Swiss Electronic Purse to go Nationwide in 1995

Postcard, the Swiss PTT Electronic Purse project has fulfilled expectations during trials in Biel/Bienne, and it is planned to extend it throughout Switzerland in 1995 with enhanced technology.

The trial has proved the Postcard to be a success technologically and popular across a broad section of the community, particularly amongst young people who know how much they are spending. Although the trial officially ends at the end of this year, the Postcard will continue to be used in Biel until a more advanced system is introduced.

Continued on page 123

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 12 - IC Card Security Life Cycle

CONTENTS

Swiss PTT Electronic Purse

Continued from page 121

The driving force behind the electronic purse concept was the move towards standardizing and simplifying operations in the plastic money sector. The PTT was well placed to lead the initiative because of the suitability of a range of services it offered which would fit the payment card concept and as the bulk payment operator with its Postgiro service. There was also concern about the high cost of handling cash and the risk of robberies, but the primary objective was to reduce the number of cards needed to pay for all PTT transactions and services to just one or two.

Postcard, which was issued free of charge, was launched in the trial town of Bienne on 29 November using the Bull CP8 8K bits EPROM multifunction rechargeable payment card for the cashless payment of goods and services, and for withdrawing cash at Postomat dispensers.

Bienne was chosen because it was an ideal size (50,000 inhabitants), had a broad range of retailers, a wide variety of public transport systems - trains, postbuses, urban transport networks, lake steamers and cable cars, adequate Postgiro coverage, and a favourable local authority response.

Field trial

It was the first ever field trial of a card combining a variety of features such as debit, prepayment and identification functions.

During the trial 13,000 people used the Postcard for cashless payments at 150 sales points for debit transactions on-line and at 70 electronic purse terminals in shops, restaurants, petrol stations, the municipal swimming pool, and cinemas.

The card could also be used to make calls from public telephones, at ticket machines for parking and bus and rail travel, purchase postage stamps at post offices, and withdraw cash at Postomat cash dispensers.

Postcard turnover averaged 120,000-130,000 Swiss francs every day.

Future development

The technical requirements for a nationwide launch of the Postcard are currently being prepared. The Bull 64K bits EPROM card, and later the Bull TB100 2K byte EEPROM card, used in the trial, will be replaced by another card for a further trial expected to start in 1994/95. The Postcard will then be extended throughout Switzerland.

Contact: Beat Tschannen, Swiss PTT, Switzerland - Tel: +41 31 62 54 45.

LT Bus Trials Starts August

London Transport's Smart Card bus ticketing trial is scheduled to start on Saturday, 28 August at the English Bank Holiday weekend.

It will involve 200 buses operated by five companies in the Harrow area of London being equipped with Smart Card readers from AES Scanpoint and Westinghouse Cubic.

Two types of electronic ticket will be available. Stored value fare cards which can be purchased from corner shops and bus stations. The cost of each journey will be deduced from the card by the reader. The other card will be the smart bus pass which will replace the photocard carried with Trave1cards or Bus Passes. Passengers will present the Smart Card to the reader which will check its validity and record the start and intended length of the journey.

The contactless cards supplied by GEC Card Technology is held near the reader to be scanned and can be left in wallet,

handbag or briefcase.

If the 18-month trial is successful it is planned to extend the system throughout London. Apart from savings through reduced ticket fraud and quicker boarding times, Smart Card ticketing is seen as a solution to the problems of accurately allocating ticket revenue when London's bus services are deregulated in 1995 and some 50 different operators will be offering services in the capital.

Contact: Roger Torode. STV Project, London Transport - Tel: +44 (0)71 918 3285.

VeriGem to Market EP Worldwide

A new joint venture company, VeriGem, formed between VeriFone, Inc., of Redwood City, California, USA, and Gemplus Card International, of Gemenos, France, plans to develop and market Smart Card Electronic Purse applications worldwide.

SmartCash will be the name for VeriGem's electronic currency solutions based on rechargeable Smart Cards with a stored value that can be used instead of cash.

The company quotes "The Nilson Report," as showing US consumer cash transactions numbered 70.9 billion in 1992 which were valued at more than $1.6 trillion, and says the market for automating cash transactions both in the US and around the world remains virtually untapped.

Terms of the joint venture are not disclosed, but VeriGem will be an independent company funded by VeriFone and Gemplus and will pursue SmartCash partnerships with financial institutions and payment processing service providers, as well as with large retail chains and franchise operations worldwide.

As an example of the speed, convenience and flexibility of SmartCash, the company says the SmartCash card could be used in a ticket kiosk to pay for travel or parking, purchase a snack from the office vending machine, pay for lunch in a fast food restaurant, and for shopping in the supermarket on the way home. Here you would use the card in the "SmartLane" - the express service lane for SmartCash users - and have your frequent shopper bonus points automatically stored on the card.

Benefits

Benefits for the consumers are seen as quicker transaction times and the convenience of carrying a card instead of a bulky purse or money clip. Also the card can easily be revalued.

Merchant costs associated with handling cash - counting, transport, insurance, and loses due to error or theft - can be significantly reduced. It is estimated that cash handling in supermarkets accounts for nearly 2% of the total transaction value. Check-out times can also be accelerated, increasing both sales and customer satisfaction.

Banks can benefit from SmartCash card issuance revenue, transaction and card revaluation fees, and reduced currency-handling costs.

The joint venture represents a long-term strategic initiative, an investment in the future of both partners and of the electronic payment business, says Harim Tyabji, Chairman and Chief Executive Officer of VeriFone. "We envision SmartCash as the currency for the information age, a fast and convenient cash alternative," he said.

Dr Marc Lassus, President and Chief Executive Officer of Gemplus, says: "We expect VeriGem to play a leadership role

in driving market acceptance of Smart Card technology worldwide, and to deliver the benefits of SmartCash to consumers, merchants, banks and service providers on a global scale."

