www.smartcard.co.uk

SMART CARD NEWS

March 1993

Volume 2 Number 2

Lufthansa AirPlus Card for Frequent Flyers

The Lufthansa AirPlus Service Card is a multi-function card and the first German credit card with a microchip.

Lufthansa describe it as “Die perfekte Travel Card,” as one card meets virtually all the needs of frequent flyers, business travellers, and companies who regularly send their executives abroad. One measure of its success is that Lufthansa AirPlus Card turnover rose from 400 million DM in 1988 to 1.8 billion DM in 1991 and to over 3 million DM last year.

Continued on page 43.

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 8 - Inter-Industry Commands for Interchange continued.

Food Stamps Smart Card Project.

CONTENTS

Lufthansa AirPlus Card

Continued from page 41.

Lufthansa last year achieved co-branding with the German banks, Deutsche Bank and Dresdner Bank - customers can chose which bank they want to use - and can offer the credit card services of EUROCARD/MasterCard giving cardholders a worldwide payment instrument on a card primarily designed to offer services and privileges to their own customers and promote customer loyalty.

The Lufthansa AirPlus service is the basis for a range of cards - the AirPlus Card, Frequent Traveller Card, Senator Card, and the Company Card - each offering a range of services.

Service features of the first three cards are:

Payment function/price advantages, payment acceptance at over 10 million points worldwide, cash service at 200,000 banks/cash dispensing machines; payment of IATA tickets, ticket purchase by telephone, and price advantages at 4,000 hotels, for car rental (Avis, Europcar, Hertz, Sixt/Budget), and on the Bundesbahn (the German Federal Railway).

Service function

Service functions include participation in the AirPlus frequent flyer programme, priority on waiting lists, access to Lufthansa AirPlus VIP lounges worldwide, and secretarial service in business centres.

Telephone function

The card, supplied by Giesecke & Devrient, is a hybrid card that carries both a chip and a magnetic stripe. The Deutsche Telekom chip is integrated in the card on request, and for a small surcharge, to enable cardholders to make cashless calls from over 35,000 German chip card telephones. Cardholders can also take advantage of the Executive TeleCard service while most credit card telephones worldwide are accessible.

The chip used for the telephone function is the Siemens SLE4402 M2 416 bit chip which has a PIN function.

Lufthansa AirPlus is currently working on adding applications on the chip in the field of travel management and selective personal data, while Siemmens say current chip could be used for loyalty or electronic purse applications.

At present the chip is located on the back of the card because initially problems were encountered in having the chip and embossing together on the front of the card with the chip being damaged in the phone card reader. (It is expected that the PTT chip will be offered by Eurocard Germany as a general card feature later this year and that they will issue about 3 million chip cards by 1996.)

Insurance

Every customer with travel accident insurance protection is covered not only for his or her flight, but for say a rail journey, as a car rental user and on hotel premises, provided the service was paid for by means of Lufthansa AirPlus. Insurance can be extended up to a maximum of 30 days on request and cover additional requirements such as health abroad.

Accounts function

Cardholders receive comprehensive statements of expenditure. For all air travel services the Lufthansa AirPlus invoice is accepted by the German revenue authorities as authentic documentation. They are also given a periodic analysis of their travel activities - flights, rental cars, hotels, restaurants.

Since last year the separation of business and private expenditure can be catered for by a second card, included in the annual fee.

The AirPlus Card is available at three different rates, and the customer can reduce the amount paid by a half or even cut it to zero depending on annual card turnover.

The Company Card is used to handle all a company’s flights via the travel department or its regular travel agent. Company personnel have the benefit of insurance cover while the company receives just one consolidated invoice from Lufthansa AirPlus instead of individual bills.

It took 150 staff two years to develop the product and there are now 70,000 AirPlus Cards in circulation. Lufthansa say that this number will almost triple to 200,000 by the end of this year.

Contact Peter Metzler, Managing Director, Lufthansa AirPlus Servicekarten GmbH, Germany - Tel: +49 6102 204113.

Toll System for France

France is to automate the toll system on its motorway network. An order, commissioned by USAP, the French umbrella organisation of France's eight motorway companies, has awarded a contract to a consortium consisting of Combitech Traffic Systems of Sweden, (part of the Saab-Scania Combitech Group) and the French companies CSEE and GEA.

In the first phase, the consortium will supply electronic toll road equipment and Smart Cards for payment at two prototype toll plazas yet to be announced. Full-scale installation work will start in 1995.

The system is a development of Combitech's Premid microwave system in which the driver inserts a Smart Card into a microwave transponder fitted on the inside of the windscreen. Special roadside equipment reads the card and debits the appropriate toll fee from the value stored on the card enabling the driver to pass through without stopping.

Ivan Rylander, General Manager of Combitech Traffic Systems, described the order as strategically important for the company in view of the major toll road systems that are going to be introduced in Europe.

Combitech has three reference sites in France and has supplied toll road systems for the UK (The Mersey Tunnel and the Dartford River Crossing) and Norway using electronic tags. It has also supplied automatic, unmanned toll road equipment for Sweden's first toll financed road, at the road bridge outside Ostersund, to be inaugurated this summer.

Contact: Kenneth Blomqvist, Project Manager, Combitech Traffic Systems, Sweden -Tel: +46 36 194040. Fax: +46 36 175960.

PrismIC Technology

Schlumberger has developed a new manufacturing process for Smart Cards which they say enhances its reliability and visual quality.

Currently, the print and visual effects are applied directly onto the body of the card. On PVC, print quality is restricted to a resolution of 133 dots per square inch.

