www.smartcard.co.uk

SMART CARD NEWS

April 1993

Volume 2
Number 4

Post Office Plans £19.5m Terminal Network In UK

In a £19.5 million investment, Post Office Counters Ltd are installing a multi-function Automated Payment Terminal (APT) network, which will eventually be developed to accept Smart Cards, throughout the UK.

Five thousand sub post offices are to be equipped with the new APTs and upgraded terminals in 700 Crown offices .

The objective is primarily to handle volume business from utilities such as the electricity boards, privatised water companies, and British Gas.

Continued on page 63

Smart Card News

Editor: Jack Smith

Technical Advisor: Dr David B Everett

Editorial Consultants:

Dr Donald W Davies, CBE FRS
Independent Security Consultant

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

Chris Jarman
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 9 - Security and the Smart Card

CONTENTS

£19.5m Terminal Network

Continued from page 61

The Post Office APTs were designed by Grid, of Abergavenny, Wales, and are being manufactured by Graseby Keltek, of Kelso, Scotland. The first have been installed in Wales for their first client, the South Wales Electricity Board, who will use them for selling their pre-payment meter tokens. The customer pays for the tokens in cash but uses a magnetic stripe card for identity purposes and to provide customer data to the Board.

Two-year role out

Further installations will follow in Yorkshire and in Scotland as part of a two-year roll out covering the UK by the end of March 1995.

The current terminals accept magnetic stripe cards, but it is envisaged that they will eventually be developed to accept Smart Cards and Smart Keys. They can be adapted for bar code reading if there is a need, perhaps for pension payments; and to read contactless cards such as are being used in the Greater Manchester and London fare ticketing schemes.

A move into Smart Card technology is a strategic development for Post Office Counters, but this will bring it into direct conflict with British Gas who are well advanced in creating their own nationwide network, part of which includes placing recharging Smart Card terminals in post offices.

How the two major national organisations will resolve the problem of different terminals on the same sites is currently under discussion, but the wider issue is that in some cases both will be competing for the same business.

British Gas are installing a nationwide network of 6,000 recharging terminals in newsagents, corner shops and post offices in their Quantum System which aims to help low income families pre-pay for Gas using Smart Cards, and reduce fraud by replacing coin and plastic token meters.

However, its stated intention is to capitalise on this infrastructure and make it available to other interested parties who could use it, for example, to pay council tax, for electricity, water, and stakes in the planned national lottery.

They have over 400 terminals accepting Smart Cards in place at the moment, including a number in Post Offices, and are clearly ahead of Post Office Counters in respect of using Smart Card technology.

On the other hand, the Post Office has agreements with a number of electricity boards to use their terminals and already does substantial business with British Gas.

Conflict of interests

This conflict of business interests will not be easy to resolve. It is likely that we will see both the Post Office APTs and British Gas Quantum terminals sitting side by side in post offices for some time, but eventually, Post Office Counters intend to have their own brand terminals in place, with British Gas using them.

The view from the Post Office is that they are both partners and competitors of British Gas but the market is big enough for both of them.

Contact: Ian Gair, National Sales Manager, Post Office Counters,London -Tel: +44 (0)71 922 1242.

Sega World to Use Smart Cards

Sega, a world leader in high-tech video games, will appropriately use Smart Cards at their new Sega World family entertainment centre scheduled to open in Bournemouth on 1 July.

The contract has been awarded to Cashcard Systems who will be providing card acceptor units and card validator units at the point of sale. The pre-paid cards, specially adapted for the application, will be supplied by Schlumberger Technologies, France, who are Cashcard's development partner.

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

Case Study

US Food Stamps Scheme

The largest off-line Electronic Benefit Transfer (EBT) application using Smart Cards in North America is being piloted in Dayton, Ohio, with implementation throughout the state expected in late 1994.

Called PayEase, the project enables some 13,000 low income families and individuals entitled to welfare benefits (limited to grocery purchases), to carry their monthly benefits in the memory of the Smart Card. The card, which replaces the dollar value of printed tickets called food stamps or coupons, is presented at the check-out to pay for grocery items and the customer is given a receipt showing the transaction amount and the card balance.

The food stamp program is administered by the Food and Nutrition Service of the US Department of Agriculture. Funding is provided by the federal government, and passed on at state level. The objective of the programme is to eliminate paper food stamp fraud and to cut paper and administrative costs incurred with the paper-based system.

$3 million contract

The National Processing Company - the largest bank in the USA in terms of volume of credit card transactions processed - in Louisville, Kentucky, was awarded a $3 million 33-month contract to design, develop and implement the EBT scheme.

About 16 months were spent on the design and development phase and the pilot became fully operational in June 1992. It covers a geographical area of six zip codes (postal codes).

The cards are issued to the recipients by the county's Department of Health and Human services.

About 25,000 microprocessor Smart Cards have been purchased for the application from Micro Card Technologies Inc., Bull CP8's US subsidiary. Some 230 Bull CP8 CAD 1002 point of sale terminals are used in over 50 participating grocery stores. This terminal is used only by the welfare recipient for PIN entry and card balance information. Other equipment (used by the cashier to enter purchase amount) is supplied by Verifone. The equipment is linked to an in-store PC which is used to transmit all check-out lanes' transactions to an NPC host computer at the end of the day.

Costs and benefits

The project will be subject to an independent evaluation by Phoenix Technologies Ltd, and NPC expect that it will validate the acceptability of the new technology by the user community of both retailer and recipient. They also anticipate that costs will compare "very favourably" with similar size pilots which have used on-line technology.

They add that volume sensitive buying of components for an expanded statewide programme, along with a number of efficiency improvements identified in the operation of the pilot, will achieve costs "well within the range of the paper based system" while providing benefit replacement, retailer checkout efficiencies, and higher security for EBT.

