Major Stored Value Card Plan in Australia

A major tender for a Stored Value Smart Card for use in small cash transactions, has been announced by the New South Wales Government in Australia.

Big name multinational companies are associated with the launch which indicates that the card scheme is likely to be introduced in Victoria and other states and eventually adopted nationwide. The tender is being advertised worldwide for a private sector operator to develop, implement and market the scheme and the Government expects responses from consortiums or financial institutions.

Continued on page 103

Secretary of State for Employment, The Rt. Hon. David Hunt Launches the Merseyside TEC Card Scheme.

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 11 - The Smart Card Development Environment.

CONTENTS

Australian Stored Value Card

Continued from page 101

Consumers will pay cash for the card and then use it to pay for small purchases such as snacks, bus, train and taxi fares etc. Trials are expected to start early next year following a six to nine month evaluation of tender documents.

Anne Cohen, NSW Administrative Services Minister, said: "We want to emphasise this is not a credit card or a debit card, it is a cash replacement card." She added that it would not have a PIN number.

The pre-paid cards will be available in amounts of $20, £50 and $100 from participating stores and other outlets, but Mrs Cohen said there was a possibility of introducing rechargeable cards later. "Based on international consultations, Integrated Circuit Card technology appears to be the most suitable and secure technology for the scheme," she said.

Consumer applications

The tender identifies essential consumer applications for the card as follows:

Application	Industry Average Transaction Value
Fast food	$5.60
Tickets (rail, bus, ferry)	$5.60
Entertainment (cinema, video, rental)	$5.60
Parking	$5.00
Taxi	$8.50
Convenience store	$3.50
Payphones	$2.60
Vending	$1.20
Betting	$7.00
Toll payment	$2.00
Petrol	$27.00

Government initiative

It is interesting that the initiative for the scheme comes from the Government. Mrs Cohen commented: "The Government is the ideal body to initiate the scheme as it can bring together the different interests of many different - and often competing - businesses and services. The Government is also in the position to be able to deliver the critical mass of consumers needed to start the scheme by providing access to public transport. It is estimated that around 1.2 million trips are conducted in Sydney each working day on bus, rail and ferry services."

Tons of coins are collected each week for the State transport ticketing operations and savings to the Government in cash handling alone is estimated to exceed $10 million a year.

The Government has put a purchase price of $US10,000 on the tender document which they say includes comprehensive marketing strategies, details of the involvement of both the Government and private sectors, and includes relevant financial data.

Huge scheme

Indications are that it could be a huge scheme with major corporations whose businesses involve small cash transactions, expressing the intention of grasping the benefits of Smart Card technology. Interested companies named by the Government include McDonald's, BP, Kentucky Fried Chicken, Coca-Cola, Village Roadshow (Australia's leading cinema network), Optus Communications (the new telecommunications carrier), Cabcharge (covering 12,000 taxis) as well as pubs, clubs and private bus operators.

Technology suppliers said to have been briefed on the tender are: NTT International Corporation, AOTC, BT Australia, Horizon Telecommunications, Bull HN Information Systems, Fujitsu Australia, Gemplus Technologies Asia, Schlumberger/CMS - France, Cardinal Network of Australia, Optus Communications, Pacific Star Communications, Security Magnetics,

AWA, GEC Plessey Telecommunications (Australia), IBM Australia, Digital Equipment Corporation (Australia), Alcatel STC Australia, Hutchinsons Telecommunications, AT&T Australia, Thorne Secure Science International, Singapore Computer Systems, Toshiba - Japan, Motorola - Scotland, Mitsui - Japan, Solaic - France, Philips - Australia, Thyron UK, Datacraft Australia, Landis & Gyr Communications - Switzerland, Singapore Telecom, Exicom, Motorola - Australia, Siemens - Australia.