In the Schlumberger process, the normal use of PVC or ABS has been replaced by polycarbonate and the visuals are printed on paper where a resolution of 185 dots per square inch can be achieved and then blended with the polycarbonate, resulting in a transparent card with high visual quality.

The card's graphics are printed by an offset press on two-sided labels which are then cut to the exact size of the card. When printed the cards are lacquered on the back. The labels are transferred to a mould where the polycarbonate is poured in its liquid state under high pressure.

The piston which compresses the polycarbonate also stamps out the cavity for the integrated circuit module. The operation takes no more than a second for each label.

The strips on which the modules are placed are now of bronze instead of epoxy resin and the modules are mounted on polycarbonate for improved insertion in the mould.

Scented inks

The new process offers interesting design and printing opportunities in the marketing field. For example, offset printing applied to magazine quality paper provides high resolution graphics and a full range of visual effects including perspective, mirroring and overprinting.

Clients can request printing inks with specific characteristics, for example, scented inks containing scent-filled microfibres mixed with colorants which could be attractive to perfume and after- shave manufacturers wishing to promote their products.

Other options are to include a real leaf embedded in a card or a swatch of lace and fabrics to promote a fashion show, as well as simulating velvet, wood, stone or marble etc.

Contact: Marc Schinder, Communication Department, Schlumberger Technologies - Tel: France +33 1 47 46 70 89.

SmartFuel System for Trucks

Trendar Corporation and AT&T in the United States, have teamed up to provide a SmartFuel System for truck stops based on AT&T's contactless Smart Cards and designed to move trucks more efficiently through fuelling islands and cut costly billing errors.

The SmartFuel System, located at the fuel pump, can accept AT&T contactless Smart Cards or standard magnetic stripe cards. Drivers using magnetic stripe cards will be asked for data such as their driver number and truck number, but for Smart Card holders this information will be stored on the cards and read by the system. The driver only has to verify the date and the sale is then instantly authorised.

When fuelling is complete, the system automatically dials out for payment authorization and by the time the driver gets to the fuel desk, a ticket is printed and ready for signature.

In addition to speeding the fuelling process, the system instantaneously sends information about the transaction to the fleet operator.

The 3K byte EEPROM card will store such information as the truck number, purchase authorisation limits, the driver's licence number, name of the fleet operator, and any discount to which trucks in that fleet are entitled.

Ernest Betancourt, Chairman of Trendar, says: "A truck stop fuel desk has to accommodate up to 60 different payment methods, and varying prices depending upon which of the nation's 77,000 fleets are involved. As a result there is a large margin for error in each transaction. A cashier can easily charge the wrong fuel price, record the billing information incorrectly, or give cash discounts on credit purchases."

According to Tom Cerwinski, AT&T Smart Cards Market Manager, "This is just the beginning of how Smart Cards can serve this industry. Today, most toll booths, weigh stations and ports of entry require trucks to stop, with costs ticking away at a dollar per minute. Equipped with Smart cards, commercial vehicles could be located, classified, weighed and identified for taxation and other purposes, while in motion.

"In addition to speeding the trip this reduces the need to have drivers carry cash, it can provide accurate records of trip expenses, and it could allow the owners to track or locate their vehicles. The same Smart card could be used to record engine information, vehicle weight, manifest and state permits, and to pay for repairs and taxes."

A prototype of the SmartFuel System was demonstrated at a meeting of the National Association of Truck Stop Operators in Orlando, Florida, last month, and the first systems will be installed in Virginia during the second quarter of this year.

Card Details

Type: Contactless

Fabricator	AT&T
Dimensions	ISO ID1
Chip type	Microcontroller + logic
Memory type	EEPROM
Memory capacity	3K bytes
Standards	ISO 7816-3
Comms protocol	T=O and T=1
Security	PIN
Cryptography	DES

Contact: Michael Jacobs, AT&T - Tel: USA +1 908 582 4767. Nancy Rutherford, Trendar Corp. - Tel: USA +1 615 367 1000.

TIMEZONE On Hold

TIMEZONE, the road traffic pricing scheme being developed by Easams, England (SCN December 1992) has been put on hold until the British Government completes its investigation into the feasibility of charging drivers in congested areas. The Smart Card based scheme was scheduled to be piloted in Richmond, Surrey, in mid-1993.

German Multi-function Card

A German Smart Card initiative involving GAD (Company for Automated Dataprocessing), IBM and Deutsche Telekom is developing a multi-function chip card which they say will provide more functions and support more applications than other chip cards.

GAD is owned by, and the supplier of dataprocessing facilities and services to, the co-operative banks in Westphalia, and the co-operation partners are planning to launch the new card over a wide area and say that in the long term it will replace magnetic stripe cards.

The card will enable users to make electronic funds transfers, cashless payments and telephone calls as well as other telecommunication tasks.

Applications within business areas such as trade, banking, and telecommunications, can be created individually and put on the card, and the partners consider this capability as the key in providing improved secure services and in limiting the range of card types.

Field study

In a field study to be started in August in Munster, 150 kilometres west of Hannover, it is intended to issue 2,000 Eurocheque (EC) cards with a chip in addition to the magnetic stripe. This will allow cardholders to use any function that is currently supported by the magnetic strip, but also additional functions supported by the chip, for example, to use Telekom card phones, to access German Btx to perform on-line banking, or to make other inquiries. Additional applications such as cashless payment for public transport services are under investigation.