VeriFone has shipped more than 2.9 million Transaction Automation systems which have been installed in over 70 countries, while Gemplus card production currently exceeds 12 million cards per month and its distribution network covers more than 50 countries.

Citizen Card for Italy

The Bank of San Mareno, Italy, has ordered a "citizen services" system to be developed and supplied by Bull Italy. The contract includes the supply of 40,000 SCOT 60 Smart Cards, and system applications involve electronic payment, health, municipal and tourist services.

Vice President for SPOM Japan

Nick Cahn has been appointed Vice President of SPOM Japan, the joint venture company formed by Bull CP8 and Dai Nippon Printing. Previously he worked with Bull in England and then with Bull CP8 in France where he gained a broad experience of the European Smart Card market.

SPOM Japan tripled card sales and doubled sales revenue last year. Orders included one for 500,000 store loyalty cards.

SNCF Orders Ticket Machines

France's national railway operator, SNCF, has ordered automatic ticket vending machine systems for its regional rail networks from the Urban Terminals & Systems Division of Schlumberger Technologies. The first phase of the contract calls for 200 ticketing machines to be followed by three further optional phases of 300 systems each.

Due to the large disparity between regional tariffs, the ticketing machines have been designed to accept all modes of payment including bank/credit cards, banknotes/coins, and Smart Cards.

The first systems will be installed in the Mid Pyrenees region, which will provide feedback to Schlumberger to bring the ticketing system to full production status.

The order is part of a major modernisation programme for the regional rail network which is used by around half a million passengers a day. SNCF studies have shown key differences in ticketing for regional rail passengers compared with main line travellers, including:

* 85% of regional travellers buy their tickets at the time of departure.
* 50% of tickets are issued for travel to work, schools and colleges.
* 50% of all tickets are for non-regular journeys.

This information has been used in developing a sophisticated ticketing system capable of satisfying the tariffs of SNCF regions with the capability of allowing the system to deliver tickets for other forms of transport such as the Metro and buses. On-line connection to SNCF's computer network simplifies management and the gathering of sales statistics.

The ticketing machines are heavily protected against weather conditions and vandalism and can be located externally to station offices to operate 24-hours a day.

Contact: Bertrand Dussauge,

Marketing Communications Manager, Schlumberger Technologies, France - Tel: +33 1 47 46 62 47.

GLOBULL Card for Nevers

Three thousand young children in the French town of Nevers (population 45,000) about 150 miles from Paris, will soon be using Smart Cards to pay for school meals and for morning and afternoon kindergarten services.

To computerize its "social and educational affairs," the town has entered into a three-year partnership with Bull CP8 aimed at turning the application into a European technological showcase. The scheme is due to become operational after the school summer holidays.

Based on elements that existed, for example, PASCAM payment manager and SCOT Smart Cards, and working with partners such as Maeis/Tegelog for multifunctional software, and Smart Ingenierie for readers and terminals, Bull CP8 has designed and acted as lead contractor in developing a system to help towns with populations between 10,000 and 100,000 in their management of school meals, creches and nurseries, pre-and post-school study facilities, and a range of municipal services.

Bull believes that its investment in the computerization of social and educational affairs is central to the greater concept of the city card.

Contact: Yves Girardot, Bull CP8, France - Tel: +33 1 39 02 44 00.

Smart Loyalty Schemes

Sales Promotion Systems, a consultancy company specialising in electronic sales promotions, are offering Smart Card loyalty schemes among a range of marketing systems.

They are working with companies in three main areas - the retail, fuel and leisure industry sectors - on loyalty and marketing applications and also prepayment card schemes.

Business associates include French supplier of Smart Cards and systems, Schlumberger Technologies.

Contact: Mike Hawkey, Director, Sales Promotion Systems, England - Tel: +44 (0)442 235600.

Student Card in Italy

Olivetti Sixcom, Italy, has designed a system for the automated handling of services offered to students within the various university structures - accommodation, catering, cultural and recreation facilities, as well as the handling of study grants, contributions and social security payments.

Known as the Carta Centodieci, the system is based on the C-Less card - a contactless card from AT&T - which is distributed to students and university staff.

Organisations involved are the University of Bologna, the Association for the Right to Study (ACOSTUD) which deals with the agreements with certain categories of student; and the financial organisation Cassa di Risparmio di Bologna, which deals with the organisational, accounting and administrative aspects.

As the card can carry a magnetic stripe, it can be used as a means of payment in the Bancomat cash dispenser service. It is also possible to integrate local applications such as the issue of local authority certificates or for health service purposes.

ID for students

The card serves as an ID for students for the bank and university organisations and authorisation for payment by means of the identity and category check of the student.

In practice, the bank deals with applications to use the service and issues the Smart Card personalised with information on each student as issued by the university or ACOSTUD.

Students with the C-Less/Bancomat card can directly debit the sums paid to their current accounts. Those who have no current account pay a sum in cash to an authorised branch of the bank, and this is debited to the card.

Advantages offered by the automation of student services include a reduction in administration for the service handler, issuing body and ACOSTUD; and greater security in determining the right to use the service and contributions.

For the issuing bank, the cards offer further advantages, including:

* the possibility of increasing the number of students holding current accounts.

* the handling of finance from the Right to Study services, such as study grants, social security payments, etc.

The system comprises a group of workstations distributed in canteens, libraries and accommodation and recreation areas. Each workstation is connected to the peripheral devices which handle the interface with the operator and cardholder, and also to the bank's host computer.

In use the student inserts the card and, as an option, his secret PIN code. If the data is correct the payment of the service selected is completed off-line.

The Carta Centodieci was used in the experimental stage of the project by the students in a canteen in the centre of Bologna. Now the first 15,000 of the 30,000 cards involved in the service are currently being distributed.

