

SMART CARD NEWS

December 1992
Volume Number 14



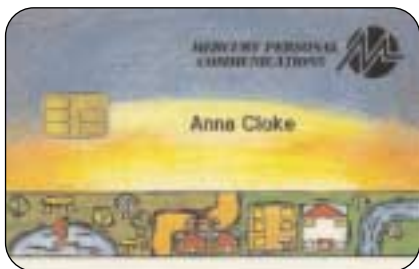
MAC - Major Pre-Paid Application In The USA ?

Philadelphia-based Money Access Service Inc (MAC) has taken a major strategic step in announcing the development of stored value cards which could become the largest electronic purse Smart Card application in the United States.



Gemplus Card International, selected to manufacture the Smart Cards for the MAC network, will be supplying its new PCOS (Payment Chip Operating System) product specifically designed for this type of market (see page 63).

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 5 - Communication
Protocols.

The French Social Security Card.

CONTENTS

Gemplus Launch PCOS Card	63
CAMs - The "Hot Topic"	64
Driving Licence Study	64
Applications Market Forecasts	65
Telepass Autotoll System	67
Richmond Road Pricing Pilot	68
Secure ID at Munich Airport	69
UEPS Developments in South Africa	70
SOLOTEC Options Card	71
£1.5m Clearing Centre	72
Smart Card Parking in Paris	72
Smart Card Diary	73
Smart Card Tutorial - Part 4 Electronic Signals and Protocols	74
Berlin Pilot Starts Next Year	80

Continued from page 61

MAC Pre-Paid Application

ATM and stored value functions will be incorporated on the card which has the capacity of holding an array of personal information such as identification, medical and insurance data, or shopping history for market research or sales promotions.

The MAC system currently has 932 participating financial institutions and some 18.6 million cardholders. MAC branded terminals can be found primarily in seven states including Delaware, Maryland, New Hampshire, New Jersey, New York, Pennsylvania and West Virginia. Pending approval there are plans to extend the network with Electronic Payment Services Inc., a new joint venture company comprising CoreStates Financial Corporation, Banc One Corporation, PNC Financial Corp and Society Corporation. This would expand the MAC network market base to 13,000 ATMs in 16 states.

The MAC Stored Value Card is being presented as a payment method "faster than cash" and it is the cash that MAC is after with US consumers each year conducting over 300 billion transactions under \$10 in value. The aim is to tap the small transactions market which exceeds \$710 billion annually.

The stored value card is being marketed to MAC institutions as providing additional fee revenue, a new source of ongoing interchange income, giving a share of the float pool, better customer retention, increased market share and new market opportunities.

For merchants and service/site providers it is claimed it will provide enhanced customer service, new market opportunities from increased traffic, incremental sales volume, added safety and efficiency, lower operating costs, and differentiation from competitors.

It is being marketed to cardholders as a fast and easy payment method reducing the need to carry cash, extra control over spending, and added safety and privacy.

Contact: Steve Fellows, MAC Network Vice President for Product Development - Tel: USA +1 215 973 7329.

Gemplus Launch PCOS Card

Gemplus Card International is launching the PCOS (Payment Chip Operating System) Card aimed specifically at the Electronic Funds Transfer type market and the electronic purse environment. It is expected to cost between 22-25 French francs in volumes of 500,000 - around half the price of existing cards in that market.

Prototype cards will be available early in the New Year and production quantities from March 1993 onwards.

The company says PCOS incorporates security electronic fund transfer functions while retaining the flexible structure of the COS family. Main characteristics are:

- * Specific electronic fund transfer management functions (secure debits/credits)
- * COS compatible file management
- * Security system based on the DES algorithm
- * ISO standard 7816-1/2/3
- * 1K bytes of rewriteable memory (EEPROM)

Gemplus see the PCOS Smart Card as providing all the essential functions for an electronic funds transfer application within a single product.

Contact: Paul Naldrett, Gemplus Card Services, London - Tel: +44(0)71 702 9030.

Thyron Appointments

Robert Maddock has been appointed Technical Director at Thyron, England. Previously he was with EDS Scicon where he worked on airport systems. Bill McCall has joined Thyron as Business Development Manager from JerseyCard where he held a similar appointment and assisted in establishing the infrastructure for expansion, for example, into town cards.

CAMS - The "Hot Topic"

Discussions to identify a Card Authentication Method (CAM) is now the "hot topic" in the financial services market, and the eventual decision will direct the method of plastic card payment in the future.

Visa is already advanced in its own CAM Study sparked off by an increasing trend in counterfeit fraud. It is believed to have a number of methods currently testing and is aiming to complete its study in mid-1993.

Perhaps the realisation of the influence that Visa could have on its member organisations in deciding on a CAM has prompted a change in focus of the Plastic Fraud Prevention Forum (PFPP) - an action committee set up by the UK Association of Payment Clearing Services (APACS) to combat plastic card fraud.

CAM, at least in the short term, is now firmly on the agenda for PFPP who want to become involved with the Visa Study "in great detail."

Steve Collins, Project Manager of PFPP said: "With Visa looking at the identification and mandating of a CAM for its membership globally there is no point in us doing the work we are doing in isolation. If we come up with a different CAM to the one Visa think should be used then we would still have to implement the one Visa identifies, so the name of the game is to try to get everyone involved in it round the table to try and reach a consensus which is not going to be an easy or quick task."

The solution is likely to involve a potentially large capital investment whatever CAM is chosen with the banks committed to an on-going cost, so they will be looking for a business case which is as near cast iron as possible.

It is understood that Barry Fergus, Project Leader of PFPP and a security professional from Barclaycard, will lead the CAM initiative.

Recently PFPP were looking closely at Smart Card technology as a secure method of off-line authorisation and conducted market research to test consumer reaction to the use of Smart Cards with PIN, digital signature and fingerprint

scanning for user verification. The conclusion from this research was that fingerprint scanning was the preferred option. The equipment used in this case was the Bull CP8 card as used at Expo '92 in Seville, Spain, with a second generation scanner from Telesincro.