Cashless payment will be supported by a special “electronic purse” function. Cardholders will load a “credit amount” electronically onto the chip without their account being debited. Only when the card is used for cashless payment will the account be debited with the amount withdrawn from the “credit amount” on the card.

All cashless payment will require the cardholder to enter a PIN at the point of sale and, as a further security measure all transactions will be secured with an authentication code. The PIN also protects the cardholder against unauthorised use if the card is lost.

Not only will cardholders be able to use Telekom card phones to make calls, but they will also be able to see how much the call has cost by pushing a button which will display the amount debited.

Deutsche Telekom is planning to install card phones throughout Germany, and the conversion of current card phones to support the new card functions has started in the area of the field study and will be completed by the end of this year.

Allocation of tasks

The co-operation between the three companies is based on the appropriate allocation of tasks and responsibilities. GAD will provide the software required by the banking branches in order to issue the cards. IBM will convert its self-service machines, such as ATMs and transaction stations, for use with the new card. German Telekom will enable its communications technology, such as card phones, Btx/Datex-J, and O-Fax, to support the card. Telekom will also provide widespread end-user devices to be used with the card.

The group have agreed to promote the card within the finance industry, but outside of this area they are free to push the card. IBM, for example, will promote it as the IBM multi-function card outside the German finance industry.

Card details:

Type	Contact
Fabricator	To be announced
Dimensions	ISO ID1
Contact location	Front
Chip manufacturer	Hitachi
Chip type	H8/3101
Memory type	EEPROM
Memory capacity	
EEPROM	8K bytes
ROM	10K bytes
Standards	ISO 7816-3
Comms protocol	T=1 and T=14
Security	PIN
Cryptography	DES

The communication protocols used will depend on the application - T=14 for Deutsche Telekom and T=1 for point of sale.

Contact: Julian Brewer, Market Opportunity Manager for Security and Smart Card Solutions, IBM UK, London - Tel: +44 (0)71 633 9633.

Case for Contactless Cards

Why did Greater Manchester Public Transport Executive and London Transport chose contactless Smart Cards for what are potentially the biggest pre-paid ticketing projects for public transport in Britain?

At the recent Smart Card 93 Conference in London. Mike Hill, Marketing Manager for GMPTE, who are expected to issue over one million cards to bus and train users for the transport application of the multifunctional card alone, said the decision had been taken after a two-year evaluation of available technologies, including an evaluation of contactless technology by the Manchester-based National Computing Centre (NCC). Their conclusion was that contactless technology was proven and offered the best solution for a public transport application.

“Contactless technology,” he said, “offers four important features over contact technology (magnetic stripe or chip cards) that make it ideal for use on public transport: reliability, security, speed and ease of use.”

Reliability

The on-bus environment was “harsh” and any equipment with moving parts would consequently be less reliable than one without. contactless readers had no moving parts whereas all contact readers did and also needed some sort of aperture in which a card was inserted and read. An aperture on an unstaffed railway station was likely to attract vandals, Additionally, all contact cards were susceptible to abrasion on the magnet stripe or gold contact which resulted in card failure. With a contactless card the input/output device was embedded in the card and therefore could not be abraded.

Security

Security was a major issue for all prepayment systems and most commentators on the subject would confirm that Smart Card technology, be it contact or contactless, was the most secure method available.

Speed

Boarding times were an important issue for both bus operators and the travelling public. The speed of an on-bus transaction was a function of the card reader’s processing capability, and the ease by which a passenger could conduct a transaction. While all technologies could process cards fast, with a contactless system the card did not have to be taken out of a purse or wallet, and did not have to be inserted into the reader. This minimised passengers fumbling and was therefore much easier to use. This was especially important for young children, the aged, mobility impaired people with limited dexterity, or passengers who wore glasses etc.

User friendly

A contactless card could be read by simply touching it on the target area of the readers, and because the card did not have to be removed from a customer’s purse or wallet, it had particular advantages for people who were encumbered or who had limited manual dexterity.

London Transport

Roger Torode, Project Leader for the London Transport trial said that contactless Smart Cards offered “significant advantages” over alternative methods.

They involved no moving parts, were less susceptible to fraud, offered greater security against accidental or deliberate corruption, gave faster boarding speeds, and were more attractive to passengers as the card was retained by them at all times and did not have to be released into a card reader.

Contacts: Mike Hill, GMPTE - Tel: +44 (0)61 228 6400. Roger Torode, London Transport - Tel: +44 (0)71 222 5600.

GSM A5X Algorithm

Problems in allowing some countries to use the A5 encryption algorithm for GSM, the Global System for Mobile Communications, are being tackled by the development of an alternative version of the algorithm, known at the moment as A5X.

While no government export licenses have been reported to have been refused, the expansion of GSM into a truly mobile global system depends on international standards. The requirement for an alternative algorithm adds another difficulty for GSM operators, but Britain's Department of Trade and Industry say that the A5X algorithm will still be a secure algorithm and that the adaption of GSM mobile equipment will be required to automatically select either algorithm under the control of the operating network.

The development work is being carried out at British Telecommunications's Martlesham Heath Research and Development Laboratory in England. However, BT point out that while they are doing some of the work they are not responsible for developing the A5X algorithm but are overseeing the work on behalf of SEPT countries. It is expected that the new version will be approved in time for the introduction of GSM Phase Two in 1994.

GSM Phase Two

At IBC's Pan-European Digital Cellular Radio Conference in Lisbon, Portugal, last month, Kari Marttinen, Telecom Finland, said that upgrading GSM from Phase One to Phase Two would involve improvement of almost every single part of the system, including the SIM (Subscriber Identity Module) Smart Card.