Early reports indicate a high rate of acceptance and satisfaction among beneficiaries who say it is easy to use and provides them with faster check-outs and a greater sense of dignity than using paper food stamps.

NPC's own research reveals that public assistance recipients who use on-line systems call customer service 800 numbers about five times a month. In contrast their experience with off-line EBT is that one recipient out of five calls customer service, or one tenth the on-line volume. While this disparity has still to be validated it appears that the recipients feel the value stored in the Smart Card they hold is more secure than if it resides on some remote and somewhat mysterious computer.

Another benefit is that current non-EBT food stamp processing dictates that there is no replacement for lost or stolen food coupons. Like on-line schemes, the PayEase system is designed to replace lost or stolen benefits after the card has been reported stolen. The only difference is a delay of 48 hours to transfer the remaining value from the lost card account to the new one because of the need to identify the unused value on the lost card.

Benefits for retailers include reduced communication costs because communication is only required at time of daily settlement.

Although no figures are available it is anticipated that off-line technology using Smart Cards will reduce fraud and counterfeiting due to the higher level of security available in card authentication and user verification.

In addition, there has been increasing paper food stamp fraud in areas not covered by the Smart Card programme demonstrating the Smart Card's ability to cut down and potentially eliminate paper food stamp fraud.

Additional programmes

Some additional welfare programmes are being considered to be added to the scheme, and an additional card has been developed which will give the Ohio State and NPC the flexibility to use either card depending on the beneficiary's requirements.

The card originally selected was the Bull CP8 TB 100 multi-application card with 24K bit EEPROM and offering DES encryption and message authentication. As of February this year the second card - the Bull CP8 8K bits EEPROM card for which a new mask (card operating system) was developed specifically for the EBT market and compatible with the existing TB100 card - became available.

The new EBT card will be able to support the Food Stamp Programme, Aid for Families with Dependent Children (AFDC) and MEDICAID authorisation. The TB100 card, with its greater memory capacity, can be used for any combination of the above welfare programmes and the Women, Infants and Children Nutritional Programme (WIC).

This development could potentially include approximately 900,000 social benefits recipients in the State of Ohio alone.

Card details:

Type	Contact
FabricatorBull	CP8
Dimensions	OSI ID1
Contact location	Front
Chip manufacturer	Motorola
Chip Referance No	SC21
Chip type	Microcontroller+Memory
Memory type	EEPROM
Mask ROM	6K bytes
EEPROM	3K bytes
RAM	128 bytes
Standards	ISO 7816
Comms protocol	T=0
Security	PIN
Cryptography	DES

Contacts: C Sidney Price, Senior Vice-President, National Processing Company, USA - Tel: - +1 502 364 2000. Christophe Zehnacker, International Marketing, MICROCARD Technologies, Inc., USA - Tel: +1 214 770 5503.

Danmont Progress

The technological trial in Naestved, Denmark, which will lead to a nationwide Smart Card scheme, is reported to be progressing satisfactorily with around 10 per cent of the inhabitants of the trial town taking part in the first four months. Danmont say this is better than expected in the starting phase.

Danmont card transactions amounted to 3,679 in September 1992 (the first month), 4,660 in October, 4,740 in November, and 12,919 in December - a total of 25,998. Services available with the card increased from 23 in September to 36 in December.

The average number of transactions per service over the four month period was 838.

Note: As the Danmont system operates off-line transactions are not registered until they are received at the clearing centre. This could lead to some diversity in the number of transactions for each month.

Contact: Henning Jensen, Managing Director, Danmont, Denmark - Tel: +45 4344 9999. Fax: +45 4344 9030.

Keeping up with Standards

European Committee for Banking Standards (ECBS)

The purpose of the Committee, which is based in Brussels, is to create technical and application standards, including standards for the IC Card, to meet the business needs of the European banking industry, and provide standards for cross-border payments.

The working structure of ECBS is in three tiers: the top tier is the Executive Committee which determines the strategy and policy for standards making and consists of senior bankers from the members and associate members of the three ECSAs (European Credit Sector Associations) who originally proposed the setting up of ECBS.

The next tier down is the Technical Steering Committee (TSC) composed of senior bankers with a more technical operational role and who will determine the tactical strategy for achieving the objectives set by the Executive Committee.

Finally there are the Technical Committees responsible for developing the standards and reports for the TSC.

Executive Committee

The Executive Committee comprises senior members of the European banking community as follows:

Bernard Dentaud	Chairman, and formerly with the Banque de France.
R I L Allen	Association for Payment Clearing Services (APACS), London
U Einhoff	Bundesverband deutscher Banken eV, Koln
A Galan Y Galindo	Confederacion espanola de Cajas de Ahorros, Madrid
A R Gori	Associazione Bancaria Italiana, Rome
K Grunberger	Raiffeisen Zentralbank Osterreich AG, Vienna
J F L Hazelzet	BankGiro Centrale, Amsterdam
J Hergersberg	Deutscher Sparkassen - und Giroverband, Bonn
Ms D Iannucci	Federation Bancaire de la Communaute europeenne, Brussels
E Kostamo	Suomen Pankkiyhdistys, Helsinki
M Ledru	Credit Agricole, Paris
G Pasquali	Groupement Europeen des Caisses d'Epargne, Brussels
M Ravoet	Groupement des Banques Cooperatives, Brussels
P H Wittman	Schweizerischen Bankvereneins, Basle
W Vanderbergen	Groupement Europeen des Caisses d'Epargne, Brussels

Chairman of the Technical Steering Committee is V Hume, Irish Bankers' Federation, Dublin.

Secretary General of ECBS is John Tunstall, formerly of APACS, the Association for Payment Clearing Services in the UK. He was also General Secretary of INTAMIC (International Association for Microcircuit Cards) from 1986 until it was disbanded last year.

The work programme of ECBS is still under consideration. There will be further reports in SCN when it is known what card issues will be addressed.

