupports popular public key protocols, including RSA and DSS.

Contact: David Moseley, General Manager, Cylink Ltd - Tel: England +44 (0)256 468186. Fax: +44 (0)256 24156.

New Vending System

Dutch Smart Card Consultants, S C Application Services, have developed a new vending system which is able to accept Smart Cards as well as coins thus giving customers choice and convenience while providing useful statistical data for operators.

Based on the “Mars Money” protocol, a hardware module sits between the Vending Machines Controller (VMC) and the Coin Validator and controls all communications. The VMC displays the received amount which is deducted from the value on the Smart Card, or if a money value is left over, the Validator will return change.

The company decided that the usual four digit LED display was insufficient and have provided a display with two lines of 16 characters to give the customer more information concerning the status of the Smart Card in use.

No special knowledge of operating vending machines is required. There is a Service Card which contains the price list and which can be changed easily by the operator. The information in the VMC - which used to be the price list - has been changed into an index list of products and only has to be installed once. This index list contains the information on the product chosen by a customer and is sent to the controller which is able to get the corresponding price out of memory.

Statistical information can be collected by the operator with a Data-collector Card. This card is recognised by the controller which sends its information to the collector, for example, the machine number and type, total number of vends, number of vends between two collections, total amount of money, amount of money received between two collections, and the collector counter.

Contact: P W M Brouwer, S C Application Services, The Netherlands - Tel: +31 2503 21500. Fax: +31 2503 21702.

Cost Savings of £1.6 million

Contactless Smart Cards to automate ticketing will save £1.6 million a year, says Mike Hill of Greater Manchester Passenger Transport Executive.

New Fabrication Technology

Sempac (Semiconductor Packaging) SA, based in Cham, Switzerland, have bought the patents of French inventor Gerard Lemaire which they say will allow chip cards to be produced at an economic price to rival magnetic cards. The patents were purchased for "a single figure sum in millions" according to President Karl Nilklaus.

The patents and exclusive rights to this special technology were acquired last year and Sempac says that each machine will be able to produce 600-700 cards per hour and that the cost per card can be reduced by up to 50 per cent.

Lamaire developed a process by which the chips can be "potted" in the cards. The concept is based on a highly developed process for producing integrated circuits and an injection moulding process.

Manufacturing Process

The manufacturing process in largely based on thermosonic bonding of gold wire on copper leadframes. and with "multi-process card technology," it is possible to perform eight process steps in a single operation. The injection moulding machine possesses special options which enable it to handle micromodules, graphics and cards optimally.

It is possible to carry out just-in-time production on a three-shift basis without interruption.

The company not only sells complete Smart Card manufacturing lines, but also licences.

Sempac was founded in July 1992 and is a subsidiary of the ESEC Group, which has its corporate headquarters in Cham, Switzerland. It is the first company in the semiconductor assembly industry to compile and co-ordinate complete chip assembly lines for Smart Cards.

Contact: Willi Truckenbrod, Vice President and General Manager Marketing and Sales, Sempac - Tel: Switzerland +41 42 44 53 53. Fax: +41 42 41 61 24.

DTI Proposes Smart Card Forum

Britain's Department of Trade and Industry are proposing to set up a Smart Card Forum for existing and potential users and suppliers, to exchange information and undertake mutually supportive activities.

At a recent meeting of over 40 suppliers, bankers and end users, the response was "not immediately enthusiastic," according to Ms Di Williams of the DTI.

"We have had few firm responses so far," she said and emphasised: "The Forum has to be industry lead. We are only acting as the catalyst and focal point if people want to go ahead."

A prospectus, which is available to interested parties, says UK Government Departments will be involved as potential users, and the DTI in its role of providing research support, industry sponsorship, and the promotion of innovative uses of IT.

The prime objective of the Forum will be to achieve maximum benefit for the UK from the development and introduction of Smart Card technology.

Success will be measured in terms of the speed with which potential users take up the Smart Card, "mirroring its much greater application in France and Japan," and increased success by UK vendors of Smart Cards and associated products.

Activities are likely to include the preparation of common positions to promote action, and conducting surveys on the potential market, research into the implications of multi-application Smart Cards, and existing patterns of use of the main industry standards.

Members will be asked to make an initial payment of £1,500, and further calls for payment may be made as necessary depending on the number of members.