The second phase would offer all of the originally planned features and would therefore be highly competitive, even superior, to any existing mobile communication system in the world.

Jonas Twingler, of the European Telecommunications Standards Institute (ETSI), said that a basic requirement emerging from this phased approach was full compatibility between phases, ie that a Phase One terminal should be able to operate in a Phase Two infrastructure environment and vice versa. This obvious, but not so innocent, requirement had caused significant difficulties for the organisations involved in the development of the standard, mainly because the Phase One specifications were "closed somewhat in a hurry" in order to meet the market demand of an already delayed system, and not all precautions to ensure upward compatibility were taken.

In the development of the Phase Two standard, a significant amount of time and resources had been, and would be, spent on sophisticated solutions to overcome inherent problems and ensuring backward compatibility.

It was intended that the Phase Two standard would be finalised by mid-1993, followed by public enquiry and voting by the National Standards Organisations, and should be ready for final release by early 1994. It would offer a considerable range of services and features and a significant increase of an already high traffic capacity.

Looking ahead, he said there was great interest to expand GSM beyond its current boundaries, and among topics which were currently being considered were pre-paid SIM cards with associated security mechanisms.

Far East progress

Chris Jenvey, Hongkong Telecom CSL, said that in the Far East region Australia should have three GSM networks this year, Thailand was expected to introduce GSM this year, and Malaysia was also pressing ahead. Singapore Telecom was scheduled to launch its GSM network later this year. The telecom market was opening up dramatically in India, while China already had trial networks in operation.

Research had revealed some interesting cultural differences such as the perceived disadvantages which the SIM card could have for some Hong Kong clients. For example, he said: "If you are lending someone else your GSM terminal, it would be considered impolite or "un-Chinese" to remove your SIM card from the phone first of all!"

Gemeasy Teletoll System

The Prado-Carenage Tunnel in the Mediterranean port of Marseille in Southern France will be equipped with the latest Smart Card-based Teletoll system designed to handle up to 1,200 vehicles per hour when it opens this Autumn.

Constructed beneath the city, the tunnel will make travelling between major districts in the city easier and connect to major highways leading to and from the city - the west highway from the coast to Montpellier, the northern highway to Aix en Provence, and the eastern highway to Aubagen and Toulon.

It is the first large privately-funded highway infrastructure in the community and will be funded by tolls paid by users. As a result, last month the Societe Marseillaise du Tunnel Prado-Carenage (SMTPC) announced its new Gemeasy remote toll payment (teletoll) system to be used within the city.

System components consist of vehicle onboard equipment comprising an ISO standard format Smart Card and a card-holder, smaller than a cigarette packet, that is used to transmit card information to the remote payment system, ground reception equipment comprising a long-range antenna which captures signals sent by the card-holder and an electronic coupler which receives and interprets signals and communicates with the computerised control and management system.

In the subscriber management centre, Gemplus GPS120 machines will be used to personalise user cards graphically (last and first names and identification number) and electrically (to program the chip) using a personal computer.

System operation

As the driver approaches the toll station, information stored on the Smart Card which is inserted in the onboard card-holder fitted to the windscreen of the vehicle, transmits information by radio signal and the barrier opens immediately without the car having to stop.

Advantages for the driver are that he or she does not have to fumble for change, lower the car window and stop the vehicle.

The same Smart Card may be used without the card-holder for other applications, creating a possible link between a subscription for the tunnel and other regional transport services such as access to parking areas, bus or subway fare payment, or perhaps for municipal services such as entrance to stadiums and other facilities.

Companies involved

Companies involved are CSEE PEAGE, who drew up the specifications for the Gemeasy toll payment application, and for the toll payment channel logic; ERO, who supplied the barriers and associated equipment; SPIE-TRINDEL, who installed the overall system: and Gemplus, who provided the remote communication systems with onboard Smart Card in the vehicles.

Card details:

Type	GPM416 and GPM896
Fabricator	Gemplus
Dimensions	ISO ID1
Chip manufacturer	Designed by Gemplus
Chip type	Memory
Memory type	EEPROM
Memory capacity	416 or 896 bits
Security	PIN

Gemplus says the Gemeasy system is the first of its type in the world that uses a standard Smart Card, such as used for pay phones or automatic teller machines.

The companies who developed the system for SMTPC are planning to promote the system in France and abroad and to have it standardised on an international level.

Contacts: Mr Saxby, SMTPC, France - Tel: +33 91 78 01 00. Jean-Pierre Gloton, Gemplus, France - Tel: +33 42 32 50 31.

Smart Cards in The Netherlands

Dutch companies and Government ministries are investing heavily in chip card projects, and over the last four years almost fifty trial projects have been started in various sectors representing a total turnover of almost 75 million guilders. As a result of this rapid growth, few people have a clear view of the market any more.

Now, four Government Ministries, which are subsidising chip card projects, are planning to form a chip card platform.

The average Dutch person has never even heard of a chip card, let alone a Smart Card. Every popular card in the country is equipped with a magnetic strip.

Despite the number of Smart Card projects, the participants remain silent regarding the results: some in fear of the project's failure, others to conceal their successes from competitors. This silence makes the Dutch chip card market obscure, but two particular projects attracted a great deal of attention.

Woerden

One was the oldest large Dutch Smart Card trial which ran from 1989 until 1992 in the small town of Woerden. The Woerden card was a payment card enabling the inhabitants to use it at innumerable large and small retailers. Some 20,000 cards containing the Schlumberger M64 chip module were made (designed and produced) by the Dutch firm of Sdu.