Contact: Luciano Cavazzana, Olivetti Sixtel, Italy - Tel: +39 2 3192 355.

New 16K bytes Chip from Oki

Oki has announced the MSM627160, its new 16K byte EEPROM CMOS chip for IC cards.

Technical details:

ROM	14336 bytes
EEPROM	16384 bytes
RAM	448 bytes
Clock frequency	5.0 MHz max
Instruction execution time	800 ns min at 5.0 MHz
No. of instructions	294
Power supply voltage	5V± 10% (single power supply)
No.of pins	5
Operating Temp. range	0 to 70 degrees C

British Rail Denial

British Rail's Network South East has denied a report in London's Evening Standard newspaper last month that it has shelved plans to use Smart Cards in automated fare collection.

Commenting on the article headed "BR ditches plan for smart card tickets," a spokesman said: "We are still investigating the possibilities," adding that a decision was not imminent.

"Once we are satisfied it can serve a useful purpose for us then we will make a decision depending on available finance to put it in place."

With both the London Transport buses and London Underground about to trial Smart Cards, BR is under some pressure to fall into line.

BR tickets can include travel on London Underground with entry and exit controlled by inserting the ticket in barrier control machines, while BR relies on ticket inspectors at platforms and/or on trains.

Innovatron Group Expands

Axime has sold its subsidiary ATM, which specialises in the distribution, installation and maintenance of payment terminals, to the Innovatron Group which is continuing its expansion in the electronic transactions sector as a system integrator. ATM has seven regional technical centres throughout France.

Contact: Francoise Marceau, Innovatron Group, France - Tel. +33 1 40 13 39 00

Saab/Peek Alliance

Saab - Scania Combitech AB and Peek Plc have formed an international trading alliance in the Automatic Vehicle

Identification (AVI) market for road pricing and fleet management applications.

Combitech develops and markets equipment for automatic identification and short range communication at toll plazas, as well as systems designed to improve the operating efficiency of large vehicle fleets. Products consist of microwave-based transponders (electronic tags) which are placed in vehicles, and transceivers located on the roadside.

Peek's product range includes motorway control and communication systems, urban traffic control systems and public transport management and information systems.

Geographical areas affected by this alliance in the short term will be mainly Scandinavia, Great Britain and The Netherlands.

Contact: Ove Salomonsson, Manager, Marketing & Sales, Saab-Scania Combitech AB, Sweden - Tel: + 46 36 19 40 00

Schlumberger SmartCrypt Orders

SmartCrypt, the new Smart Card encryption system for pay - TV from Schlumberger Technologies (SCN February 1993), has won orders in Belgium and France.

RTBS will use SmartCrypt in a Belgian terrestrial broadcast application, while Reseaux Cables de France, which is one of the largest independent cable network operators in Europe and currently serves 10 French and has 250,000 subscribers, will start using SmartCrypt this month.

The new encryption system from Schlumberger frees cable and satellite TV broadcasters from traditional subscription - based methods of charging.

The SmartCrypt system includes a programme encryption encoder, a set - top decoder, and an administration system. The decoder has the unique feature of twin Smart Card readers - one card functions a detachable security processor providing state-of-the- art scrambling technology and security. As this card can be changed inexpensively, this provides an extra level of long term protection against piracy of programme signals. The second card can be used for a wide variety of payment options. It holds electronic tokens which entitle consumers to view particular programmes, or view for a unit of time, and transfers these rights to the primary Smart Card once inserted into the decoder.

This Smart Card access control mechanism makes it possible for service providers to sell programmes in highly targeted forms, as viewing rights to, for example, the latest film release, a sports competition, or an opera season.

Electronic " Tickets"

A particular attraction is that it makes it feasible to purchase electronic "tickets" to these events in the same way as you would buy a newspaper - over the counter in retail outlets in the shopping centre, station or airport. Alternatively, access rights can be sold as basic units of viewing time which are cancelled as they are used.

The product makes it possible for TV channels to be composed of a core transmission provider, publishing programme material from a very wide collection of independent producers, and the rights holders can be credited with the royalties from each film or event viewed.

Contact: Yvette Ramos, Marketing Product Manager, Schlumberger Technologies, France - Tel. +33 1 47 46

59 61, Fax: +33 1 47 46 68 49.

Danmont trail Report

Danmont will publish a report in September on the trail results from Naestved as well as the background for building up this Intersector Electronic Purse.

The report will cover the six - month trail period from a technical, marketing as well as a business point of view. It will be available from 1st. September price DKK 4,800 (for orders received before 30th. August) or DKK 6,600 for orders after 30th. August.

Contact: Henning Jenson, Managing Director, Danmont, Denmark - Tel: +45 4344 9999.

Philips Health Card Order.

TRT Philips Smart Cards & Systems has won an order to deliver 200,000 additional cards to the French health sector programme SESAM/VITALE (System Electornique de Saisie de L'Assurance Maladie).

This programme has now validated a number of concepts in the use of electronic prescriptions using Smart Cards and is now ready to be deployed over four of the initial cities where large scale trails were carried out - Boulogne sur Mer, Bayonne, Charleville Mezieres, and Rennes.

In addition to supplying the 200,000 cards which will have M9 masks (a Bull CP8 development), Philips will supply 1,5000 Minitel terminals.

Philips says it will deliver 4 million cards to the health sector in 1993, and estimates it will deliver in excess of 10 million to this sector in 1994, mainly to the German market.