ECBS are at Place de Jamblinne de Meux 34/35, B-1040 Brussels, Belgium. Tel: +32 2 734 9910. Fax: +32 2 736 4988.

Demise of TeleGuide in Sweden

TeleGuide, the pioneering home shopping service based on Smart Cards and the videotex network in Sweden, ended last month despite providing some 100 services to between 22,000 and 23,000 subscribers and with interest in the scheme still growing.

The service was launched in late 1991 as an equal partnership between Esselte AB, IBM Sweden and Televerket (the Swedish PTT). But its existence was threatened when Televerket announced in the second half of last year that it was changing its business strategy and was pulling out of the venture. Efforts to find a replacement partner failed and it was decided to end the TeleGuide service on 31 March. The normal videotex service will continue until the end of the year.

Anders Falkman, of IBM Sweden, said: “We had a good application which needed more time to develop. However we are happy with the use of Smart Cards in this application and believe that Smart Cards are the best security tool in this environment’’.

Services provided by TeleGuide included phone directories, paying bills, mail order purchases, sending flowers, booking holidays and tickets for the theatre or cinema.

Social security service workers who used to spend time in shops buying food and paying bills on behalf of elderly clients could use the TeleGuide service to order specific foods.

TeleGuide cardholders either had accounts through credit cards like Visa or Mastercard, or through one of the three participating banks, or were billed monthly by TeleGuide.

The system

Security functions at the user end were based on the IBM Personal Security card - an 8K byte Smart Card, a videotex terminal developed by Loewe Opta GmbH with a built-in Smart Card reader, and a videotex PC kit with built-in modem developed by IBM Sweden. The network was managed by Televerket.

Card details:

Type	Contact
Fabricator	IBM
Dimensions	ISO 7816
Contact location	Front
Chip manufacturer	Hitachi
Chip reference no	H8 type
Chip type	Microcontroller+Memory
Memory type	EEPROM
Memory capacity	
	EEPROM8K bites
	ROM10K bites
	RAM256 bites
Standards	ISO 7816
Comms protocol	T=14
Security	PIN
Cryptography	DES

To log onto the network the user had only to insert his card into the reader and key in his four-digit PIN. The terminal checked that the card was a genuine TeleGuide card and, if this was confirmed, the user was prompted to enter his PIN code which was sent to the card to be verified, thus identifying the user to the card.

Identification of the various components in the network was performed through a two-way random “handshake” in which one-time cryptographic keys were exchanged.

Authentication of transactions was supported by a Message Authentication Code (MAC) generated by the card on behalf of the consumer. Before this happened the consumer had to be satisfied with the details of the transaction and approve it. For example, if he purchased three theatre tickets this transaction would be displayed on the screen with the cost. If he was satisfied with the transaction he would “sign” his approval by entering his PIN number again. The PIN was verified by the card which was then authorised to generate a MAC for the transaction data sent to it by the TeleGuide terminal.

Contact: Anders Falkman, Project Manager IBM Sweden - Tel: +46 8 580 21215.

Siemens Crypto Chip - SLE 44C200

Siemens has produced a range of new controller chips in advanced CMOS technology for Smart Card applications. There are three such products in the range (see table below) of which the 44C200 is the flagship. These new chips are based on the 8 bit SIECO CPU which is the Siemens version of the ubiquitous 8051 microcontroller core. Each of these chips incorporates a chip management system (CMS) which handles the interface between the physical security structure of the chip and the rest of the operating system and application program modules. The CMS incorporates the necessary tools to effect the ISO 7816-3 communication interface, the security algorithms, management of the EEPROM, transport code logic for personalisation and an application independent processor identification mode.

It should be noted that this chip management system uses 2K bytes of the available ROM memory for the 44C200 chip and 1K bytes for the other devices.Each microcontroller chip also contains 32 bytes of one time programmable memory (OTP) that may be used to effect the necessary security flags. All the chips also contain a sleep mode which is necessary for conformance with the ETSI standards for GSM. The chips are supplied by Siemens to the IC Card fabricator as a chip module (COB - chip on board).

It is the 140 bit co-processor (developed as part of an EEC initiative) that will have particular significance in security applications that will use public key cryptography. By the use of this co-processor the Siemens chip is capable of generating RSA digital signatures in less than 100mS. At the current time there is significant interest in digital signature mechanisms based on algorithms such as the following,

* RSA
* Fiat - Shamir
* DSA
* Schnorr
* Guillou - Quisquater

Whilst the RSA algorithm has attracted most of the attention until recently, the introduction of the digital signature algorithm (DSA) by NIST (National Institute of Standards Technology - USA) has changed the centre stage arrangement. The Siemens co-processor is adequately defined to handle any of these algorithms. In general these algorithms are based on modular exponentiation of about 512 bits.

The Siemens processor uses an optimised 140 bit wide parallel arithmetic unit. The processor has been optimised to operate with the standard ISO clock speed of 3.57 MHZ and is capable of executing a modular exponentiation,

$$C = M^d \qquad \text{Mod } N$$

With N of 540 bit word in an average time of less than 400mS. This would be equivalent to a straightforward RSA signature function. Siemens claim this offers a performance improvement over other conventional applications by as much as a factor of 6.

The co-processor has been fabricated in a remarkably small area of about 5mm2 where the length of the longitudinal edge of the inner field is about 4mm. The chip is fabricated in 1 micron CMOS technology. The small chip area was achieved by reaching a packing density of 10,000 transistors per mm2 . The word length of the co-processor was chosen at 140 bits to be a compromise between processing speed and the chip area.

It can be seen that the chip is really optimised for operating on 540 bit words by 4 successive 140 bit wide cycles (20 bits are allowed for overflow). The co-processor contains five 560 bit registers, a 140 bit arithmetic unit for 3 operands, two corresponding barrel shifters and four 8 bit interface registers. At 5 MHZ the co-processor can implement a modular multiplication with 540 bit operands in about 0.4mS. The chip allows three 140 bits operands to be processed in parallel.