However, this does not indicate a preference by the banks for using Smart Cards, despite the announcement by Visa itself that it would support members' use of Smart Cards. Watermarking and holographics etc will be examined in an equal light.

Driving Licence Study

Britain's Driver and Vehicle Licensing Agency (DVLA) is carrying out a feasibility study for a new format driving licence to include a photograph of the holder, and will consider the use of Smart Cards.

Photographs on driving licences are required by 2001 under the European Commission's directive 91/439/EEC. However, the directive also prescribes a new format with "pictogrammes" replacing narrative text to describe the categories of driving entitlement to be achieved by July 1996.

DVLA consider it would be desirable to bring forward the photographic requirement and introduce it with the pictogramme changes.

In addition the EC are currently working on an appendix to the directive that will give member countries the option of using plastic cards for their driving licences.

The DVLA study is to evaluate the feasibility of including photographs on driving licences within the timescales and to establish whether the licence should remain paper based or become a plastic card application.

"The feasibility study will also consider the benefits of using Smart Cards rather than other types of plastic card," says the DVLA.

At present there are some 46 million driver records on the DVLA database of which about 35 million are active.

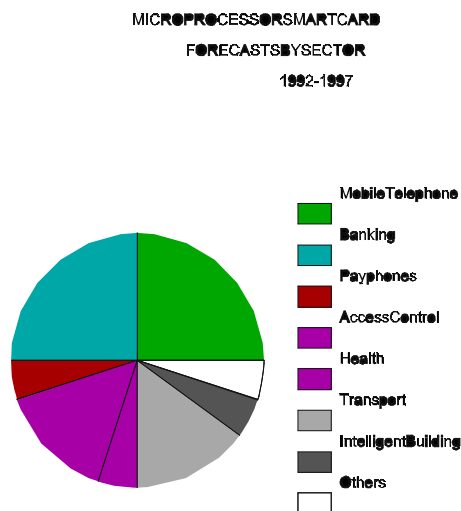
Applications Market Forecasts

Smart Card applications market forecasts by industry sector for the period 1992-1997 show interesting differences between the expected demand for microprocessor cards and contactless cards.

Contact cards with their ability to carry out complex calculations and processing are particularly suitable for applications requiring high levels of security, and it is forecast that half of the market will be shared equally between mobile telephones and banking, while transport is expected to account for 50 per cent of the market for contactless cards.

In presenting his forecast (see figures) at an introductory tutorial to Smart cards at the European Payments 92 conference in Edinburgh, Scotland, last month, Robin Townend, Senior Research Manager, Barclays Bank, said it was probably more revealing to address the question of who was going to place orders, and for what by examining the market sector forecasts as the importance of the technology differed across industry.

Previous predications had always promoted the banking sector as the first mass market, but outside France this had clearly not been the case. "This demonstrates that the Smart Card cannot be viewed as the magnetic stripe bank card replacement," he said.



Mobile Telephones (25%)

GSM (Global Systems for Mobile Communications) is starting to move significantly with networks rolling out throughout Europe (SCN No.3) and is expected to become the biggest single user of Smart Cards (Subscriber Identification Modules) which provide the data necessary to access the network, authenticate and bill the holder of the card. In addition to Europe, Singapore, Hong Kong and Australia plan to use the GSM standard and others will follow.

Banking (25%)

Carte Bancaire member banks in France have already issued over 17 million Smart Cards for their card payment system. Norway, the only other country to adopt Smart Cards in retail banking (1.5 million cards) may revert back to magnetic stripe based solutions now that telecommunications costs there have been substantially reduced.

"This does not mean there will be a decline in migration to Smart Cards in the banking sector," said Mr Townend, "but demonstrates that the business case varies from country to country. In fact, the business case varies from issuer to issuer within the same country."

In the UK, "the jury is still out" at the APACS Plastic Fraud Prevention Forum (PFPF) concerning the future direction of the Cardholder Verification Study.

"The final short-list of solutions has been drawn up and is currently being evaluated. Either way we can conclude that at some point in the future we will migrate to Smart Card technology. I predict we will see the Smart Card emerging in significant numbers within retail banking over the next five years. The issue here is terminals - there needs to be a critical mass of hybrid terminals deployed ahead of the card issue programme."

Since Barclays launched the PDQIV portable hand-held terminal in 1989, said Mr Townend, nearly 7,000 have been deployed in the UK. The

PDQIV is the forerunner to a proliferation of EFTPOS devices which support Smart Cards for data processing - this trend will continue.

In the development of several national "Electronic Purse" systems issuers will migrate from small memory Smart Card to microprocessor cards which offer more functionality and can be "recharged."

There will be continued growth, albeit small volumes, of Smart Cards used for access to Corporate Cash Management and Treasury systems and banking networks. The SWIFT network, for example, is to be protected by Smart Cards.

Payphones (5%)

Small memory Smart Cards will remain the order of the day for payphone applications but many operators will offer services based on microprocessor cards.

Access Control (15%)

Physical and logical access control systems represent current growth areas for Smart Cards and constitute many sales of small closed user group systems. Here the issue of standards is less relevant, and in fact can be advantageous in security applications. Physical access control covers the protection of installations such as nuclear power stations, Military establishments and large Corporate facilities. This market will continue to grow and become increasingly more sophisticated with personal identification techniques using various biometric identification systems providing user ID delivered on Smart Cards. Logical access control Smart Cards have proved the most effective means of protecting access to computer systems and networks. Today all High Street Banks in the UK offer Cash Management Systems protected by Smart Cards.

Health (5%)

The market for microprocessor Smart Cards in the

health sector is seen not as a large scale patient card but as a Health Care Professional card.