Contact: Ms Di Williams, DTI, Room 4/150, 151 Buckingham Palace Road, London, SW1W 9SS. Tel: England +44 (0)71 215 1902.

Smart Card Diary

Smart Card '93 Conference and Exhibition, Wembley Conference Centre, London, 16-18 February.

Six conference streams covering communications, market overview and marketing systems, finance and security, medical, technology and innovations, and transport and travel. In addition there will be a half-day seminar on 15 February providing a practical introduction to Smart cards for new and potential users. A second hall has now been opened for exhibitors. Contact Conference Secretariat Tel: +44(0)733 394304.

The 1993 Pan European Digital Cellular Radio Conference: GSM Under The Spotlight, The FIL Congress Centre, Lisbon, Portugal, 16/17 February.

With GSM networks now in place and rolling out, the conference will concentrate on markets plans and expectations, reports from network operators and manufacturers, and examine critical issues and the needs and expectations of users. Contact Tania Starley, IBC Technical Services, London - Tel: +44 71 637 4383.

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.

Swiss Card Order Goes to France

Philips Smart Cards and Systems Division in France are to deliver 400,000 pre-paid Smart Cards to the Swiss PTT. This is the first time that the Swiss PTT have opened up the market by going outside of Switzerland to order Smart Cards.

Smart Card Tutorial

Part 5 - Communication Protocols

At the current time there are two communication protocols that are in general use,

T = 0 asynchronous half duplex character transmission
T = 1 asynchronous half duplex block transmission

The T = 0 protocol is the predominant protocol in France and was the only protocol specified in ISO 7816 - 3. In 1992 ISO standardised the T = 1 protocol as amendment 1 to ISO 7816 - 3. Clearly the IC card and the interface device must operate with a common protocol. The method by which they achieve a common optimum configuration has been the subject of much discussion over the last few years. This principle is intended to be achieved by the use of protocol type selection (PTS). This is effectively a special command sent from the interface device to the ICC after the answer to reset. In order to maintain backward compatibility with existing commercial systems that may only be capable of handling the T=0 communication protocol some changes are necessary to the original ISO 7816-3 standard. A new concept is proposed which identifies the principle of two modes of operation,

- Negotiable mode
- Specific mode

An ICC that operates in a negotiable mode may have its communication protocol changed by the use of the PTS command. An ICC that operates in the specific mode cannot accept a PTS command but may be put into the negotiable mode by a further assertion of the reset command.

Although the ICC indicates to the interface device (by means of TA2) its capability to change to the negotiable mode, an existing device in the market place may however be unaware of these changes and therefore will not be prepared to reset the card.

The operation of these mode changes are shown in fig.1. It should be noted that a multi protocol card which by definition offers the negotiable mode of operation should give priority to the T=0 communication protocol. In other words if the T=0 protocol is available it should be the default protocol offered in the answer to reset.

The TA2 interface byte which is part of the answer to reset data (discussed in part 4) gives the necessary information to allow the appropriate choice of protocol. The coding of this byte when present is shown in fig.2. In fact the presence or otherwise of this byte is used to determine the mode of operation of the card as follows,

TA2 present in ATR	-	Specific mode
TA2 absent in ATR	-	Negotiable mode

It can be seen that bit 8 in the TA2 byte is used to tell the interface device whether the card can change to the negotiable mode.

Protocol Type selection (PTS)

Protocol type selection is used by the interface device to change the communications protocol and/or the default values of FI and DI. The PTS command must be issued immediately after the answer to reset and only applies when the IC card is in the negotiable mode.

The interface device may choose to operate by using the first indicated protocol after the answer to reset and by using the default values of F and D. This results in an implicit selection of the protocol and the communication parameters. Should the interface device wish to effect any change to this situation then it must issue the PTS command.

The PTS request consists of an initial character PTSS (coded FFhex), followed by a format character PTSO, and three optional characters PTS1, PTS2, PTS3 and PCK the check character. This is shown in fig.3. The response from the ICC follows the same format as the request.

The PTS0 format character is encoded as shown in fig.3. The bit map is used to indicate the presence or otherwise of PTS1, PTS2 and PTS3. These are encoded by bits 5, 6 and 7 respectively where a logic `1' level indicates the presence of the character. The protocol type is indicated by bits 1, 2, 3 and 4 which are binary encoded for T=0 to T=15.