The chip uses a number of features in the circuitry for performance enhancement. Look ahead algorithms are used for speeding up the multiplication, division and exponentiation process. The normal exponentiation time has been improved by reducing the number of multiplications. On average the number of multiplications required is defined as follows,

$$M = 1.5 \log_2 N$$

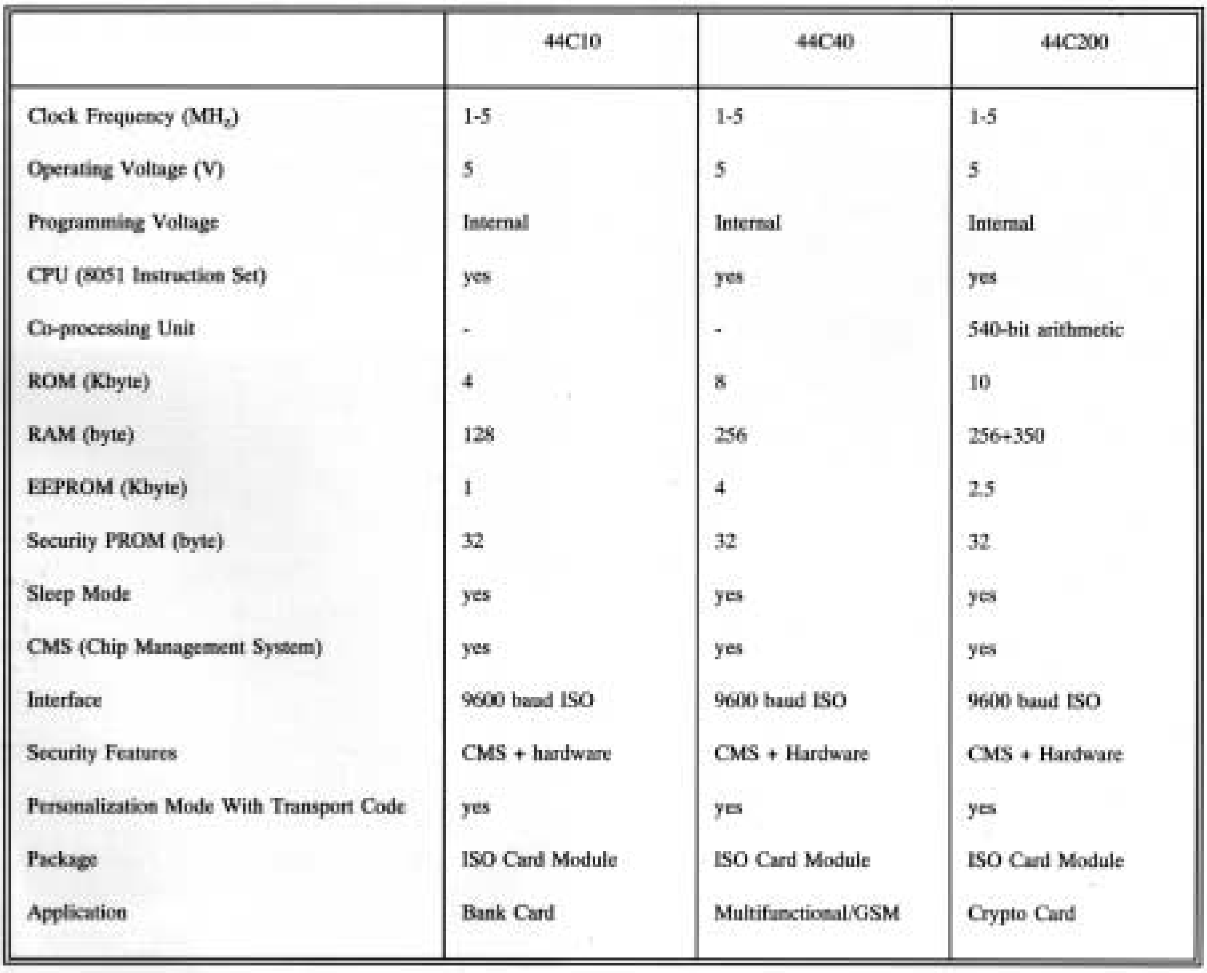
The Siemens co-processor has optimised this to the following number of multiplications,

$$M = 4/3 \log_2 N$$

A further acceleration factor of 2.8 has been achieved by reducing the number of sequential steps. Multiplication is clearly based on addition whilst the modular operations are based on iterative subtractions. The three operand adder allows these operations to take place concurrently. It is possible to execute in parallel one multiplication step and one modulo operation all in one clock cycle.

The Chinese remainder algorithm may be used for algorithms, such as RSA with an acceleration factor of 3.5 to 4. Thus an RSA digital signature with 540 bit parameters and a clock of 3.57 MHZ may be implemented in less than 0.1 seconds.

The Siemens co-processor probably represents the fastest implementation of public key algorithms available today (or even in the pipeline) with a chip suitable for Smart Card applications. The complete chip occupies less than 25mm which is the target size for Smart Card use. The user has 8 K bytes of ROM available for the operating system and application programm, 2.5 K bytes of EEPROM for program and data memory as well as 256 bytes of RAM.