Contact: A J Selezneff, International Marketing manager, TRT Philips Smart Card & Systems, France - Tel: +33 1 41 28 75 84. Fax: +33 1 41 28 79 68

OSCAR - A Short Review

OSCAR (Open Access Routine) is a Smart Card operating System written by GIS for the OKI MSM 627xx series of microcontroller units. The IC Card as supplied by GIS incorporates the MSM 62785 chip which has 8K of EEPROM. In order for prospective developers to get hands on experience GIS supply an evaluation kit with the following components,

OSCAR Cards (X2)
IC Card Reader
Utility and library software. (On disk for a PC)
Various manuals.

Perhaps the most pleasing part of the kit was the very neat IC Card reader. This reader is as small as they come and takes all its power off the PC serial port.

GIS propose two main functions for the OSCAR Card,

-general purpose operating system
-secure processing for transaction, authentication and authorisation.

As they point out OSCAR could be used for any application requiring the storage and retrieval of small to medium volumes of data with restricted or general access. Whilst OSCAR offers a number of security services (encipherment, decipherment and message authentication) it must be appreciated that it might not be appropriate for applications where a higher level of data processing ir required.

The software supplied with the

evaluation kit will allow the user to examine and modify the cards supplied from a menu driven utility. A number of C libraries are supplied along with all the source code (including the DES algorithm). The two IC Cards supplied are development devices and allow the user to initially format and re-format as required.

OSCAR Operating System Commands

OSCAR commands are implemented in accordance with ISO 7816 - 3 using the T=0 protocol but are not in conformance with the emerging ISO 7816 - 4 (still in dispute). The commands are shown below.

Free Card Space	CLA 10h	INS 00h
Card Directory	CLA 10h	INS 02h
Free File Space	CLA 10h	INS 04h
File Directory	CLA 10h	INS 06h
Select Virtual Card	CLA 11h	INS 00h
Select File	CLA 11h	INS 02h
Select A Password	CLA 11h	INS 04h
Select A MAC Key	CLA 11h	INS 06h
Make A Virtual Card	CLA 12h	INS 00h
Make File	CLA 12h	INS 02h
Remove File	CLA 12h	INS 04h
Change File Attributes	CLA 12h	INS 06h
Read From File	CLA 13h	INS 00h
Encrypted File Read	CLA 13h	INS 02h
Read Result	CLA 13h	INS 04h
Read Version	CLA 13h	INS 06h
Write To File	CLA 14h	INS 00h
Encrypted File Write	CLA 14h	INS 02h
New Password	CLA 14h	INS 04h
Select Enc Key	CLA 15h	INS 00h
Encrypt Data	CLA 15h	INS 02h
Generate MAC	CLA 15h	INS 04h

Although users can write their own programs to evaluate the card (C libraries provided) the evaluation kit supplies two utilities,

OSC - FMT. EXE , Explore . EXE

the first utility is used to format (or reformat) the IC Card and the second utility can be used to evaluate the command structure. The explore utility operates as a menu driven program that maps the basic commands as shown in the table.

OSCAR is really a file management system with considerable flexibility. The core concept is one of virtual cards where number 255 acts as the root used by the operating system. This virtual card contains 9 files for file and memory management.

Users may create a number of virtual cards (set by the distributor) which are used for the data storage domainds. Within each virtual card you can set up files and set their attributes (free, password, access control, locked). The password system allows the use of 6 separate codes for each virtual card (numbered 1 to 6). The checking password command (present password) is a little messy because it insists on the use of enciphered passwords (to allow for remote access). This means that you must first establish a session key. The select key command takes 8 bytes from any nominated file and then exclusive OR's this with a pseudo random number. The random number generator is seeded by the 2 bytes in file number 4 (root virtual card number 255). The principle here is that the correspondent knows the nominated key file and is provided with the random number in order to generate the session key.

Summary

The OSCAR card allows a flexible file management system to be developed and tested. The DES algorithm can be used for encipherment and decipherment of data but apparently only in electronic code book mode (ECB). The message authentication routine (according to ANSI X9.9) provided is fairly slow taking some 5 seconds to handle a 255 byte file. The key management system could usefully be improved depending on the particular application. Overall however this is a professionally produced product that will allow users to to get hands on experience in a relatively painless way.

Contact: Ramanuj Banerjee, GIS Ltd, Cambridge, England. Tel: 44-(0)223-462200

Finnish Electronic Purse

The Finnish Electronic Purse system, called AVANT, was officially inaugurated last December with non-reloadable memory cards for use only in telephones. The next stage will be the introduction of the first reloadable Smart Card application for parking in Helsinki to be followed with other applications being added to the card.

AVANT has been developed by Setec Oy and will be operated by a new company, Toimiraha Oy, set up by the Bank of Finland. Setec Oy, also a subsidiary of the Bank, is the manufacturer of the cards and some equipment including secure terminals and in-car parking meters (See this page).

The city of Helsinki has ordered forty thousand meters which motorists will purchase. The retail price has not yet been decided.

Distribution of the cards will be handled appropriately by petrol stations as the first application will be for parking tickets, and by a kiosk chain which has easily accessible sites in shopping centres and railway stations etc. Cardholders will initially pay for the amount they wish loaded onto their cards in cash. The next stage will be to have automatic loading in ATMs and perhaps by EFTPOS terminals and possibly by commercial banks. Eventually it may be possible to use home banking facilities to load the card using the telephone and a modem.

Discussions are taking place with some 50 telephone companies in Finland - one justification for having a single card - and most have already agreed to join the scheme. Talks are also going on with the Finnish Post Office, Municipalities and retailers.

Fred Granberg, International Operations Manager Smart Cards, of Setec Oy said: "We are opening up a nationwide reloadable card system starting with public pay phones and parking which we believe will spread quickly to other cities. The next steps will be other municipal services, public transport (buses, trains and metro), retailers, retail chains, petrol stations, and road tolls."

The card currently being used for instance in the city of Tampere for the telephone application is disposable. The first application using rechargeable cards for parking in Helsinki will be the Setec Oy EEPROM microprocessor contact card which conforms to ISO ID1 dimensions. It will feature the AVANT logo shown above.