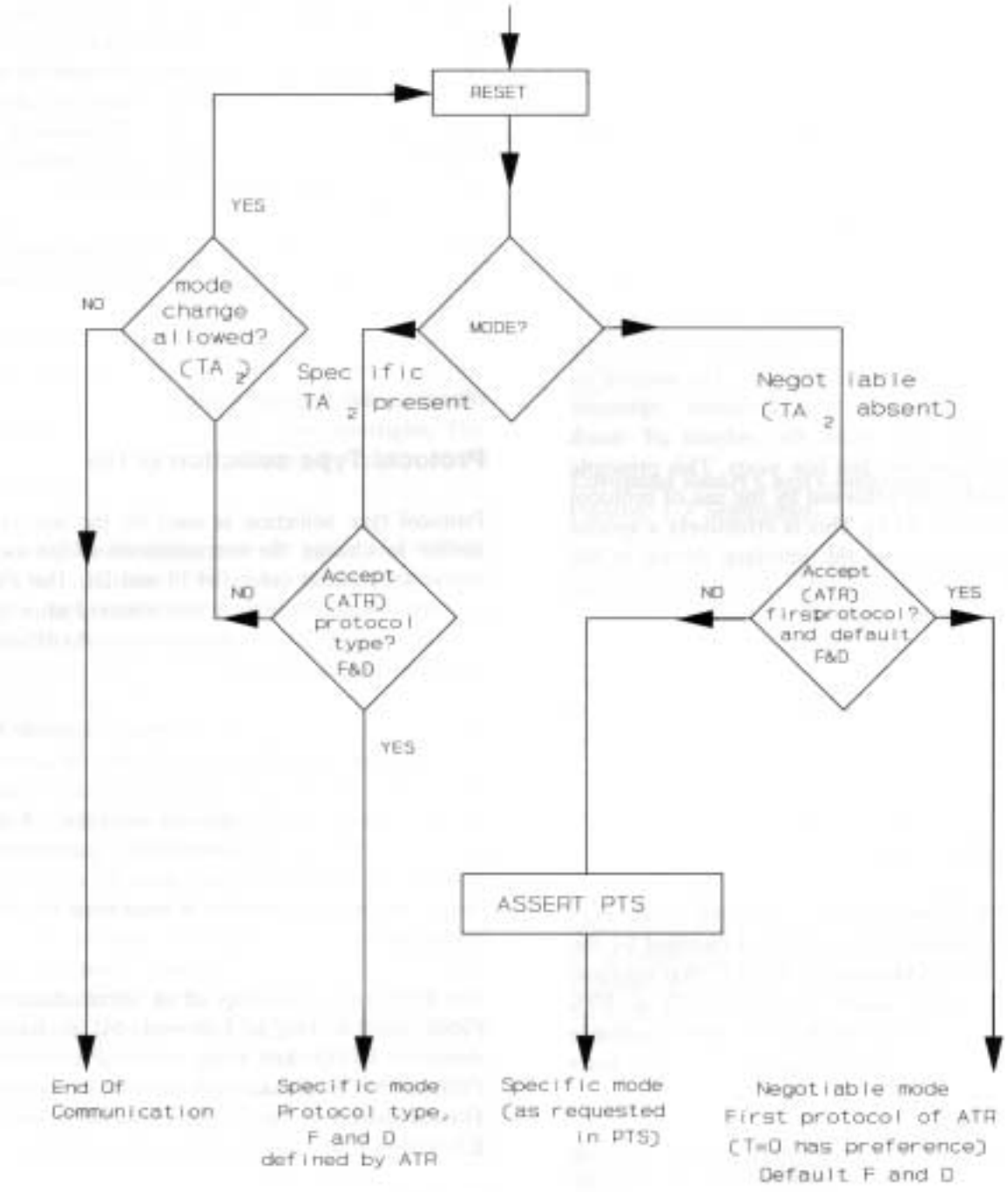

Fig 1. MODES OF OPERATION

The PTS1 character when present is used to define the values for FI and DI as coded for TA1 (see part 4). These parameters are used for defining the work etu (elementary time unit).