	44C10	44C40	44C200
Clock Frequency (MH$_z$)	1-5	1-5	1-5
Operating Voltage (V)	5	5	5
Programming Voltage	Internal	Internal	Internal
CPU (8051 Instruction Set)	yes	yes	yes
Co-processing Unit	-	-	540-bit arithmetic
ROM (Kbyte)	4	8	10
RAM (byte)	128	256	256+350
EEPROM (Kbyte)	1	4	2.5
Security PROM (byte)	32	32	32
Sleep Mode	yes	yes	yes
CMS (Chip Management System)	yes	yes	yes
Interface	9600 baud ISO	9600 baud ISO	9600 baud ISO
Security Features	CMS + hardware	CMS + Hardware	CMS + Hardware
Personalization Mode With Transport Code	yes	yes	yes
Package	ISO Card Module	ISO Card Module	ISO Card Module
Application	Bank Card	Multifunctional/GSM	Crypto Card

Table 1. Siemens SLE44C Chip Card Controllers

Australian Smartpark

A number of shopping centres provide free or cheap parking for their customers, but in the new Melbourne Central complex in Australia the operator has found that by using Smart Cards incentive parking can be offered to customers combined with an up-to-date analysis of shopping habits.

Called Smartpark, the scheme involves drivers being given a Smart Card instead of the usual paper ticket to gain access to the car park of the city's largest shopping centre.

Card retained

As shoppers pay for their purchases they are asked for their parking card which is inserted into a terminal reader connected to the cash register. Sales are recorded on the card and the more money that is spent the cheaper the cost of parking at the centre.

As customers are leaving they hand in their card at the car park pay desk. If their purchases exceed a certain amount, parking is free.

The card is retained by the operator and stored data is transmitted to a central computer for statistical analysis which provides information on the busiest outlets, shopper habits, and business activity at different times of the day or week. The card is then reprocessed.

Gemplus Card International, France, have supplied 6,000 GPM 896 Smart Cards for the Smartpark scheme.

Residential Smart Card Phone

Schlumberger Technologies have developed a residential Smart Card telephone designed for use in rented property, holiday homes, hotels and hospitals.

The new telephone enables the user to pay for telephone calls using a pre-paid Smart Card cutting out the need to carry coins.

Other advantages for the user are that it can be used for both outgoing and incoming calls, the credit remaining on the card is displayed throughout the call, and a warning tone and blinking display warns when the call credit drops below 30 seconds.

Benefits for the operator/service provider include guaranteed payment, use of the float, and no billing.

Wall-mounted or table-top versions are available.

Contact: Marc Schindler, Communication Manager, Schlumberger Technologies, Smart Cards and Systems - Tel: France +33 1 47 46 70 20. Fax: +33 1 47 46 68 49.

Low Cost Reader 3

US3 Inc. has announced the first in a series of Smart Card readers, the US3221RS, for systems development applications such as computer security and point of sale equipment.

The unit, which interfaces through a RS232 port to a host computer, reads and writes to both memory chip cards and microprocessor Smart Cards.

All Smart Card operations are controlled by the host computer, while the protocol used corresponds to the chip protocol within the card.

Available exclusively from Cristel UK, the US3221RS is priced at £120.

Contact: Terry Warmbier, Cristel UK - Tel: England +44 (0)296 393134. Fax: +44 (0)296 393136.

German Healthcare Application

Gemplus have come up with a solution to bring mobility to the German healthcare application - the biggest project of its kind in the world in which 72 million German citizens with medical insurance are to be issued with Smart Cards.

The scheme will make it easier for health professionals to collect and process administrative data related to their patients, cut the time spent on administrative tasks and eliminate errors due to manual transcription. The Smart Card will also reduce the forms management costs for healthcare insurance companies.

Smart Card readers have been developed for health professionals to use in their offices to access patient cards, but until now there has been no provision for professionals visiting patients in their homes.

At Cebit 1993 in Hannover last month, Gemplus was demonstrating its Gemplus Pocket Reader which plugs into the PCMCIA slot on any portable PC turning it into a Smart Card reader and allowing the health professional to access the insurance card to collect data.

Data stored in the pocket reader can later be processed into a PC or printed out on a reimbursement form when the professional returns to the office.

Contact: Sophie Escand, Gemplus Pocket Reader Product Manager, France - Tel: +33 42 32 51 29.

Omron Standards Status

The card reader division of Omron Corporation, Japan, has been accredited with the following quality standards: ISO 9001-1987, BS 5750 Part 1, 1987, and EN 29001-1987. UK distributor for Omron cardware is Card Systems (UK) Ltd - Tel: +44 (0)273 495034.

A Closer Look at the MFC

The new MultiFunction Smart Card (MFC) was the focus of attention when it was demonstrated at CeBIT '93 International Computer Fair in Hannover, Germany, last month because of the variety of applications that can be made available on one card.

In many Smart Card applications, for example, card telephones, the Global System for Mobile Communications (GSM), and the German health insurance card scheme, operation is limited to a single function and users need a different card for each service.

This is why there is so much interest in multi-functionality. Using the same card a user can, for example, make telephone calls, withdraw cash, pay for goods in shops, book travel tickets, and carry out banking functions from the comfort of home.

As reported in SCN last month, the MFC is a co-operative development by GAD (Gesellschaft fur automatische Datenverarbeitung eG in Munster), Deutsche Telekom and IBM Germany.

They chose ORGA Kartensysteme GmbH to carry out the specification and implementation of the card.

Crucial to the widespread use of the card is for common chip technology to be used in the banking, retail and telecommunications sectors so that Smart Card to terminal security is maintained.

Applications benefits

A particular attraction of the card is the benefits available to the user who can configure the card according to his personal needs. He can select the applications he wants on the card, delete applications, or change them or add to them. The number of applications is only limited by the memory capacity of the card .

Major functions of the operating system include the separation of the transport and application level by implementing the block transfer protocol ISO T=1 and the national (Germany) block transfer protocol T=14; support for the relevant security architecture for access to and transfer of data and programs; and support for a file system for storing data and programs with the option for loading or updating data, programs and applications at a later date.

Applications are represented in the MFC as a data structure in an hierarchical file system which is similar to the directory structure of a PC. This file system can contain data areas both in transparent form and in various formatted forms. Access to data areas is protected by the security functions of the operating system. Controlling or calling of an application is effected on the relevant terminal by means of command calls.