Transport (15%)

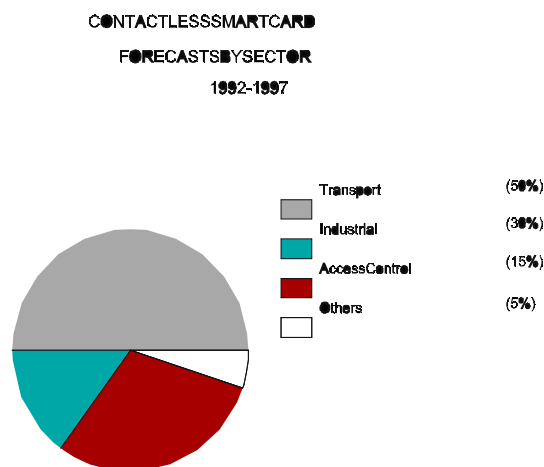
The large user of microprocessor Smart Cards in the transport sector is likely to come from the automotive industry as a service log and vehicle history. The Nissan Car Life programme, for example has over 1 million users. Other uses are in the airline industry for passenger movement and frequent flyer programmes.

Intelligent Buildings (5%)

This concept involves a multi-functional card providing a range of applications such as physical access control, personal files with emergency medical data etc, and payment functions for vending, canteens and shopping.

Others (5%)

This category includes various applications across the industry such as food stamps, national ID cards, home shopping applications and gas and electricity metering.



Transport (50%)

Contactless cards have found a niche in the transportation sector. Automatic Vehicle Identification (AVI) and public transportation systems are the two key markets to date. Examples include toll revenue collection, car parking, bus and rail ticketing systems.

Access control (30%)

As mentioned before access control is a growth market for Smart Cards of all types.

Industrial (15%)

Industrial applications relate to the use of contactless cards as an auditing device. For example, in manufacturing the card follows the manufactured article through the entire production cycle and in some instances through to the customer as an ongoing service record.

Others (5%)

Some contactless Smart Cards are being used in banking and payment system applications mostly for conditional access of Corporate Cash Management and Treasury services. Vending machines are also a growth area.

-The user need not stop at either the entrance or exit.

-The system must not be obligatory for use of the motorway.

-The system must be fully integrable with current payment systems and allow smooth transition.

-The car mounted unit must be cheap.

-The installation of the car mounted unit must be simple.

-Fraudulent use of the system must be prevented.

Telepass users are provided with a free in-car unit (car box) which is mounted on the windscreen of the vehicle and uses a Smart Card for recording entrance point details and for payment of the toll. It acts as a quasi-passive transponder, i.e. it contains no radio frequency generator but re-modulates the carrier wave which is sent from overhead beacons.

The Smart Card can also be used to pay at non-Telepass toll booths by inserting it into the same machine used to debit via prepaid magnetic card, thus meeting one of the prime requirements that if a vehicle enters the motorway at a Telepass booth it should be able to exit at a toll booth where there is no Telepass system.

Autotoll Operation

As vehicles approach the toll booth areas, microwave beacons interrogate the car box and send it the relevant data when the car is at an entrance or exit. The beacons are placed above the lane and are linked to a local server computer which sends, receives and processes all the information for the car's progression through the system. There are a minimum of three beacons per tollbooth, the first connected directly to a VAX while the others are connected to a personal computer which acts as a server to the VAX host.

Also connected to the network are a vehicle classification system, an optical barrier and a car number plate capture system.

Beacon One is situated about 100 metres up traffic from the tollbooth covering all the approach lanes

Telepass Autotoll System

Italy's Automatic Pay Toll System on the motorway between Milan and Como now has 75,000 users who use AT&T contactless Smart Cards to pay charges automatically without having to stop at the toll booths.

Called Telepass, the system was designed for Societa Autostrade, the Italian company responsible for most of Italy's motorway system, by Sixcom Olivetti Group, Marconi and AT&T. It became fully operational in mid-1991 after successful customer acceptance testing with an initial trial of 10,000 users.

The design philosophy behind the system was:

and "wakes up" the car box. If no card is in the car box the driver receives an audible warning telling him either to insert the card or use the normal tollbooth.

Beacon Two is activated by a car passing an optical barrier and polls the car box which responds with the Smart Card number (in the case of an entry point) or the data stored on the Smart Card (in the case of an exit point). While the car is approaching Beacon Three the computer system checks the Smart Card against a black list.

In the case of an entrance, Beacon Three transmits the entrance time and date, the entrance code and the vehicle class. In the case of an exit, the toll is calculated and the exit time, date and code are transmitted to the card in addition to the toll value.

If a vehicle passes either Beacons Two or Three without a response being received from the car box then a violation is recorded and a video camera captures the number plate of the vehicle.

Card Function

The card can function in two ways, either as a prepaid stored value card or as a charge card issued on the customer's bank account. In both cases the card can be inserted into machines at service areas to obtain a reading or print out of the transactions.

The card operating system allows new applications to be added to an already issued card, limited only by the card memory which is currently 2K Bytes of EEPROM available for user data. Potential uses include digital mobile communications and purchasing petrol. However, there are no plans at present to add such services, current marketing strategy focusing on increasing the client base using the Telepass system.

Contact: Gabriele Cottura, Strategic Marketing Manager, Olivetti Sixcom - Tel: Italy +39 125 521324.

Richmond Road Pricing Pilot

A new road traffic pricing project using Smart Cards and currently under second prototype testing at the GEC Marconi Research Centre, at Chelmsford, England, will be piloted in the Borough of Richmond, near London, around mid-1993.

Easams, the Surrey-based systems engineering and transport studies arm of GEC Marconi, is developing a new advanced system for road pricing called Timezone, which looks more user and environmentally friendly than the complex European Commission funded system devised for Cambridge (SCN No.2).

The Easams project involves Smart Cards, small In Vehicle Units (IVUs), and UHF lamp-post mounted beacons. The system will be piloted using a variety of Local Authority vehicles.

Designated Areas

It is envisaged that drivers will only be charged when they enter designated areas during busy periods. They will be charged for every minute they are in the system, but won't be penalised if they are stopped at road works, for example, as the IVU detects and stops after two minutes. If they decide to park at a parking meter they can press a button on the IVU which will tell them that parking costs say 50p an hour and will start charging at that rate.