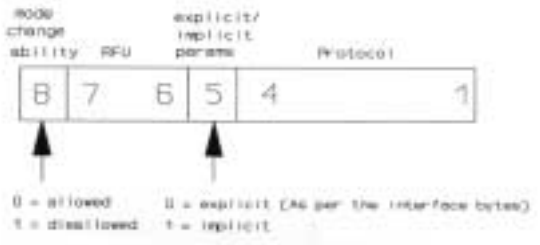

Fig 2. THE TA2 INTERFACE BYTE

The check character PCK is computed such that the exclusive OR (XOR) of all the characters from PTSS to PCK inclusive is equal to zero.

When the ICC implements the PTS request message correctly it replies by echoing the same request as the response message. If bit 5 of the PTS1 response character is set to zero then the default values of F and D will be used.

The T=0 communication protocol

The interface device always initiates the command for the T=0 protocol. Interaction between the interface device and the ICC results in successive commands and responses. For this protocol, data can only flow in one direction for the command response pair. In other words, either the command message contains data for the ICC or the command request data from the ICC which is then included in the response.The direction of data flow is implicit on the definition of the command and hence both the interface device and the ICC need to have the necessary a-priori knowledge. When it is required to transfer data in both directions for a particular command then a get response command may be used after the primary command to recover the response data.