Security architecture

DES, the US Data Encryption Standard, is used as the basis for the cryptographic method used in the card. Other security measures include checking of the PIN in the chip, authentication through challenge/response procedure, encryption and decryption of data, creation of cryptograms, access protection in the file system or on data areas of the applications.

The applications

The first MFC applications were created for banking and telecommunication applications with the emphasis on the implementation of an electronic wallet and the linking of services with Deutsche Telekom cards. Available applications are:

Credit wallet/credit limit

The participating bankguarantees its customer a credit limit which is reduced after each payment transaction. The customer can replenish the wallet at his bank's self-service terminal. All transactions are stored in cryptographic form.

Debit wallet/telephone charge storage.

The card can be used to make calls on public card telephones, but the customer can also recharge the telephone charge storage of his MFC by "buying" new telephone units by means of the debit wallet on his MFC.

Self-service banking/Non Cash.

This application allows the customer to gain access to non-cash payment transactions such as credit transfers, replenishing the credit limit etc, as well as to retrieve account information using the self-service terminals in the banks which are equipped with hybrid card readers ie for magnetic stripe and Smart Cards.

Videotex/Home banking

In this application videotex banking is easier for the cardholder as he does not have to enter a transaction number. The MFC authorises each transaction from its application.

VTX access (Datex-J)

Here the MFC authorises access to Telekom's videotex system and permits post-authorisation, for example, the retrieval of chargeable pages or services.

Okart telephone card

This Telekom service, which allows telephone calls from public telephones to be paid for by monthly invoice, is also available on the MFC.

The MFC is also suitable for use with public fax machines, while applications for public transport systems and parking charges will soon be united on a "City Card."

Economic advantage

The range of functions, high level of security and relatively low cost, gives the MFC an economic advantage, particularly in the communication costs compared with magnetic stripe cards. For example, PIN checks, authorisation, card disabling in the system take place outside of the card in the case of magnetic stripe cards and usually involve an on-line connection. With its intelligent processor chip, the MFC enables these functions to be carried out locally.

Contact: Dieter Hovemeyer, ORGA Kartensysteme GmbH, Paderborn, Germany - Tel: +49 5251 5098. Fax: +49 5251 5098.

Visa Joins AirPlus Card Scheme

Lufthansa AirPlus Servicekarten GmbH, Germany, which has successfully co-branded its AirPlus cards with Eurocard and the Dresdner Bank and Duetsche Bank, has announced that it is also to co-brand with Visa and the Bayerische Landesbank. This makes the credit card services of Visa International available to Lufthansa's frequent flyer and company customers worldwide.

The new card, announced early this month, is the first Visa card with a chip in Germany. The Deutsche Telekom chip is integrated on the back of the card to enable cardholders to make cashless calls from German chip card phones.

At present there are some 82,000 holders of the AirPlus range of cards (See SCN March 1993) and the target number of users by end 1993 is 140,000.

This is the second Visa card programme this year to be co-branded with a European airline and follows the launch of the Iberia Visa card programme in February by Grupo Banco Popular Espanol and the Spanish airline. In 1992, Visa co-branded business card programmes with the Italian airline, Alitalia, and the Irish airline, Aer Lingus.

The Lufthansa AirPlus-Visa Card will combine the worldwide acceptance offered by the Visa network of cash machines and merchants with the range of frequent flyer benefits from Lufthansa which include waiting list priority, participation in the Miles & More scheme, worldwide telephone function and the telephone chip, price advantages and insurances.

Using the new cards, customers can obtain cash from 130,000 Visa cash dispensing machines and pay for goods and services at over 10 million merchants around the world. In Europe, cardholders will be able to use their cards in nearly 57,000 ATMs and at over three million merchants.

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

Smart Card Diary

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.

à la CARD-Symposium ‘93 Technology, Steigenberger Hotel, Hamburg, Germany, 16/17 June.

This 3rd international card conference focuses on recent developments in the card industry. Topics include cards in health care, standardisation, innovative card applications, transport, security, manufacturing and development, telecommunications and networks, and new technology in Germany and Europe. There will be an accompanying exhibition under the heading “cards and innovation.” Contact Hopenstedt & Wolff - Tel: Germany +49 40 271 3323. Fax: +49 40 270 8066.

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.

CarteS 93, Palais des Congres, Paris, France, 20-22 October.

International plastic card forum with conferences, lectures, workshops and a major exhibition. Contact: CarteS 93 - Tel: +33 1 49 68 51 00. Fax: +33 1 47 37 74 56.

Smart Card Reader

A new Smart Card and hybrid card reader, the 160A from American Magnetics Corporation, accepts a wide range of cards including ISO and CP8 chip cards, contactless Smart Cards, and duel technology combining magnetic stripe.
It includes a number of vandal resistant features and is designed for unmanned applications such as public telephones and self-service terminals.

The insertion reader has an optional low power card latch, under software control, which retains the card during the transaction.

Spring loaded card guides provide accurate referencing for bowed or warped cards while the chip contacts are safeguarded from operator damage by an internal contact screen.

Contact: Steve Poulston, European Sales Manager, American Magnetics Corporation, Tewkesbury, England. Tel: +44 (0)684 295475. Fax: +44 0684 295100.

Smart Card Tutorial - Part 8
Inter Industry Communications for interchange - continued.

In this part of the tutorial we will look at the basic commands described in the draft ISO 7816-4 standard. As we have mentioned previously these commands really operate against the assumption of a passive file management architecture. In other words the application in the card is really a file management system with some attention paid to access control. This of course was the only situation possible with a memory type smart card. The advent of microprocessor chips in the smart card opens up new avenues for active applications within the card. Under these circumstances it seems unlikely that such applications would allow many of the commands described here, who for example would allow any terminal to write, uncontrollably to the memory of an electronic purse application. One of the main advantages of a smart card is as a secure data carrier and in our next part we will take an initial look at security to see how everything needs to fit together.