Important parties to the contract were:
- the banks, who absorb 60% of the costs.
- the Ministry of Economic Affairs (20%).
- the Retail trade council (20%).

The Smart Card technology proved successful as all the hardware and software functioned perfectly. However, in the end, the banks decided to give preference to their originally established Beanet network for magnetic strip cards.

Schiphol Travel Pass

The other project, the Schiphol Travel Pass (STP), allows regular users of Amsterdam Schiphol Airport, to enter Holland without having to show their passports. Instead they insert the STP card into a reader, and then their identity is confirmed by reading their fingerprint which is compared with the template stored on the card.

The STP is designed and produced by Sdu, the privatized State printers who also produce amongst other things the Dutch passport. Twenty-five thousand STP cards, with a Schlumberger M64 chip, have been issued.

The success of the STP project was viewed in Holland as a miracle. After all the subject of boundary transgression is surrounded by the many rules of powerful organisations. Thus the partial replacement of the passport was not thought of and implemented in a day.

There is space on the card for other functions, but the only one currently used is for parking in the 150 places reserved for STP holders.

Supermarket

Ahold, the largest supermarket chain in the country, is experimenting in one of its branches with a card for regular customers. Working on the project is ComputerCentrum Van de Velde, whilst

the card comes from Sdu and contains a Bull CP8 TB100 chip module. Marketing managers from every large retailer would like to know what Ahold's findings are, but the giant remains silent.

Other projects

The Dutch railways (NS) have completed trials with a contact free card developed by Nedap and are now preparing a larger trial. It is undoubtedly the intention to make the railway card suitable for all other forms of public transport, but nobody will announce this officially.

The university and the academic hospital in Limburg have a joint chip card in use for certain simple applications such as paying in the canteen. Thus there are many organisations who are using Smart Cards internally. Their projects are themselves clear: in principle the card fulfils only a few functions, in a few locations, for a single group - an organisation's regular clients. Such singularity often increases a project's chances of success.

Government

The government has always played an important role in this field. The Ministries of Economic Affairs (EZ), Health & Culture (WVC), internal Affairs (BiZa) and Transport and Communications (V&W) are convinced that the country will be well served if all manner of telematics are quickly developed, and the government has co-financed more than ten projects. Using subsidies the government wishes to function as a starter motor. After start-up the projects must function independently as quickly as possible.

Currently the government views the development of the many chip card projects with mixed feelings. On the one hand there is enthusiasm over the progress, on the other hand there is concern that - with a few exceptions - the project participants know little of what each is doing, which technological standards are being applied and how they are treating the question of privacy.

Platforms

The Government, particularly the Ministry of Economic Affairs, is seeking:

* a clear picture of the chip market, and
* the promotion of co-operation between projects.

To achieve these goals, the Ministries devised a plan for a chip card platform. At the end of 1992, this plan was sent to 175 organisations with the request to give their comments and to become members. It is hoped to organise the first meeting this Spring and form the second chip card platform in Holland.

Last year the Dutch welfare sector formed its own Smart Card platform called National CareCard. Members involve insurance companies, the Ministry of Health and the chip card industry.

Three trial projects are operating, in Breda, Groningen and Delft. The last is the largest and is supported by welfare insurer DSW with 30,000 cards from Sdu, equipped with a Gemplus NCOS 24K chip module. Provisionally this card will contain only a limited medical dossier in order to avoid possible problems concerning privacy (a sensitive point in Holland).

A representative from the Ministry of Health said at a National CareCard seminar that his subsidy tap had virtually run dry: "In the short term we are sceptical, but a National CareCard will come, of that we are certain!"

Jurjen de Jong

Contact: Drs P M Jongert, Sdu Chipcard Technology, The Netherlands - Tel: +31 70 378 9202.

Card Watch Campaign

As Card Watch, the £500 million UK campaign against plastic card fraud enters its second year, the major banks and building societies have said "not yet" to using Smart Card technology to combat crime.

Richard Allen, Chief Executive of APACS, the Association for Payment Clearing Services, told a press conference early this month that the Smart Card was seen as "another longer term contender" as a Card Authentication Method.

The industry was currently working on a number of technological solutions - some further down the line than others and some more practical to implement, but he stressed that they were still in the research and development phase.

It was anticipated that the most powerful long-term barrier to plastic card fraud would come as a result of a combination of Cardholder Verification Methods (CVMs) and Card Authentication Methods (CAMs).

As an industry they were currently investigating CVMs such as PINs at point of sale, photocards and biometric techniques such as finger scanning, voice recognition and digitised signature recognition.

Regarding Card Authentication Methods, details of individual methods under evaluation were highly confidential, he said. Some related to the magnetic stripe which appeared on most plastic cards today, and the Smart Card or integrated circuit card was another longer term contender.

At the launch of the 1993 campaign, the banks and building societies announced that the rise in plastic card fraud had been contained in 1992, with losses totalling £165 million. This figure was down £600,000 in a year when card fraud had risen by 35 per cent.

More than 5,000 cards went missing in the UK every day last year with losses amounting to £5 a second.

Plans by Card Watch in 1993 include a £2 million national advertising campaign, rewards for retail staff who prevent frauds (last year, over 100,000 shop staff received over £7 million in reward money), and research into patterns of plastic card crime.

Smart Ski Card in Austria

A contactless and batteryless Smart Card from Tactel, a subsidiary of Tadiran Ltd., Israel's largest electronic group, is providing quick access control to skilifts at three Austrian winter resorts.