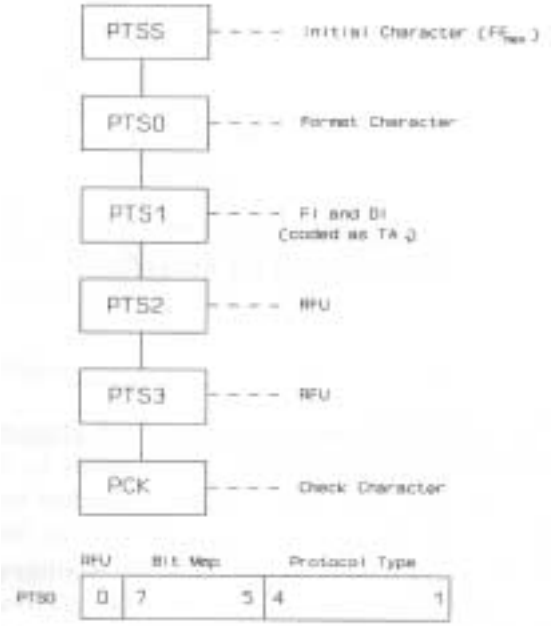

Fig 3. PTS REQUEST AND RESPONSE

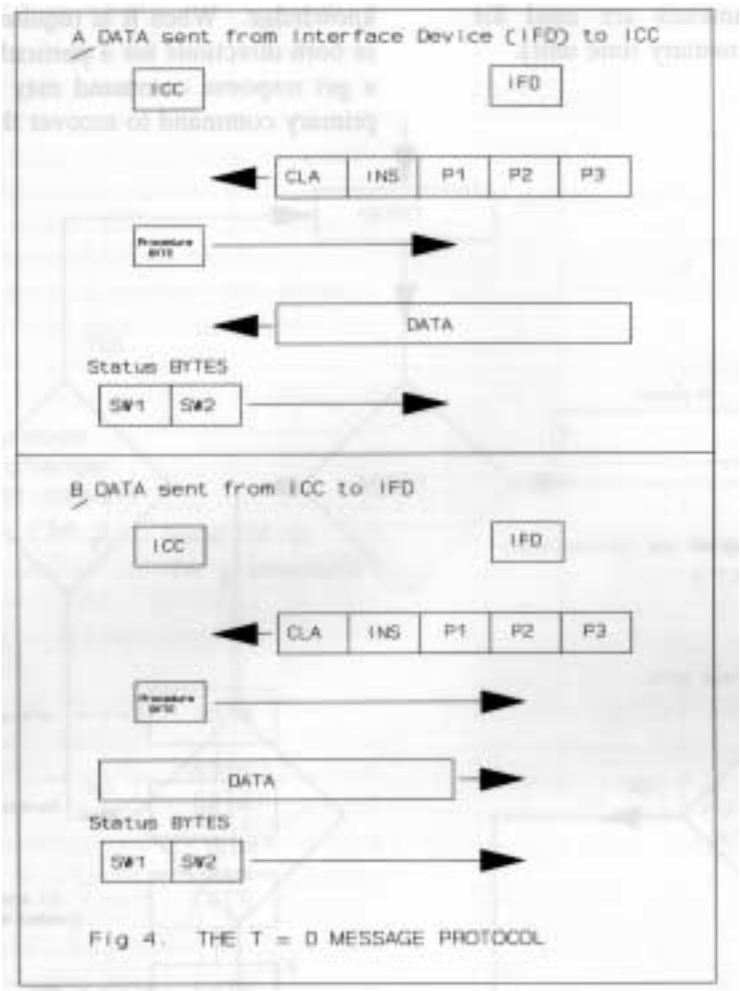

Fig 4. THE T = 0 MESSAGE PROTOCOL

The command message consists of a 5 character header which the interface device sends to the ICC. The ICC then replies with a procedure byte after which either data is sent to the ICC, or from the ICC, depending on the particular command. This procedure byte is to allow the interface device to control the Vpp EPROM programming voltage. In the case of EEPROM memory this procedure byte is effectively redundant. The message flow for the T=0 protocol is shown in fig.4. The command header consists of the following 5 bytes,

CLA- the instruction class (FF is reserved for PTS)
INS- the instruction code (e.g read memory)
P1- instruction code qualifier (e.g memory address)
P2- additional INS code qualifier
P3- the length of the data block

When P3 is equal to zero the data from the card will be 256 bytes. When data is to be transferred into the card then a zero data transfer is implied.

The normal condition for the ACK procedure byte is for this byte to echo the instruction byte (INS). Other options allow the interface devices to control the Vpp programming voltage as required. The card may optionally send a NULL procedure byte (60hex) which allows further time for the processing of the command. In this situation the IFD should await a further procedure byte. The ISO standard also allows the card to send the first status byte (SW1) as the procedure byte.

There are two status bytes SW1 and SW2. These bytes are sent from the ICC to the interface device on completion of the command to indicate the current card status. The normal response is,

SW1, SW2 = 90hex, 00hex

When SW1 = 6X or 9X various error conditions are reported by the card. ISO 7816-3 defines 5 such error conditions,

SW1 = 6E- Card does not support instruction class
= 6D- Invalid INS code
SW1= 6B- Incorrect reference
= 67- incorrect length
= 6F- no particular diagnosis

The T=0 protocol also includes an error detection and correction mechanism. This was described in part 4 and relies on the receiver detecting a parity error upon which it takes the I/O line to the low logic level within the first etu guard time (10.5 + 0.2 etu) for a minimum of 1 etu and a maximum of 2 etu. The transmitter looks for this condition and retransmits the corrupt character.

Next month we shall complete the discussion on communications with the T=1 protocol.

Schiphol Travel Pass

Amsterdam's Schiphol Airport, was the first airport in the world to introduce a Smart Card to allow frequent travellers to pass quickly and automatically through passport control. They were followed by Munich Airport, Germany, which has introduced a high security Smart Card ID system for employees of the various organisations involved in the running of the airport (SCN December 1992).

The system at Schiphol Airport was tested from mid-February to the end of April 1991 with some 200 regular travellers before becoming fully operational at the beginning of 1992.

The scheme is only available to Dutch residents who travel more than five times a year by air, and they are still required to carry a valid passport when travelling.

Called the Schiphol Travel Pass (STP), the system was developed by the Airport, Travel Card Nederland BV, Immigration, and the Ministry of Justice. The Smart Card has the holder's personal data stored on it, a unique number, and his or her fingerprint in digitized form. At the STP checkpoint, the validity of the card and the fingerprint of the traveller are checked automatically.

The fingerprint readers are supplied by ESCOM, and the Smart Cards by Slumberger Technologies, France. To date, over 1,000 cards are in use at the airport.

Passport control initially has one STP checkpoint in the southern section of the terminal, but another is under development for the northern section, and it is planned to add a further two checkpoints in the western section during this year.

The traveller has to pass two checkpoints, one where the validity of the card is checked and one where his or her fingerprint is checked with the fingerprint stored in the chip.

Contact: Nico Scheffer, Amsterdam Airport Schiphol - Tel: Netherlands +31 20 601 9111.