In part 7 we described the command APDU (Application Protocol Data Unit) as shown in fig 1.

The body of this command APDU contains the data (if present) and one or two bytes defining the length of the data sent or received (see part 7 for further detail).

Observant readers will have noticed that earlier in the series when we described the T=0 communication protocol (part 5), we refer only to a fixed 5 byte header. The command APDU shown in fig.1 has only 4 bytes. Well this new part to the standard is aimed at a more general purpose application protocol data unit which allows for data to be sent in both directions (not available when using T = 0). But this part of the standard is none the less upward compatible since the 5th byte was used to indicate the length of the data which now exists in the body of the command as the 1st byte of the body of the APDU.

CLA INS P_1 P_2	Body

Header

Fig 1. Command APDU Structure

b8	b7	b6	b5	Meaning
0	0	0	X	Message Structure & Coding as per Standard
0	1	0	X	Message Structure & Coding as per Standard Least Significant Nibble Coded as per table 3.
0	0	1	X	Message Structure Only as per Standard
0	1	1	X	Reserved for Further Use (RFU)

Table 1. Most Significant Nibble Of The Class Byte (68=0)

The Class Byte

The first byte in the header is the class byte. In the past this byte has been used by the various suppliers of IC cards operating system also as a way of identifying their particular commands.

The part 4 of the standard attempts to give more meaning to the class byte by using it to define conformance or otherwise with the structure and coding used in the standard. The following tables define the proposed use of the class byte,b8b7b6b5

b8	b7	b6	b5	Meaning
1	0	0	0	Proprietary
1	0	0	1	Proprietary
1	0	1	0	Message Structure as per Standard Least Significant Nibble Coded as per Table 3.
1	0	1	1	Message Structure as per Standard
1	1	0	0	Message Structure as per Standard
1	1	0	1	Message Structure as per Standard
1	1	1	0	Message Structure as per Standard
1	1	1	1	(Except CLA=FF$_{\text{hex}}$) Outside Scope of Standard
1	1	1	1	(CLA=FF$_{\text{hex}}$) Reserved for Protocol Type Selection (PTS)

Table 2. Most Significant Nibble Of The Class Byte (b8=1)

b4	b3	b2	b1	Meaning
X	X	-	-	Secure Messaging Format
0	0	-	-	No Indication
0	1	-	-	Secure Messaging Encoding
1	0	-	-	Proprietary
1	1	-	-	RFU
-	-	X	X	Logical Channel Number

Table 3. Least Significant Nibble Of The CLA (As requested in tables 1 & 2)

If readers cannot quickly follow the logic of these tables they are excused. However, we have recorded them here in the event that they may serve some useful purpose in the future.

Perhaps the most important thing to note is the use of CLA = FFhex which is used for protocol type selection as discussed earlier.

The Commands

The draft standard currently defines 11 commands which have varied between all combinations of mandatory and optional. They are currently all optional which says a lot about the use of this standard.

ETSI have taken a different line by defining a similar set of commands which are mandatory. The coding of the instruction byte (INS) for each of these commands is shown in table 4.

INS in hex	Meaning
OE	Erase Binary
20	Verify
82	External Authentication
88	Internal Authentication
A4	Select File
B0	Read Binary
B2	Read Record
C0	Get Response
C2	Envelope
D0	Write Binary
D2	Write Record

Table 4. Inter-Industry Commands

Erase Binary

This command is used to set part or all of an elementary file to its logically erased state. The parameters P1 and P2 in the command header APDU are used to define the offset address of the first data unit to erase. The command assumes that the elementary file (EF) has previously been selected. The data field in the body of the APDU may be used to set the offset of the first data unit not to be erased.

Verify

The principle purpose of this command is to allow the verification of a password. The password is sent as part of the command data. Here the P2 parameter is used as a code to define the whereabouts of the relevant reference data in the card. We will have more to say about aspects of security in the next part of the tutorial.

External Authentication

This command is intended to authenticate an external identity (e.g the interface device (IFD) or terminal) using the challenge response technique. The IC card sends a random number (for example) to the IFD which then encrypts the number using its secret key. The resultant cipher is returned to the IC Card (using the external authentication command) which using the same key can check its corrctness and hence the authenticity of IFD. This proves that the IFD and IC card are members of a set in that they share the same secret key. Another approach is to use a public key system which can achieve the same result without actually having to share the same secret key. Again the P1 and P2 parameter bytes are used to reference the algorithm and secret data in the card.

Internal Authentication

This command completes the bilateral authentication in that the IFD checks the authentication of the card. In this case the random data is sent to the IC card by the IFD. The card then replies with the enciphered version of the random data. The IFD can check this cipher to prove the authenticity of the card.

Select File

The inter industry commands defined in the draft standard are all effectively operations upon a file. It is the purpose of this command to select the relevant file prior to the necessary operation. The file remains selected until another invocation of the select file command. The file may be referenced either as a path description (discussed previously) or as a file name. Within the command header the P1 and P2 parameter bytes are used to select which addressing option is being used. The data body of the command then carries the information necessary to select the required file.

Read Binary

The read binary command is used to read data directly from the selected EF file. The P1 and P2 parameter bytes are used to choose the offset from the start of the file for the first byte to be read. The Le byte in the data body of the command is used to define the number of bytes to be read. The main point to notice here relates to the data structure of a particular file. Quite clearly one cannot mix data stored in binary format with that recorded in a structured record format. A read binary command applied to a file stored in record structure would result in formatting information being mixed in with the data.

Read record

This command is used to read one or more records from an EF file. Normally the file would be selected with a select file command. However it is possible with this command to use a short EF identifier to select the particular file required. The P1 and P2 parameter bytes are used to establish the protocol of which record is accessed. It is also possible to read from a defined record until the end of the file. The Le byte in the data body of the command is used to define the total number of bytes to be read. This command of course should be rejected if the selected file is not stored in a record format.