Smart Cards have replaced barcode or magstripe technologies which proved unsuitable in the outdoor environment, required additional manpower on the part of the skilift operator, and were inconvenient for the skier who, in addition to having to carry ski equipment had to insert the magstripe or barcode ticket into readers.

The new Smart ski ticket was designed so that it could be fitted on the sleeve of the skier's jacket so the skier only has to put his or her arm near the reader for it to be read. The card is then updated and access either granted or denied.

Ten thousand cards

Ten thousand 128 byte contactless read/write Smart Cards have been issued in the resorts which include Bad Kleinkirchheim, one of the largest in Austria.

Skiers are issued with the cards in exchange for a deposit refundable when they return the card. They are able to purchase either multi-day or limited access passes and the cards are programmed to be debited differently based on the type of service provided such as regular skilift or cable car. This capability was not feasible using the other methods.

Benefits for the operators are that they require less manpower to control access and less maintenance on the card readers. The skiers benefit from have fast and convenient access to the slopes.

Tactel worked through their Austrian subsidiary ELIS GmbH and with SYSTEMS an Austrian company specialising in ski ticketing systems.

Card Details

Type	Contactless batteryless
Fabricator	Tactel
Dimensions	Special non-uniform design - thickness 2.7mm to 4.7mm
Read/write distance	Typical 12cms
Memory type	EEPROM
Memory capacity:	
Program	1.5K bytes (out of 2K bytes capacity)
EEPROM	128 or 256 bytes
RAM	128 bytes
Security	Company proprietary

Contact: Shmuel Barkan, Managing Director, ELIS GmbH, Austria - Tel: + 43 222 891 003525. Fax: + 43 222 894 2243

Hungary Defies Setback

Despite the failure of its most ambitious Smart Card project last year, Hungary is continuing to develop Smart Card applications in a variety of fields such as in access control, loyalty schemes, health and transportation.

The Research Institute of the Hungarian Post and Telecommunication started a Smart Card cashless payment system trial as part of a new experimental computer network in the medium-sized town of Eger. It was introduced as a new service of the Postbank.

Five terminals were equipped with card-handling terminals from Bull CP8 connected to the counter desk computer and used for obtaining cash and pay for postal services. The transactions were recorded separately, summed and sent daily to the centre via network.

A special workstation was assigned for card maintenance. Here the PIN code and payment limit could be changed and the card unblocked.

An ATM was installed at a post office and another at the bus station. programmed to dispense 100 Ft and 1,000 Ft banknotes according to the card limits. They communicated with the network via a front-end processor, but were also prepared for off-line working. Identifying and payment limits were calculated in the ATMs, according to the Smart Card demands.

Eleven Point of Sale terminals from Dassault Electronique were installed in places like petrol station shops and stores. They were connected to the data capture centre via telephone link and once a day downloaded the transaction data and received black list updates. The Smart Card used was the Bull CP8 M9 8K byte EEPROM card.

The experiment was started in November 1988 with the development of the network and the payment system. Testing started in October 1991 and lasted until March 1992. About 100 Smart Cards were issued to clerks of Postbank and Post Offices in Eger and the average number of transactions per card was about 7-8 per month.

Unfortunately the operators experienced problems with the equipment and found the operation cost of the card too expensive and came to the conclusion that the Smart Card system was not economical either for the bank or the customer. At the same time the banks in Hungary decided to introduce a unified bank card system based on the magnetic stripe card.

Tibor Ronai, Director of UNICARD Association Hungary, says they would like to retry the Smart Card banking trial in Eger, possibly with another bank, other hardware and software tools and with more co-operation with suppliers.

Meanwhile, he says, a number of Smart Card projects are being tested or are at the planning stage in Hungary. There are six institutions, for example, the National Security Office, the Central Physical Research Institute and bank branches, where Smart Card based access control systems have been installed, while similar schemes are in progress at the Prime Minister’s Office and at the National Technical Development Committee.

This year a pilot project starts in the health application area with 500 Smart Cards. Other projects in preparation include a car service card, a club card, a loyalty card, and a transportation card.

Contact: Tibor Ronai, Director UNICARD Association, Budapest, Hungary - Tel: +36 1 180 4242.

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.

Special Conference Card

The colourful 10 ECU card featuring European flags (see page 1) given to the 320 conference delegates at Smart Card '93 in London could be used with Smart Card telephones on the Orga and Siemens stands at the exhibition.

On the back of the card are the logos of the companies who were involved with the card - Orga, who fabricated the card; UNIQA, Orga's parent company in Germany; Siemens, who supplied the chip; GPT who provided the telephones and BT who provided the telephone lines.

Only 1,000 of the cards were printed so they are likely to become collectors' items.

SEMPAC Represented in China

SEMPAC (Semiconductor Packaging) SA is to distribute its Smart Card lines and ESEC semiconductor assembly products through Barco Ltd., a Swiss and Chinese joint venture that represents European products in China.

A subsidiary of the ESEC Group based in Cham, Switzerland, SEMPAC is the first company in the semiconductor assembly industry to compile and co-ordinate complete chip assembly lines for Smart Cards. It will now be able to offer its products and local service in China, as well as through its service and sales subsidiaries in Phoenix, Arizona; and Singapore.

Smart Card Tutorial -Part 7

Inter - Industry Commands for Interchange.

So far in the tutorial we have discussed the scope of the ISO Standard 7816 parts 1,2 and 3. As we have mentioned previously any concept of interoperability requires adherence to these basic standards for the physical and electronic properties of the IC card. Whilst we encountered problems, due largely to the need to maintain conformance with early comercial implementations of the IC card system, there is none the less an overwhelming industry acceptance of these standards. We are now going to have a look at the scope of the ISO 7816-4 draft standard which is still subject to significant disagreement.