Depending on what the client wants, the Smart Card may be purchased in a fixed amount and then thrown away, or it may be a re-chargeable card which can have value added at garages, post offices etc. In the latter case the card can provide audit information when it is recharged on what the motorist did to incur the charges and provide, anonymously, statistical information on traffic patterns.

An NMOS card from McCorquodale Smart Card Systems is currently under test but will be upgraded to a CMOS card for further development because of its greater storage capacity and lower power consumption.

People who attempt to abuse the system can be detected by a TV detector type van and have their car number plates photographed and be sent a summons in the post. Visitors would need to purchase a sticker.

Contact: Ivor Thorne, Project Manager - Tel: England +44(0)276 63377.

Secure ID at Munich Airport

A high security Smart Card ID pass system for all personnel at the new Munich Airport, opened in Germany earlier this year, is claimed to be unequalled anywhere else in the world.

More than 20,000 Siemens Nixdorf Smart Cards - the SCC (Security Computer Card) V2 - have been issued as ID cards for employees of different organisations such as the airport authority, airlines, the federal air traffic control authority, police, customs, businesses etc.

With its integrated processor and resident crypto-algorithms - DES (the US Data Encryption Standard) and SCA 85 (a proprietary algorithm) the SCC can perform dynamic authentication procedures. It is also the first Smart Card worldwide to receive the high security certificate Q4 (which corresponds to B2 in the US "Orange Book") from the German Information Security Agency (GISA) for the card operating system software which controls all security-related operations and accesses.

The airport is divided into four different zones, each with its own access level. The public area includes parking areas and sections of the terminal building where passengers check in or people wait for arrivals.

The second area has restricted access for the public, for example, passengers waiting to board aircraft after check-in.

The limited security area includes the interior of the freight terminal and the various catering companies that provide in-flight meals for passengers.

The security area includes all flight operation

areas such as the terminal apron, taxiways and runways.

Clearly not everyone employed at the airport is authorised to enter every area. Over 20,000 employees from more than 200 companies and public authorities operate in the three areas subject to restriction. Many are only authorised to enter a single area while others are constantly on the move, using their Smart Card in one of the 230 card readers on the site to pass from one zone to another. It is estimated that there are about half-a-million checks or more daily.

In addition to the security application the Smart Card allows access to employee parking areas, is used for time recording, as a driver's licence for the shuttle buses and replaces cash in the staff restaurant.

A photograph of the authorised holder is taken with a video camera and etched onto the card together with his or her name and the name of the employer. As an additional security measure a computer-controlled diamond cutter partially removes the black-coated surface of the card resulting in a picture and text in relief. Any attempt to forge a card by sticking on a photograph, for example, would be immediately detectable by running a finger over the surface.

Card details:

Card type	Contact
Chip manufacturer	Siemens
Chip Ref No.	SCC V2
Chip type	8-bit CPU
Memory capacity	
Mask ROM	6Kbyte
EEPROM	3Kbyte
RAM	128-byte
Comms protocol	T=1 or T=14
Security	PIN
Cryptography	DES
	SCA 85

Contact: Manfred Reichherzer, Siemens Nixdorf, Munich, Germany -Tel: +49 89 636 2471.

UEPS Wallet in South Africa



The Universal Electronic Payment System (UEPS) electronic wallet Smart Card application in South Africa is undergoing a strategic change with the development of a common standard for a joint initiative by all the banks who want to join in. By having agreed standards it will provide the platform for saturation implementation of the market without the expense of duplication of terminals at the point-of-sale.

UEPS was launched on a large scale in the first half of 1991 by SA Perm Building Society, a division of the Nedcor banking group, and Megalink, the system operator and switching subsidiary.

The system concentrated on targeting specific areas for intense marketing to avoid having either insufficient card or terminal population. This strategy has proved successful and the system has been well accepted by both cardholders and retailers and Net 1 has so far supplied some 100,000 Gemplus Card International Smart Cards and 3,000 point-of-sale units for the system.

However the growth path is seen clearly as having agreed standards and a joint initiative by the four major banking groups in South Africa - ABSA, First National Bank, Nedcor and Standard Bank. Gemplus has produced a new mask for the proposed joint initiative and a common standard is expected to be agreed by February next year.

The banks have not yet formally agreed on the initiative, but Net 1 Products (Pty) Ltd, the Gemplus distributor in South Africa, expects to increase its staff by 60 per cent in 1993 and supply over 10,000 terminals and between two and three million Smart Cards.

Current system

In the current system all client cards have a magnetic stripe for use at ATMs and there is provision for signatures on the cards. When the card is issued the client's existing bank account is linked to the card and the client selects one or more passwords (one for loading value, and one for spending).

The norm is to select a single password for both functions and the system is transparent in that the card recognises that only one password has been selected and can be used for all functions without regard for the second password option.

If the cardholder forgets his or her password all stored value on the card can be credited to the home linked bank account before a new password is entered on the nil balance card. The unique sequence number of the bank teller card is written to the Smart Card to provide a trace of the party responsible for personalisation of the card.

After the cardholder has loaded funds onto the card this stored value can be used to purchase goods or services at participating retailers.

Apart from paying off-line, cardholders can perform routine functions such as load and off-load funds, obtain balances and list transactions, change passwords and obtain cash from ATMs (through mag-stripe) or from retailers by increasing the value of the purchase transaction.

A Special Credit Facility (SCF) enables salaries, medical aid payments and pension refunds to be automatically loaded at a Funds Transfer Machine when such arrangements have been made.

Another service, the Special Payment Facility (SPF) allows the cardholder to pay bills using his card at a Funds Transfer Machine where the merchant has provided Megalink with details of

its clients and the amounts due.

In this case the cardholder simply selects the "bills" function and is presented with the merchant's name and the amount owing. The client can then accept the amount shown or alter this before making payments. Settlement is achieved centrally by Megalink.

On average retailers settle once per day and have their accounts credited with the next settlement run.