Get Response

The T = 0 communication protocol has a number of limitations compared with the newer T = 1 protocol. For instance the T=0 protocol does not allow data to be sent in both directions as part of one command. The Get response function allows you to obtain response data generated as part of a command which also contains data as part of the command, whilst using the T=0 protocol. This command is initiated by the IFD. The Get response command belongs to the transmission oriented inter industry commands.

Envelope

This is the second command belonging to the transmission oriented inter industry commands. The envelope command may be used to overcome the lack of a chaining facility in the T=0 communication protocol. Accordingly it allows the IFD to assemble a command and data into a number of envelopes where the total data may exceed 255 bytes which is the normal limit of the T=0 communication protocol data transmission from the IFD to the ICC. Again this command is initialised by the IFD and is really only appropriate for the T=0 communication protocol. The concept of chaining using the T=1 communication protocol has been described previously.

Write Binary

The write binary is the complementary command to read binary. This command is used to write data into an EF file in an unstructured way (i.e not in a record format). The relevant file should previously have been selected by a select file command.

The actual physical writing of data to the memory of an ICC can be quite a complex operation. The process differs between EPROM and EEPROM memory. In this tutorial we have largely ignored the EPROM memory which requires the IFD to supply the memory programming voltage to the Vpp connector. This voltage varies (significantly) between the different chips which is why the necessary information must be contained within the answer to reset (ATR) interface bytes. The EEPROM devices generate the higher voltage required within the chip. It is also necessary for the correct timing sequence to be generated for the memory write operation. This operation typically takes 5mS. An erase operation also takes about 5mS. Some ICC devices have a page operation (typically 32 bytes) when the write and erase operation may be applied to a page at a time. Hence the writing of 32 bytes in this case will only take 5mS. Typically chips with EEPROM memory also allow an overwrite function. When the erase state of the memory is the `1’ condition then this amounts to a logical `AND’ operation. If the erase state is a `O' condition the overwrite operation amounts to a logical `OR' operation. Therefore a complete write operation may iinvolve two steps, an erase followed by an overwrite. All of these processes should be transparent to the application programmer.

Write Record

This is the complimentary function to `Read Record'. The command operates similarly to the read record, where the P1 and P2 parameter bytes are used to define the required record in the EF file. The command also allows the EF file to be identified by a short EF identifier which will override the currently selected file. The Le byte in the data body of the command is used to set the length of the data block. The command allows one of two write modes, append and update.

The Append operation adds a new record to the end of the file whilst the update is used to rewrite a defined record. This command should of course be rejected when the selected file is not structured as a file of records.

This completes our discussion of the Inter - Industry commands. As we have previously mentioned these commands are still subject to further debate in the ISO forum. Further more the commands are at some variance with those being standardised by ETSI. These problems are further compounded by the confusion over the role of security within the ISO standards and this will be our topic of conversation for next month.

Next month Security and the Smart Card

David Everett

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

□ UK £375

□ International £395

□ Please invoice my Company

□ Cheque enclosed

□ Please charge my credit card
Visa/Mastercard/Eurocard/Access

Name_______________________________________

Position____________________________________

Company___________________________________

Address____________________________________

____

Tel.____

Fax.____

Name_______________________________

Address_____________________________

____

Card No.____________________________

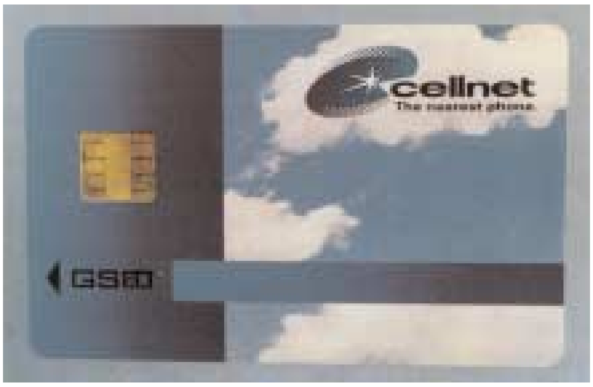
Expiry date__________________________

Signature____________________________

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

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

New Cellnet GSM Card



Cellnet has redesigned its Smart Card for GSM (the Global System for Mobile Communications) in advance of testing which will begin later this year.

The cards have been supplied by Gemplus Card International, and the new design features Cellnet's distinctive "Clouds" design as well as the "Cellnet - The Nearest Phone" logo.

Design agency, Stuart & Knight, described the task as a challenging one as the commercial card will be jointly branded with service providers thus limiting space and design options.

This design will not necessarily be the one chosen for commercial launch so the new cards may become collectors' items.

During the trial period, the Cellnet cards will only be available from participating service providers who will issue them to selected customers.

Cellnet plans to launch GSM in the UK in mid-1993 regionally, and to market nationally in 1994.

Roaming services

In the meantime the company has reached agreements to provide international GSM roaming services for mobile phone customers with Tele-Mobil (Norway), Telecom Finland, Tele Danmark Mobil (Denmark) and Televerket Radio (Sweden).

These agreements clear the way for future GSM roaming services and Cellnet customers will be able to use their phones in these Nordic countries while visitors from these countries will be able to use their phones on the Cellnet network in the UK, yet still be billed by their respective home operators. By the end of this year, Cellnet expects to have signed International roaming agreements with some 10 European partners.

The International roaming services will be commercially available during 1993 as coverage is rolled out.

Cellnet has installed over 140 GSM base stations to date and will have 360 by end 1993. It currently has a working trial network in the Greater London area.

Targets are 60 per cent population coverage by end 1993 and 90 per cent coverage by end 1994.

Contact: William Ostrom, Cellnet, England - Tel: +44 (0)753 504358.