For the purpose of the tutorial we will skate around the contentious areas and concentrate on the basic principle which is really the definition of a file management system and its interaction with a user. The following discussion will examine the four basic concepts of the ISO standard,

- File structure
- Message structure
- Basic commands
- Command and data transport.

File structure

There are three categories of files,

- Master file (MF)
- Dedicated file (DF)
- Elementary file (EF)

The Master file is a mandatory file for conformance with the standard and represents the root of the file structure. It contains the file control information and allocable memory. Depending on the particular implementation it may have dedicated files and /or elementary files as descendants (See fig 1).

A dedicated file has similar properties to the master file and may also have other dedicated files and/or elementary files as descendants.

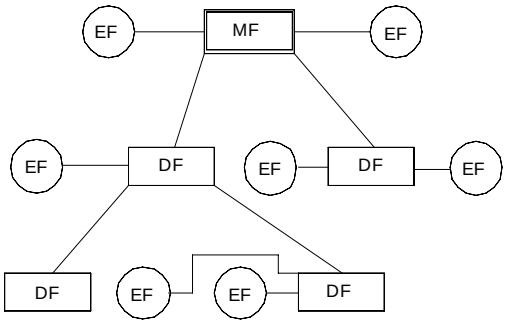

Fig. 1. Logical File Organization

An elementary file is the bottom of any chain from the root MF file and may contain data as well as file control information. An elementary file has no descendants. A number of elementary file types are defined as follows,

- Working file
- Public file
- Application control file
- Internal secret file

The working file is for storing application data whilst the public file allows data to be accessed unconditionally. The application control file always allows read access whilst the internal secret file contains data not accessible outside of the IC.

Each file is referenced by a two byte identifier which allows the path to any file to be defined from the root directory. This path concept is the same principle as used in the PC by MSDOS. Dedicated files may also be referenced by file name.

The data structure for an elementary file allows four options,

- Linear fixed
- Linear variable
- Cyclic
- Transparent

These four structures are shown symbolically in fig 2. The first three options are based on the use of records as encountered in any computer system. The transparent option just refers to a

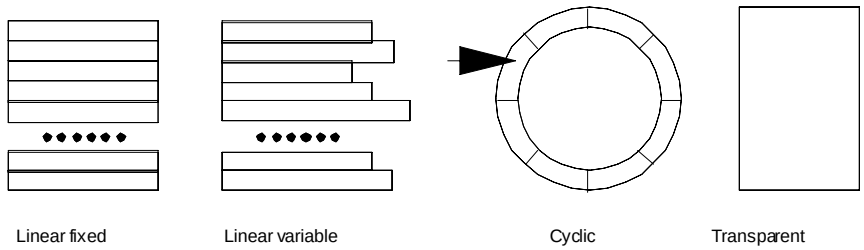

Fig. 2. Elementary File Structures

block of data without the record structure. In this case the data must be accessed by a relative address to the start of the data block. The first three structures would normally access data by reading and writing records. Where the file management system takes care of the absolute address of the data.

This concept of a file structure really only permits the concept of reading and writing data into elementary files. The dedicated file concept allows a partition between data structures where a particular application may select a particular structure. This dedicated file may be used to control access to the data in the daughter elementary files by the use of password verification. In this sense the file structure supports the segregation of multi application data where the separate applications exist at the interface device.

This is really an incomplete picture which may support the historical use of IC cards as data carriers but does not define the principle of multi applications co-existing in the IC itself. What is really required is the concept of executing application programs in the IC and maintaining adequate security segregation between these applications. We shall return to this subject when we discuss the security of the IC card and we will show how this file structure concept may be extended in order to allow active multi - application operation.

The ISO 7816 - 4 proposed standard makes considerable use of the ASN.1 (Abstract Syntax Notation One) syntax rules for the encoding of data. These rules use the principle of TLV (Tag, Length, Value) encoding of the data field. The tag identifies this field, the Length parameter gives the size of the data (in bytes) whilst the value represents the field data. This concept allows variable length fields which may be individually identified. This is an alternative approach to a bit mapped structure where the fields and length are predefined and a single bit in a tag field is used to indicate the presence or otherwise of the field. A bit mapped approach was used in the ATR (Answer To Reset) data to indicate the presence or otherwise of the specific interface characters (see part 4 of the tutorial).

The ASN.1 encoding has a two byte overhead for each data field compared with the one bit of the bit mapped approach. Each encoding scheme has its benefits but it is clear that when data space is at a premium then the bit mapped approach is better whilst the ASN.1 encoding offers more general flexibility. Some concerns have been raised in that the use of ASN.1 may be subject to patent royalties.

The file control information referred to earlier for the MF and DF files is proposed to consist of two parts,

-The file control parameters (FCP)
-The file management data (FMD)

The file control parameters are defined as an ASN.1 encoded data field that describes the necessary parameters such as file size, file identifier and optionally the file name. It also defines the type of file (i.e MF, DF, or EF) and the data structure (i.e Linear fixed, linear variable, cyclic or transparent). The proposed coding tables are given in the standard.

The file management data is also constructed as an ASN.1 object and may contain Inter - Industry or provider specific objects. It may be used for example to store security data for encipherment or password checking.

Message Structure

This part of the standard builds on the command response structure described in part 3 of the standard by defining the concept of an application protocol data unit (APDU). This APDU contains the command or response message and allows for all options of data transfer, as shown in table 1.