Parcard In-car Parkmeter

The Parcard in-car parkmeter developed by Setec Oy in Finland is easy to use and has several advantages likely to be attractive to municipal authorities responsible for providing parking as well as to city planners.

For a start it eliminates the need for unsightly coin parking meters and ticket machines, expensive maintenance and repairs due to breakdowns, vandalism and theft; and coin collecting and handling.

The system provides for the supervision of parked vehicles. The parking warden carries a control device which copies the in-car parking meter's display through infra-red communication, even in the dark.

Motorists do not have to carry coins, dash back to their vehicle to put in further coins, or walk back and forth to a ticketing machine or to a kiosk selling parking vouchers. A further advantage is that the motorist pays for the exact time parked and does not drive away annoyed at having paid for parking time not used.

Parcard is easy to use and payment is carried out inside the vehicle. The in-car meter can be preset with different charges for up to 10 zones which may be intended either for long- or short-time parking. The driver inserts the Smart Card in the meter, selects the parking zone number and required parking time (with a safety margin thus avoiding parking fines), pushes the start button and removes the card taking it with him.

On returning to the car the driver presses the stop button and recovers the remaining parking time.

A timer function is included in the Parcard meter so that motorists can park early in the morning and set the time when parking becomes chargeable.

The meter, which is a Smart Card reader, includes a security module and communication is protected by an encryption algorithm. The card can only communicate with the security module in the meters and, as the card is not personalised, it can be used in any Parcard meter.

A potential city card

Several parking providers can use the same system and be credited for the motorists who park on their sites. Neighbouring cities can co-operate under the same concept increasing the attraction for motorists. The same cards can be used in private car parks, the owners of which would enter into a clearing contract with the city.

As the reloadable Smart Cards are based on the principle of a general-purpose electronic purse, the system could be expanded to cover municipal services, such as public transport, road tolls, entry to museums and to make other small cashless payments, giving it the potential to become a city card.

Contact: Fred Granberg, Setec Oy, IC Card Division, Finland - Tel: +358 0 89411. Fax: +358 0 8786133.

First IC Card in Vietnam

The Vietcombank has placed orders with Bull CP8 for SCOT 60 cards, TLP 224 NV card readers, and PinPadLINKs, making it the first to use an IC card in Vietnam.

Philips Cards for German AFC

Philips are supplying Smart Cards for an Automatic Fare Collection (AFC) system in the German towns of Kempten and Reutlingen.

Requirement for an open MAC

The danger of companies developing various multi-application cards (MACs) could lead to a fragmented market of incompatible cards and inhibit the growth of Smart Card technology.

This, basically, is the view of a number of companies involved in the IC chip card industry who met in Hamburg, Germany, this month under the chairmanship of H D Kreft and J Dethloff, of Angewandte Digital Elektronik GmbH (ADE) in an attempt to harmonize the Smart Card market.

Market penetration is seen as depending on:

* One card which is suitable for all the services of today's different cards.

* Newly issued Smart Cards being connectable to the international data network of the well-established and stable international magnetic stripe card system.

* The Smart Card being an open and highly secure system for the different card service suppliers and card issuers.

Compatibility

To achieve this aim, Kreft and Dethloff have developed RICH which stands for a "Reference for International Card Harmonization" (patent applied for). This software is aimed at ensuring the compatibility of multi-application cards (ie that programs in both the card and the card terminal conform to ISO 7816.)

In a general description of RICH Version 1.0, ADE examine the closed MAC and the open MAC market solutions. In the former, the cardholder can use his card only for applications of the specific service provider pool. In contrast to this

is the concept of the open MAC which is open to all the different applications of different service providers on one card instead of users having to carry different cards for different services.

The description says that RICH makes sure that both the closed and open MAC concepts meet the standards and can communicate in a pre-determined and foreseen manner.

Among the perceived benefits of RICH are:

* assuring buyers that there is one standardised international compatible product line backed by different suppliers.

* supplying the card market with a tested Smart Card software set.

* reducing development risks and costs for different component manufacturers.

* Enabling IC device and equipment manufacturers to serve the market with standardized compatible Smart Cards.

* Enabling system houses to start work without needing to concentrate activities on the interface level between cards and terminals.

RICH Coupler

In addition, the RICH concept describes a RICH Coupler capable of operating both contact and contactless Smart Cards through a single slot.

Further information on RICH can be obtained by contacting Angewandte Digital Elektronik GmbH, Bundesstrasse 25, 2051 Brunstorf, Germany - Tel: +49 4151 8890-0. Fax: - +49 451 8891-29

New Card from France Telecom

France Telecom's PASTEL card (Passeport Telephonique) which enables users to make calls from public telephones and have the charges billed to their home or a specified telephone account, has been renamed the Carte France Telecom and has a new logo.

Used by about one million people in France, it will continue to be available in three versions - National, International and Selection, the latter being programmed to call a maximum of ten numbers. France Telecom aimes to increase this market to 1.6 million cardholders in 1996.

Suppliers of the Carte France Telecom are Bull CP8 and TRT Philips.

Mars Card Trial

Mars Electronics International are trialling a cashless payment system for vending using Gemplus GPM416 416 bits EEPROM memory cards. The trials are taking place on working sites - a car showroom, a health centre and a factory.

The Mars Card system reduces the need to carry coins or search for the right change. It can be programmed with "free vends" to extend courtesy services to customers or staff.

The system can be installed on a vending site within a matter of hours either in card-only mode or with a Mars Electronics changegiver offering both card and coin acceptance. It is compatible with all popular makes of vending machine.