The High Speed Self Service (HSSS) facility is available to all cardholders who want to speed up low value transactions and forego the security and delay associated with entering passwords.

To increase market penetration and provide for existing magnetic stripe credit cards, the terminal software has been extended by Net 1 to accept all well-known brands of credit and petrol cards. These transactions are also stored on the Retailer Smart Card and settled at the same time as the other client Smart Card based transactions. Point-of-sale terminals are fitted with a modem for transaction authorisation above the floor limit.

UEPS in Namibia



In neighbouring Namibia, UEPS has been pioneered by SWABOU (South West African Building Society) under the Megalink brand name. The system has been running in the capital Windhoek since July 1992 and is now being extended to Swakopmund.

The system in Namibia is a pure Smart Card initiative and does not provide for magnetic stripe

usage at ATMs or points-of-sale.

It is marketed as a general purpose payment card with concentrations of participating retailers in specific localities. Demand from both cardholders and retailers is reported to be strong.

A number of surrounding countries have expressed interest in UEPS and are closely monitoring developments in South Africa before committing to similar installations.

Contact: Andre Mansvelt, Net 1 Products (Pty) Ltd - Tel: Johannesburg, South Africa +27 11 880 5850.

SOLOTEC Options Card

South London Training and Enterprise Council (SOLOTEC) has issued some 1,800 Smart Cards to enable young people to buy practical, job-orientated training.

Called the Options card, it is available to 16 and 17-year-olds living in the London Boroughs of Bexley, Bromley, Croydon or Sutton who have left full-time education whether they are in employment or currently without work. Up to £2,700 is made available by SOLOTEC towards the cost of training for a nationally-recognised vocational qualification (NVQ).

The Smart Card - the Philips TB 100 multiple application EEPROM card - contains the user's name and identification number and records the young person's progress through the programme.

It can be keyed into a computer to show on screen the details of training programme, including costs, how much has been spent and the balance left in the account. This information is confidential to the cardholder who has a PIN to ensure that no-one else can access the information without his or her permission.

Contact: SOLOTEC Training Account - Tel: 081 313 9232.

£1.5 million Clearing Centre

A £1.5m computer centre is to be set up to clear rechargeable Smart Card payments in the Greater Manchester Passenger Transport Executive (GMPTE) electronic ticketing scheme which is to be extended from its transport base into local authority applications and as a general prepayment card.

This clearing centre will process transaction data and provide the information necessary to provide settlement to service providers, merchants and point-of-charge outlets without the involvement of banks.

The centre will be provided by AS Scanpoint (UK) Ltd, who are delivering the total Automatic Fare Collection (AFC) system, and will be located in the Greater Manchester area although no site has yet been selected.

GMPTE is already a licensed deposit taker and plans to set up a joint venture company - Prepayment Cards Ltd - with AS Scanpoint which will be a subsidiary to the Executive with the same licensed deposit taker status.

The original implementation plan provided for 800 outlets, including post offices and newsagents where customers will be able to charge their card. Now the Executive are reviewing the mix and plan to add convenience stores on the basis that the amount of money going on the purse is likely to increase if they are charged up in a shop that sells more commodities.

Discussions have been taking place with local councils, education and health authorities for the extension of the card use in other areas as a viable alternative to cash and cash collection.

A school pilot scheme is being planned for mid-1993 for attendance and registration systems and for school meals. The Executive have also had three proposals for loyalty schemes and are believed to be close to agreements which will incentivise the use of the purse.

In another development, several manufacturers have been invited to look at the feasibility of

attaching a card reader to the side of a telephone as a method of loading value on the card. The user would dial his or her bank and use a PIN which only works with their telephone for security. When asked how much value they want to put on their card, they use the phone key pad to enter say £10, and £10 goes on the card.

In the first phase Smart Cards will be issued to over 500,000 concessionary bus and train passengers, later increasing by early 1995 to over one million for the transport application alone.

Contact: Mike Hill, GMPTE, Manchester, England - Tel: +44 (0) 61228 6400.

Smart Card Parking in Paris

Parisians in a large part of the city are now paying for their parking using the Paris Carte pre-paid Smart Card. Launched in November 1991 the scheme now covers the 1st to the 5th arrondissements (Department subdivisions) and is being extended to cover all of the capital by 1995 when all pay-and-display parking systems will accept the card.

Paris has some 9,000 pay-and-display units (each serving 11 or 12 parking places) rising to 13,000 by 1995 - half of the total in France. In the 1st arrondissement alone there are more coin and card operated units than in the whole of Marseille, France's second city - a fact recently explained by Project Leader Jacques Brunet with the comment: "Parisians don't like walking."

In the first phases motorists have had the choice of paying either by card or cash, but new Smart Card only machines are to be introduced later. The throw away card, which can be purchased at tobacconists, is available in values of 100 and 200 French francs.

A major benefit for the Paris Council has been in streamlining its pay-and-display management by reducing the approximately four tons of coins per day with the associated security and transportation.

The Paris Council selected Smart Cards from two manufacturers, Schlumberger Technologies and Gemplus Card International (F1024, SE416, GPM416). The F1024 is a 1280 bit EPROM and the 416 is a 416 bit EEPROM.

New applications for the Paris Carte will soon be developed such as paying for municipal services, swimming pools and museums.

DataCard to Supply Mercury PCN

DataCard Corporation has announced that it is to supply Mercury Personal Communications with Smart Cards for its new cellular telephone Personal Communications Network (PCN) to be launched in the UK in mid-1993. Orga Card Systems (UK) are also supplying Smart Cards to Mercury.

The 8K byte EEPROM card will be designed, manufactured and personalised by DataCard for use as the Subscriber Identification Modules (SIM). They will also provide special "plug-in style SIM" size cards specifically designed to plug inside mobile telephone handsets. Cardinal has been involved in providing the operating system for DataCard.

The design platform, says DataCard, "makes it easy to expand the card's functionality" as Mercury's requirements change.

Mercury says it will launch its PCN service in mid-1993 initially to people living and working in and around London and the M25 orbital motorway, with the service expanding swiftly into the South East before moving in other parts of the country.