The result is an APDU which can define the length of data to be transmitted in each direction. The structure of the APDU is shown in fig 3.

The fields in the APDU are an extension of those described earlier as shown in table 2. for a command APDU.

It should be noted that this allows a number of options. The data length field may be either 1 byte (the default) or up to three bytes. This extended operation is identified by an optional field contained within the historical bytes of the ATR. Depending on the command/response data type shown in table 1. the Lc and Le field may or may not be present, for the cases 1 and 3 there is no command data. The APDU only contains those fields that are used as shown in fig 4.

The response APDU contains the response data field (if present) and the status bytes referred to in part 4 of the tutorial as shown in fig 5. These status bytes have a normal response code of 9000 hex. A number of error conditions have been identified and are described in the proposed standard.

CASE	COMMAND	RESPONSE
1	NO DATA	NO DATA
2	DATA	NO DATA
3	NO DATA	DATA
4	DATA	DATA

Table 1. Command/Response Data Option

Code	Name	Length	Description
CLA	Class	1	Class of Instruction
INS	Instruction	1	Instruction code
P1	Parameter 1	1	Instruction parameter 1
P2	Parameter 2	1	Instruction parameter 2
Lc field	Length of Command Data	variable ≤3	Number of bytes present in the data field
Data field	Data	variable =Lc	String of data bytes sent in the command
Le field	Length of Response Data	variable ≤3	Maximum number of data bytes expected in response

Table 2. Fields in the application protocol data unit

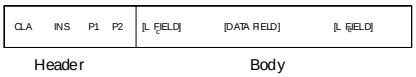

Fig. 3. Command APDU

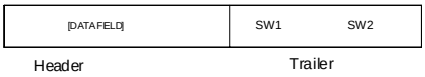

Fig. 5. Response APDU Structure

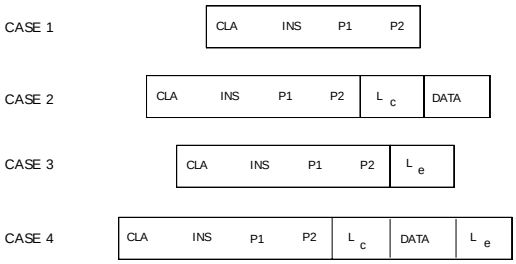

Fig. 4. APDU Structures for different Data Cases (table 1)

Next month we will continue our analysis of the proposed Inter-Industry commands

David Everett

Czech Patient Card

The first Patient Card project in Czechoslovakia is now being implemented with some 3,000 Smart Cards issued in three medical areas - the treatment of diabetics, high risk patients and traumatology.

Developed jointly by Orga and IMA the system uses a Smart Card as a portable file for documentation.

The diabetic card was developed in partnership with a hospital in Ostrau with the object of improving documentation of therapies, thus using medicines more efficiently.

The card for “high risk” patients is being tested by workers who are subject to high environmental stress and pollution. The intention is to document the exposure and to initiate preventive measures. Clinical and laboratory data are transferred by means of the card and can be updated if the worker changes his job.

A third card is used in the treatment of traumatic injuries in the knee area. Post-operative measures are documented and forwarded to rehabilitation clinics by means of the card.

Card details:

Type	Contact
Fabricator	Orga
Dimensions	ISO ID1
Contact location	Front
Chip manufacturer	Not disclosed
Chip type	Microcontroller+Memory
Memory type	EEPROM
Memory capacity	2K byte EEPROM
Standards	ISO 7816-3
Comms protoco	lT=14
Security	PIN

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

Pre-paid Card in South Africa

First National Bank of South Africa in a joint venture with the Foundation for African Business and Consumer Services, have issued a pre-paid card with two functions - to pay taxis fares or to buy goods in shops.

About 105 taxis in Bloemfonntein have been fitted with mobile card readers. The taxi purse is not PIN protected and can be loaded with a maximum of 100 rands (about £20). The retail purse is PIN protected and can be loaded with a maximum of 1,000 rands.

NTT DATA Cards

NTT DATA, of Japan, have developed a number of applications for their S-Type range of Smart Cards with the best known one being the Nissan Car Life System card. But other applications include point of sale, club membership, a university campus card, health and intelligent buildings.

The health/medical information system in Goshiki-cho became fully operational in April 1990 and involves a hospital and ambulances. About 4,700 cards have been issued to the elderly, infants and pregnant women.

The card contains general personal information, emergency information, a history of medical examinations and diagnosis record and treatment data. Security mechanisms in the card protect the patient's privacy, for example the office clerk using a Smart Card can only access general personal information.

Ambulances and emergency rescue teams carry a palmtop terminal which enables them to read general personal information and obtain emergency information from the Smart Card.

The card can also be used to hold a child health record, including details of birth, growth, weight and height reviews and immunisation details.

NTT DATA's Smart Card system for intelligent buildings can be used to perform many different functions throughout the building.

At the Fuchu J-Tower Building, a Smart Card is used to control 41 entry and exit gates with card operated gates on each floor as well as to underground parking facilities and computer rooms.

In addition it can be used as a pre-paid card at shops, restaurants, cafe's and vending machines within the building. Staff who want to put value on their card can do so at two paying-in machines or at five ATMs of the bank in the building. About 2,000 cards have been issued

Contact: Yoko Tomioka, International Affairs Department, NTT DATA Communications Systems Corporation, Tokyo, Japan - Tel:+81 3 5546 8082. Fax: +81 3 5546 8083.