The aim of cashless vending systems is to eliminate the inconvenience and risk of coin handling, and a selling point is a reduction in vandalism, costly repairs and extensive downtime as there is no cash to attract thieves. But the Mars Card System offers in-machine revaluation of cards whereby customers can revalue the card directly on cash/card machines by paying cash into the machine. The company sees the facility of keeping cards in credit as keeping the vending machines in use and a convenience for customers.

Management information is provided by the system, for example, accurate cash audits show how much money is in the cash box at any point, and information is provided on the number and value of free vends given, thus helping to control subsidies.

Contact: Sales and Marketing Department, Mars Electronics International, England - Tel: +44 (0)734 697700. Fax: +44 (0)734 692668.

TECs Look at a Standard System

Three Training Enterprise Councils in England have joined together to implement a Smart Card scheme with a common data structure. While TECs like Dudley and South London have launched their own Smart Card schemes, Birmingham, Stockport and High Peak, and Hertfordshire, have joined forces. About 1,500 cards supplied by McCorquodale, are expected to be issued for the trial in the three areas.

The cards will contain information on the cardholder's training plan, a value expressed in money or hours, attendance, an event log ie when issued, fixed data such as name and address, employment history, qualifications, and training achievements which will be virtually a mini c.v.

The cards will be issued in a total of five different designs.

Contact: Alan Andrews, Birmingham TEC, England - Tel: +44 (0)21 622 4419.

Oki Distributor in UK

Card Systems (UK) Ltd has been appointed a franchised distributor for the United Kingdom by Oki Semiconductor.

As the sole UK distributor for Omron cardware products, Card Systems' agreement with Oki will enable the company also to supply and support the Oki MSM627 series of Smart Cards and the OSCAR Smart Card operating system.

Contact: Guy Boxall, Director, Card Systems (UK) Ltd, England - Tel: +44 (0)273 459034. Fax +44 (0)273 459123.

Danmont Card for Copenhagen

Following successful trials in Naestved, plans are now being made for a national roll-out of the Danmont prepayment card, starting in the Danish capital, Copenhagen, on 2 December.

This is the day when a sizeable number of public payphones and parking meters will be ready to accept the Danmont card instead of coins. The card can be used for a variety of small-scale purchases and it is likely that other services will quickly be available for cardholders.

At present the cards are disposable when the full amount has been drawn form the card, but a rechargeable card should be available in 1994/95.

Contact: Henning Jensen, Managing Director, Danmont, Denmark - Tel: +45 43 44 99 99.

Smart Card Diary

ESCAT 1993 (European Smart Card Applications & Technology) Conference, Hotel Kalastajatorppa, Helsinki, Finland, 1-3 September.

Topic areas include telecommunications, financial (electronic payments), transportation (and multi-purpose cards), and health applications. Contact: Eija Ohrnberg - Tel: Finland +358-0-752 3611. 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: Simon Reed, Charta Associates, England - Tel: +44 (0)442 231844. Fax: +44 (0)442 236604.

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.

European Payments '93 (EFTPoS & Home Services), Sheraton Hotel, Edinburgh, Scotland, 16-18 November.

A tutorial on biometrics and cards will be held before the conference which includes a day devoted to remote services. Contact: Paula Biagioni - Tel:

+44 (0)41 553 1930.

Bull Announce Two New Cards

Bull CP8 has announced two new cards at either end of its range. The SCOT 30 DES 2K bytes EEPROM card is described as ideal for applications that require a low cost ISO standard card with a small protected memory which, the company says, is a combination that ordinary memory cards cannot offer.

Applications being targeted are for city, loyalty, club membership, company, leisure, amusement park, customer and subscriber cards, and as a reloadable prepayment card.

Card details:

Type	Contact
Fabricator	Bull CP8
Dimensions	ISO ID1
Contact location	Front
Chip manufacturer	Motorola
Chip reference no.	SC242
Memory type	Microcontroller+memory
Memory capacity	
Mask ROM	3K bytes
EEPROM	2K bits EEPROM
RAM	128 bytes
Standards	ISO 7816-3
Comms protocol	T=0
Security	PIN
Cryptography	DES

At the other end of the scale, the new SCOT 1000 DES offers 8K bytes of EEPROM and is aimed at applications requiring a large re-writable memory. A "turbo" option gives communication at up to 115-200K bits or 12 times faster than current cards while conforming with the ISO T=0 standard protocol.

Card details:

Type	Contact
Fabricator	Bull CP8
Dimensions	ISO ID1
Contact location	Front
Chip manufacturer	SGS-Thomson
Chip reference no.	ST16F48
Memory type	Microcontroller+memory (SPOM chip)
Memory capacity	
Mask ROM	16K bytes
EEPROM	8K bytes
RAM	288 bytes
Standards	ISO 7816-3
Comms protocol	T=0
Security	PIN
Cryptography	DES

Smart Card Tutorial - Part 11

The Development Environment

I can not help thinking that the semiconductor manufacturers have missed a trick when it comes to the ICC development environment. It is not easy for application developers to independently create their own schemes due to the somewhat closed shop approach of the majority of semiconductor manufacturers and card fabricators.

In the mid 70's the microprocessor was almost unheard of, then suddenly over just a few years the world was inundated with microprocessors for everything. A position that today we all take for granted. The course of events at the time seemed so obvious with the aggressive marketing of specifications, application notes and simple evaluation or development kits by the major semiconductor houses. At the time I remember the superb development packs produced by Motorola for their 6800 microprocessor. But today we seem to have the reverse, getting information is worse than getting blood out of a stone. With one particular semiconductor manufacturer (not Motorola) I was personally bounced from office to office for a week just to find out the die size of a chip in current production. After numerous faxes and telephone calls the question was never answered. Do they really expect me to have to get out a ruler. (Note: any school laboratory is perfectly capable of removing the resins covering the die assembled as part of the chip micromodule).