Smart Card Diary

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

With GSM networks now in place and rolling out, the conference will concentrate on markets plans and expectations, reports from network operators and manufacturers, and examine critical issues and the needs and expectations of users.

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

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

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.

Part 4 - Electronic Signals and Transmission Protocols.

The electronic properties and transmission characteristics of the IC card are fundamental to interoperability. These specifications are defined by ISO as part three of the 7816 standard. This standard is subject to an amendment for the T=1 transmission protocol and a proposed review for protocol type selection (PTS). The principal subjects to be considered are as follows,

- Electrical characteristics
- Character transmission
- Answer to reset (ATR)
- T=0 transmission protocol
- T=1 transmission protocol
- Protocol type selection (PTS)

We will consider each of these topics in turn.

IC Card Electrical Characteristics

We have previously discussed the position and definition of the IC connector and have identified 8 contacts of which 6 are currently defined,

- V_{CC} Power supply
- GND Ground or reference voltage
- CLK Clock
- V_{PP} Programming voltage
- RST Reset signal
- I/O Serial Input/Output

Power supply (V_{CC})

The power supply to the IC is defined to be between 4.75 volts and 5.25 volts with a maximum current consumption of 200mA. Both of these parameters have problems. Newer chip fabrication technologies are moving sub micron, 0.8um is already commercially available and 0.5um is not that far away. These chips may operate with a supply voltage of 3 volts which results in lower current consumption. Most card acceptor devices (CAD) operate at 5 volts as specified in the ISO standard. Whilst a 3 volt IC may be designed to operate between 3 volts and 5 volts, running a 5 volt IC at 3 volts is a non starter.

A current consumption of 200mA is far too high for modern electronic equipment particularly when the equipment is portable and driven by a battery power supply. Most IC cards have a power consumption of between 10mA and 20mA (at 3.58MHz). ETSI in the development of their standards have adopted a far more rigorous specification of 20mA maximum for normal use and a 10mA maximum for use in portable equipment. They further defined the concept of sleep mode (not covered by ISO 7816-3) where the IC chip can reside in a latent mode preserving volatile memory contents with a maximum power consumption of 200uA.

Clock signal

Although the integrated circuit could contain its own clock circuit for driving the internal logic, in practice most IC chips are supplied with an external clock by the interface device. It should be noted that the speed of the serial communications on the I/O line is effectively defined by the frequency of this clock. The ISO standard aligns with the use of two widely used external clock frequencies, 3.579545 MHz and 4.9152 MHz. The former frequency is the more widely used (being based on the NTSC colour sub carrier frequency) and results in a clock divider of 372 in order to produce a 9600 bit per second (not exact but within tolerance) serial communication speed. The latter frequency has a simple divisor of 512 in order to achieve a 9600 bit per second communication speed. The standard defines the situation after reset whilst allowing the frequency to be selectively changed by means of protocol type selection.

Programming voltage V_{PP}

This signal is designed to provide the high voltage required to enable writing to the non volatile memory. The more popular IC's use EEPROM memory where the high voltage is generated by a charge pump on chip. However the EPROM memory type needs the high voltage (usually 12.5V or 21V) to be externally provided on the IC connector. There have been problems in the past with terminals supplying the wrong programming voltage with somewhat drastic effects. Because of

this and the significant advantages of having a rewritable memory the EEPROM memory is by far the most popular for IC card applications, hence the role of V_{pp} is rapidly diminishing.

The Reset Signal

The reset signal is asserted by the interface device and is used to start up the program contained in the IC ROM. The ISO standard defines three reset modes, internal reset, active low reset and synchronous high active reset. Most microprocessor ICs operate using the active low reset mode where the IC transfers control to the entry address for the program when the reset signal returns to the high voltage level. The synchronous mode of operation is more commonly met with the memory card ICs as used for telephone applications.

The sequence of operations for activating and deactivating the IC is defined in order to minimise the likelihood of damage to the IC. In particular the inadvertent corruption of the non-volatile memory (EPROM or EEPROM) must be avoided. The activation sequence for the interface device is defined as follows,

- Take RST low
- Apply V_{CC}
- Put I/O in receive mode
- Put V_{pp} in idle mode
- Apply clock
- Take RST high (active low reset)

The IC deactivation sequence for the interface device is as follows,

- Take RST low
- Take clock low
- Deactivate V_{pp}
- Put I/O in the low state
- Deactivate V_{CC}

Serial Input/Output (I/O)

The ISO standard defines a single line for the interchange of data between the IC and the interface device. This means that the line must change direction depending on whether the IC is transmitting or receiving. In practice this cannot

be instantaneous and the expression 'line turnaround time' is commonly encountered in the modem world. The transmission protocol must take account of this need to turn the line around.

Character Transmission.

The transmission characteristics operated by most microprocessor IC cards are based on an asynchronous half duplex mode of operation. In the T=0 communication protocol this involves the transmission of bytes whilst the T=1 protocol defines a block mode of operation. As we have already observed the serial communication is operated by the use of a single chip connector, where the direction of data transmission has to change depending on whether the IC card or interface is transmitting data. This is referred to as half duplex communication whereas two I/O signal connectors would be required for full duplex operation where transmission can take place in both directions concurrently.

The asynchronous type of transmission is similar to that used by the serial RS232C connector met on the personal computer. Although the PC operates in full duplex mode. The transmission of a single character (defined as 8 bits) requires an overhead of several bits as follows,

- Start bit (*used for character frame synchronisation*)
- Parity bit (*for error detection*)
- Guardtime (*separation between characters*)

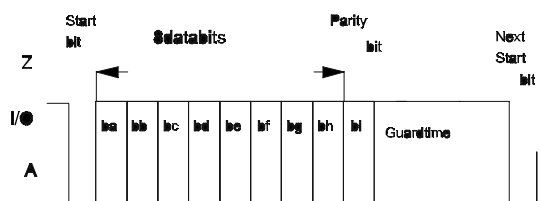


Fig1. Asynchronous Character Frame

The format of a character frame is shown in fig.1. The receiver examines the I/O looking for the transition from the mark or high state to the space or low state. The sampling of the line is required to be such that the receiver monitors the state of the line in the centre of each bit period with a precision of $\pm 20\%$. The parity bit is defined to achieve even parity which means that the number of 1's in the 8 data bits and the parity bit together results in an even number.