If I assume that the reaction to my approach to the suppliers is typical then new potential users must be finding it difficult just to obtain the basic chip specifications. Smart Card News decided to produce an article comparing the technical specifications of the major semiconductor suppliers offerings. After one month and numerous reminders some companies have still failed to supply even the basic information.

In terms of development hardware and software whilst most chip manufacturers have some form of offering they are often hidden away to deter all but the toughest enthusiasts. The problem seems to be the distribution route for Smart Card chips. Those organisations undertaking a card fabrication role are the intermediary between the user (here the application provider) and the chip manufacturer. One of the major roles of the fabricator is to develop and supply complete application systems and not surprisingly they are often less interested in the do it yourself brigade. However there is a need for both and it seems clear to me that the first chip manufacturer to get his act together will probably lead the field in what is becoming a rapidly emerging market with enormous potential.

In this part of the tutorial we will examine the various approaches to application development based on tools that are available in the marketplace. In separate articles we will review some of the standard offerings in more detail.

We have often discussed the basic components of the IC chip (reproduced in fig. 1). For now we need to remember that the core operating system resides in the ROM memory and this will be executed on reset. The EEPROM memory will hold the application data and optionally additional application programs. It should be noted here that we have tended to ignore the use of non volatile EPROM memory. This memory is limited to write once and is therefor not as flexible as EEPROM memory. However it can be used to store application programs and to store data that is not required to change and for which there is sufficient capacity to meet the application requirement. In

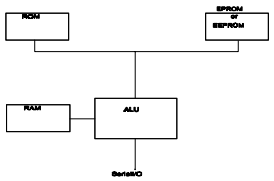

Fig1.TheICBasicArchitecture

our discussions readers may consider the use of EPROM memory as appropriate in some application scenarios. The advantage of EPROM memory is that it occupies a smaller area than the equivalent EEPROM capacity. Accordingly this results in a lower cost device.

The RAM memory is the working space used by the application whether executing in ROM or EEPROM. From a developers point of view it is important to realize that the ROM memory is fabricated as part of the chip manufacturing process. This requires a more extensive development and results in a typical turnaround of about 3 or 4 months from the semiconductor house for the receipt of working samples. One manufacturer (Atmel) has recently produced a new chip that has 16K bytes of EEPROM where 8K bytes are used for the operating system instead of the ROM memory. This memory can be programmed as the last step in the chip manufacturing process and therefore enables a more rapid turnaround time.

There are broadly speaking three development options that may be pursued, shown here in increasing order of complexity,

- Use an existing application in the ROM, where the EEPROM is used for the management of application data.

- Add an application program to the EEPROM to work in conjunction with the ROM program.

- Develop an application for the ROM.

In all cases there is a need to develop a matching application in the terminal to which the IC card will be connected. Each of these development options will be considered in turn .

a) Suitable application already provided in chip ROM

This is the easiest entry point for an application developer assuming that an IC card can be obtained for which an appropriate program already exists in the ROM. A number of suppliers provide IC cards in this format including,

GEMFILE (from GEMPLUS)
OSCAR (from GIS)

in both cases sited here the chip is already programmed with a file management application along the lines of the emerging ISO 7816 - 4 proposed standard. Conformance to the proposed standard is not a matter that we need to discuss here. These IC cards are designed for general purpose evaluation and development. Here the task of the developer is to produce the application in the terminal device that will be used in conjunction with the card. It is clear of course that the application may involve more than just the terminal and will often include other components such as a host computer system. When we refer to the terminal application development it is intended to include the application system into which the IC

card operates.

We have assumed that the development process follows conventional design principles with the definition and production of the necessary specifications along the following lines,

- Technical requirements specification
- Functional specification
- Architecture specification
- Component specification
- Test specification

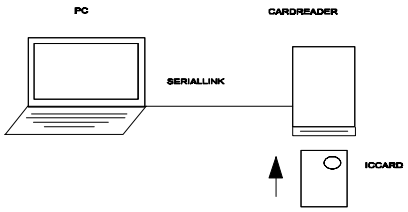

Fig2 BasicCardEvaluationConfiguration

In this part of the tutorial we are concerned far more with the tools available for managing development. We will leave the rigors of software specification, design and development for another occasion. Here in particular we would like to evaluate an existing component to assess its viability for incorporation into the business application. In fig. 2 we show a typical set up for evaluating the IC card. In this tutorial we have always used the ubiquitous PC as our core processing engine. This should not be taken to mean that other processing systems are excluded but only that we are reflecting the simplest and most readily available development tools.

Now the basic standards start to become important. We would expect the IC card to conform to ISO 7816 - 1/2 in terms of physical size and location of the contacts. Also we would hope that the card would conform to ISO 7816 - 3 in terms of its electrical and signal characteristics. The main point to watch here is the communications protocol for the IC card. The T=0 protocol is well tried and tested whilst the T=1 protocol is somewhat newer and subject to options. Perhaps the least explored area is protocol type selection where the IC card is capable of operating with more than one communication protocol. I am not aware of any commercial product that is capable of handling this complexity. In fact it is far more appropriate for the terminal to handle different protocols say both T = 0 and T = 1 whilst the card may handle only one of these protocols.

Accordingly the basic set up for evaluating the IC card product is a PC on which an evaluation software package has been installed and an IC card reader (conforming to ISO 7816 - 1/2/3) which is usually connected to one of the serial ports on the PC.

The evaluation package would normally contain a menu that allows the user to issue the allowable command range and to show the IC card response. Thus in general facilities are provided that allow the user to read and write data into the EEPROM memory. The full command range will be defined in the documentation that comes with the IC card specification. These commands should operate as per the ISO 7816 - 3 standard and are usually similar to the set of commands currently under discussion for the proposed ISO 7816 - 4 standard. We described these commands in an earlier part of the tutorial (part 8).