The guard time is defined to be equal to two bit periods (although for block mode it can be changed to a 1 bit period). This is similar to having two stop bits on a UART (Universal Asynchronous Receiver Transmitter) as used in the PC.

A more common definition of the asynchronous serial transmission at reset would be 9600 bits/second, 8 data bits, even parity, 2 stop bits with half duplex mode of operation. The half duplex refers only to data transmissions in one direction at a time which a PC is perfectly capable of managing with its UART. The RS232C interface however defines two separate wires for data transmission and reception which would need hardware modification in order to interface with the single wire IC card directly.

There is a further problem with the asynchronous character transmission that makes life difficult for a PC to act as the interface device. The 7816-3 standard defines an error detection and recovery operation (mandatory for T=0) that cannot be managed by the normal PC UART. When the receiver detects a parity error on reception it takes the I/O line to the space or low state in the middle of the first stop bit guard time. The transmitter is mandated to sample the I/O line at the start of the second stop bit guard time period. When the error condition is sensed then the transmitter should retransmit the erroneously received character. Clearly the transmitter cannot be outputting stop bits but must let the line go high during the guard time in order to sense the line state. Given the close coupling normally achieved between an IC card and the interface device one has to question whether this level of error control has sufficient benefits to outweigh the disadvantages. Error

control at a higher level in the OSI model is preferable in this situation and although this could be handled at the application level the T=1 communication protocol applies error control at the frame level.

Answer to reset

After the reset signal is applied by the interface device the IC card responds with an answer to reset. For the active low reset mode the IC should respond between 400 and 40,000 clock cycles after the rising edge of the reset signal. The answer to reset is at most 33 characters (including the initial character) and consists of 5 fields,

- The initial character (TS)
- The format character (TO)
- The interface characters (TA_i, TB_i, TC_i, TD_i,)
- The historical characters (T1,T2....TK)
- The check character (TCK)

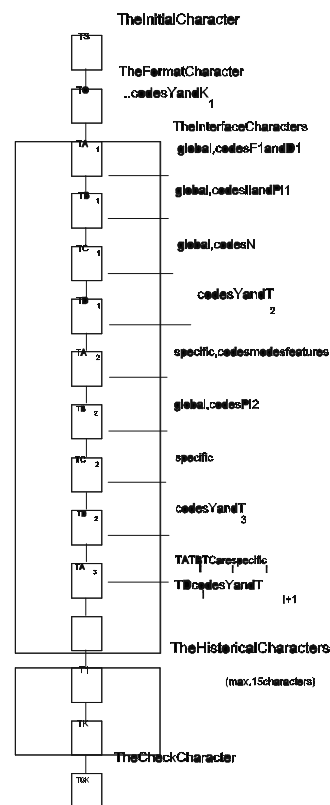


Fig.2 General configuration of the Answer-to-Reset

Each of these fields is sent in order as shown in fig.2. The initial character TS is really a bit synchronisation pattern which may be sent in order to determine the data transmission rate (auto baud rate sensing) and also to determine the sense of the logic. The format of the TS character is shown in fig. 3. This shows the two possibilities of the direct and inverse convention. In the inverse convention where the logic level 1 is the space or low state the most significant bit is transmitted first. With the direct convention where the logic level 1 is the mark or high state then the least significant bit is transmitted first. This means that the selection of the appropriate logic sense will result in the initial character being interpreted as '3F' for the inverse convention and '3B' for the direct convention in hexadecimal coding.

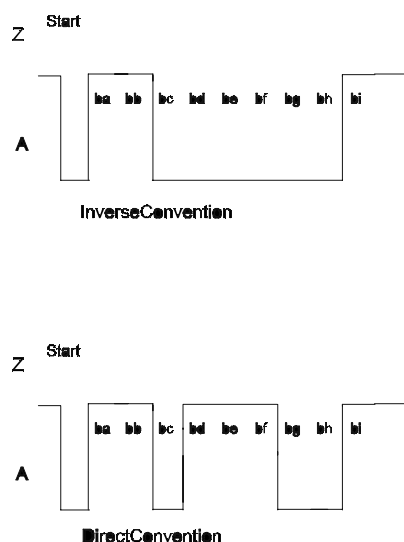


Fig.3InitialCharacterTS

The format character TO provides information necessary to interpret the remaining answer to reset characters. The most significant 4 bits use a bit map to indicate the presence or otherwise of TA₁, TB₁, TC₁ and TD₁. For example if the most significant bit (b8) is set then TD₁ is present in the interface characters field. Similarly the presence of TC₁ is indicated by the state of the 'b7' bit and so on.

The least significant 4 bits of the TO format character give the number (binary encoded) of bytes in the historical field. The use of 4 bits restricts the maximum size of the historical character field to 15 bytes.

The interface characters (TA_i, TB_i, TC_i, TD_i,) are the complex part of the answer to reset. They carry information relating to the available communication protocols as well as the programming voltage and current parameters for the EPROM. There is currently a proposed revision to the ISO 7816-3 to remove ambiguities and to ensure an effective method of operation for changing the protocol type and the protocol parameters. Much of the complexity is brought about by the desire to achieve backward compatibility with commercial implementations of the T=O communication protocol. At the current time there are commercial applications running either the T=O or T=1 communication protocol whilst multi-protocol operation is somewhat scarce.

The proposed revisions to the standard may alter this situation. We will discuss the interface bytes and protocol type selection against these proposed revisions but readers are warned that these recommendations are only provisional.

The interface bytes (which are optional) are defined in fig.4. The T₀ and TD_i characters contain bit maps which indicate the presence or otherwise of the following TA_i, TB_i, TC_i, and TD_i bytes.

The TA₁, TB₁, TC₁, and TB₂ characters are referred to as the global interface bytes and are fundamental to the operation of the card.

$$Work\ etu = \frac{1}{D} \times \frac{F}{f} \text{ sec}$$

An elementary time unit (etu) is the nominal bit duration used in the character frame. Thus as described previously one character frame is equal to 12 etu (1 start etu, 8 data etu, 1 parity etu, 2 guard time etu).

The default values for F1 and D1 are 1 which is defined in the tables to give a value for F of 372 and D of 1. Hence the work and initial etu are the same. At these default values the frequency of the clock should be in the range 1MHz - 5MHz.

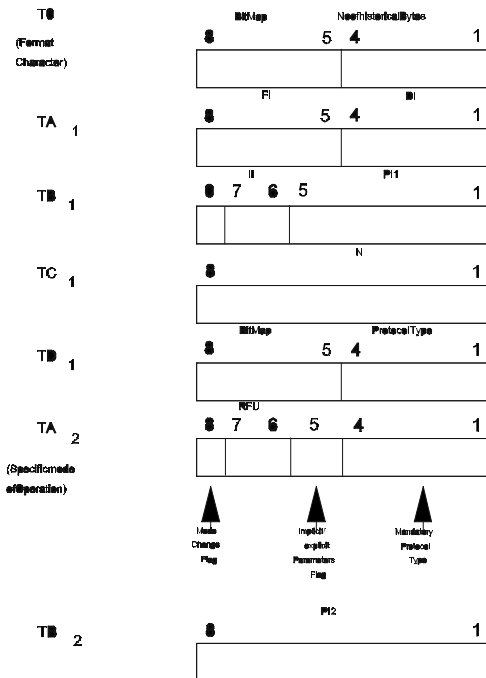
TB₁ is used to define the EPROM programming voltage and current. The value of II and PI1 are used against tables to obtain the value of I mA and P volts. It should be noted that TB₂ is used to define the programming voltage with higher granularity (8 bits instead of 5).

TC₁ provides the value of N which defines the extra guard time to be used between successive characters. N can be in the range 0 - 254 etu. When N is equal to 255 this indicates that the minimum guard time (2 etu for T = 0 and 1 etu for T = 1) should be used. As noted previously the T = 0 communications protocol requires the extra guard time to enable the parity error detection and signalling to be implemented.

TD₁ indicates the protocol type TDI as between 0 and 15,

- T = 0 Asynchronous half duplex byte transmission
- T = 1 Asynchronous half duplex block transmission
- T = 2/3 Reserved for full duplex operation
- T = 4 Reserved for enhanced half duplex byte transmission
- T = 5..13 Reserved for further use (RFU)
- T = 14 Non ISO protocols
- T = 15 Reserved for future extension

It should be noted that Japan uses T = 14 for a National block asynchronous protocol.



TA₁ defines the basic characters of the serial transmission, FI is the clock rate conversion factor and DI is the bit rate adjustment factor. The binary encoded fields are compared against tables supplied in the standard to achieve actual values for F and D as defined below,

$$Initial\ etu = \frac{372}{f} \text{ sec} \text{ (} f \text{ usually} = 3.579545\text{MHz)}$$

The TD₁ byte also contains a bit map that indicates the presence or otherwise of TA₂, TB₂, TC₂ and TD₂.

The proposed revision defines a new use for the TA₂ interface byte which has a special role in the selection of communication protocols and parameters. We will discuss this further in the communications section.

The Historical Characters

The historical characters may be used to convey information relating to the life cycle of the card. There are clearly other possibilities and the use of these characters is still subject to agreement. This subject is being considered further as part of the emerging part 4 of the ISO 7816 standard.

The Check Character (TCK)

The check character should not be sent when only the T = 0 protocol is indicated in the answer to reset. In all other cases TCK is sent as the last character of the ATR. The check character is calculated such that the Exclusive OR of all the bytes from T0 to TCK inclusive is equal to zero.

Next Edition:

We will continue with a discussion of the T = 0 and T = 1 communications protocols along with an explanation of protocol type selection (PTS).

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 _____

Name _____

Position _____

Address _____

Company _____

Address _____

Card No. _____

Expiry date _____

Tel. _____

Signature _____

Fax. _____

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.

Berlin Pilot Starts Next Year



Slide 1



Slide 2

An integrated Smart Card prepayment system is to be piloted early next year with Berlin's transport service, the BVG.

Called the Berlin Card, it will be based on a multifunction processor chip card offering an "electronic purse" function plus a range of functions for accessing computer systems and buildings or premises.

The EEPROM card from Siemens Nixdorf uses two cryptographic symmetrical algorithms, - Smart Card Algorithm (SCA) and Data Encryption Standard (DES).

Initially the prepayment card will be used to purchase tickets for local travel on selected buses and trains. The card can be credited with a maximum of DM 999 at attended terminals connected to the system operator. Bank cards will be accepted at these terminals in addition to cash.

Debiting will be carried out at mobile, attended

ticket printers supplied by ALMEX using machines upgraded by the addition of Smart Card readers and therefore able to run the debit electronic purse function. Data resulting from transactions will be collected in a data exchange module integrated in the machine.

At BVG headquarters, this data will be read in, edited for accounting and statistical purposes and then transferred to the accounting and clearing system via a PC equipped with file transfer. At a later stage in the project the debit function will be extended to stationary ticket machines.

After successful piloting with the BVG, it is planned to introduce the card as the Berlin Card for use with other service providers, possibly including public institutions such as museums, libraries and swimming pools etc.

Taxi companies have also expressed interest in the card, principally because the need to carry cash is reduced thus lowering the security risk, and because with a prepaid card the payment is guaranteed.

Contact: Manfred Reichherzer, Siemens Nixdorf, Munich, Germany - Tel: +49 89 636 2471.



Christmas Shopping made easy using JerseyCard's new electronic purse Smart Card.