Now some applications may only need this basic file management system with its somewhat limited security capability. In this situation the task of the developer is to build the terminal application which can be developed using the same hardware configuration as shown in fig.2.

b) Develop an additional program to the ROM operating system

The next level of sophistication in terms of a development strategy would be to add an additional application program which can be executed from the EEPROM memory. Clearly the ROM operating system must be designed from the start to allow this form of development. The COS (Card Operating System) supplied by Gemplus as a standard product allow for this enhanced application.

The COS operating system includes the concept of filters. This is a means by which the operating system can transfer control to an application program that has been loaded into the EEPROM memory. The developer will need to design his application using the appropriate software tools (an assembler is a minimum requirement) for the particular chip that is used by the IC card. Having developed this application then the machine code may be written into the EEPROM memory using the standard write memory command which is provided by the ROM operating system.

The trick provided by the COS operating system is the ability to set a vectored address in a defined memory location. When the operating system is executing it will examine this address at the appropriate moment (e.g on receipt of a command from the serial port) and if the address has been set then control will be transferred to the new application program residing in the EEPROM memory. This allows the additional application to manage the commands received over the serial interface. The COS operating system allows some flexibility in the way these filters are managed. From a developers point of view this approach is attractive because it allows a very fast development path. Security may be enhanced but without having to wait for the delay in reprogramming (and developing) the mask ROM operating system. The only draw back to this style of development relates to the use of valuable EEPROM space for storing the application program. The adequacy of the security features is a function of the operating system. There is no inherent reason as to why this should not result in a secure development path. It must of course be accepted that the developer of the operating system will be looking for a return on his investment but for many situations this must still lead to a cost effective development path.

c) Develop a new ROM operating system

This is of course the most involved of all the development paths. It is readily apparent that this can be a non trivial task and for an operating system with the complexity of the COS operating system referred to earlier almost certainly accounts for many man years of development. However for those situations where card cost is an overriding factor then the development of a ROM operating system allows the use of the EEPROM to be minimal or perhaps avoided all together.

The development environment in this situation is considerably more complex and results in the need for more components as shown in fig. 3. The centre of the development kit is the chip emulation system. This is manufactured to contain the components of the chip in an accessible form. Thus returning to fig. 1 the developer, by means of the development workstation is able to access the memory components separately in a form of test mode. Thus the workstation can load an operating system into the ROM memory area (usually implemented using RAM) and instruct the chip to execute the program. Like any normal ICE (In Circuit Emulation system) the developer can set break point and debug his program. The chip emulation system and in particular the probe is manufactured to behave exactly like the single chip equivalent. Some times this is achieved by using a bond out version of the IC card chip where all the address and data busses are made available to the emulation system.

Having developed the new operating system in the emulator the total application can be tested by connecting a PC which contains the terminal end of the application. These two units are connected together by using what is sometimes called a faker card. That is a printed circuit board which has the same dimensions as an ISO 7816 -1/2 IC card at the connector end but which has a longer tail with a cable for connection to the emulator. The business end is plugged into a standard card reader (which can normally cope with the elongated tail) which is connected normally by a serial link to the PC terminal application.

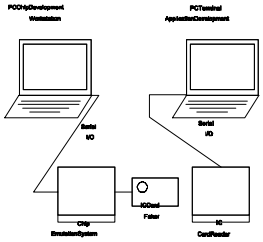

Fig3.ICCApplicationDevelopmentConfiguration

By this means the developer can test the total application before having to manufacture the chip with the new operating system program. When the code has been tested as satisfactory in the emulation system then you can be pretty sure that when the chip is fabricated with the same code in the mask ROM that it will behave in the same way. This is not to suggest that the testing of the working sample produced by the semiconductor house can be avoided but only that one may reasonably expect success the first time round in the majority of cases where the initial emulation was fully evaluated.

David Everett

Next month: IC card security life cycle

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.

Cambridge Congestion Metering

The Cambridge, England, road traffic congestion metering trial is due to start in September using Smart Cards from McCorquodale Card Technology.

This is one of the European Commission funded trials under the ADEPT (Automated Debiting and Electronic Payment for Transport) project which is introducing automatic debiting and Smart Card technology into five European cities to demonstrate automatic toll collection, and road use pricing as a means of managing traffic demand.

Philip Blythe, Senior Research Associate, Transport Operations Research Group, University of Newcastle-upon-Tyne, England, said the plan was for a demonstration to take place in Cambridge in September. "It is really a technology demonstration as one of the five sites in the European Commission's ADEPT project.

"The Department of Transport are providing us with a small amount of additional funding to test out some different forms of pricing. Rather than just the congestion metering proposed for Cambridge, we will also be testing distance-based charging and open toll based charging."

Mr Blythe said that McCorquodale had produced several hundred Smart Cards free of charge for the project, and also provided 800 demonstration cards for publicity purposes.

Of the other four field trials under the ADEPT initiative, only the one in Goteborg, Sweden, is currently up and running. This is the world's first demonstration of multi-lane road pricing with Smart Cards which have been supplied by Gemplus.

The project in Thessaloniki, Greece, is expected to start this month and involves mono-lane and multi-lane tolling. Parking management, debiting and booking will be developed in Portugal's Lisbon project expected to start at the end of this year, while the field-trials in Trondheim, Sweden, will follow later to develop non-stop tolling, multi-lane road-pricing and other transponder-based applications.

Mr Blythe said that these trials would enable the development of application-specific systems but, at the same time, pursue the possibilities for integrating them all into a single system architecture.

Pictured below is the in-car keyboard and display and the transponder to be used in Cambridge.

Contact: Philip Blythe, Senior Research Associate, Transport Operations Research Group, University of Newcastle-upon-Tyne, England - Tel: +44 (0)91 222 8352.