Financial institutions

Financial institutions briefed are Sakura Finance Australia, Mitsubishi Bank of Australia, The Fiji Bank, Westpac Banking Corporation, The Bank of Tokyo, Barclays Bank Australia, BNP Pacific (Australia), Australia and New Zealand Banking Group, The Sumitomo Bank, Hong Kong Bank of Australia, Advance Bank Australia, IBJ Australia Bank, St. George Bank, The Dai-ichi Kangyo Bank, Bank of America Australia, Macquarie Bank, Commonwealth Bank of Australia, The Daiwa Bank, The Sanwa Bank, National Australia Bank, Bank of Singapore (Australia), Bankers' Trust Australia, The AMP Society, Cathay Finance International, DBS Bank - Singapore, United Overseas Bank Group - Singapore, and Citibank - USA.

Contact: Tony Overstead, Project Co-ordinator - Tel: +61 2 339 7276. Fax: +61 2 339 7700.

Merseyside TEC Future Card

Merseyside Training and Enterprise Council (TEC) has ordered 6,500 Smart Cards from DataCard for use as its Future card to pay for training benefits.

Most young people will join the Future scheme straight from school. All 16 and 17-year-olds, and certain young people of 18 or over entering employment and training in the Merseyside TEC area are entitled to the Future card. It is sent to the young person by the TEC after it receives a personal training plan agreed between the young person and his or her training supplier or employer.

The Smart Card carries a record of the holder's personal details, training plan and achievements. The information on the card is checked and updated using a Smart Card reader linked to a computer. The TEC uses this information to make payments to the supplier for the training received, and also for statistical purposes.

Card details:

Type	Contact
Fabricator	DataCard
Dimensions	ISO ID1
Contact location	Front
Chip manufacturer	SGS-Thomson
Memory type	EEPROM
Memory capacity	2K bytes
Standards	ISO 7816-1-2-3
Comms protocol	T=O
Security	PIN
Cryptography	DES

Contact: Angela Hoare, Merseyside TEC, Liverpool, England - Tel: +44 (0)51 236 0026. Adrian Cannon, Smart Card Business Manager, Datacard, England - Tel: +44 (0)81 570 6522.

Innovatron/Bull Patents Clash

The Innovatron Group, formed by Roland Moreno and which filed the pioneer patents on Smart Card technologies in 1974 and 1975 is to oppose some of Bull CP8's patents in Germany.

In a statement released in Paris this month, Innovatron says it has granted licenses to more than 175 companies worldwide including the giants of

electronics and information technology. Bull CP8, was one of Innovatron's first licensees and filed a whole range of patents close to those of Innovatron some years after Innovatron and some of them are still in the process of being granted particularly in Germany.

The statement said: "Now, Bull CP8 has decided to conduct an active licensing policy, separate from Innovatron's. For this reason, Innovatron feels bound to protect its basic interests as inventor and creator of Smart Card technologies and to oppose in Germany the granting of those Bull CP8's patents which are close to Innovatron's."

Schlumberger Appointment

Jacques Brault is to head Transactions Systems, the new business grouping with Schlumberger Technologies bringing together the Smart Cards and Systems Division and the Urban Terminals & Systems Divisions. He was previously General Manager of Urban Terminals & Systems. George Kayanakis, General Manager of the Smart Cards and Systems Division is to head Schlumberger Technologies' Retail Petroleum Systems Division.

Banks in SA Agree on Standards

South Africa's four major banks - ABSA, First National Bank, Nedcor Bank and Standard Bank -announced early this month that they have agreed on the standards required for the development of Smart Card applications for the South African financial industry.

It is envisaged that the large-scale introduction of Smart Cards, which allow off-line PIN validation and some degree of portability for terminals, will bring millions of South Africans into the formal banking net.

Smart Cards are already used in the Universal Electronic Payment System (UEPS) electronic wallet application (SCN December 1992) by the SA Perm Building Society, a division of the Nedcor banking group, and Megalink, the system operator and switching subsidiary. More than 100,000 Gemplus cards are used at some 3,000 points of sale. This development encouraged the banking groups to get together to develop a common standard which will conform to international standards.

At a conference in Johannesburg early this month, Mike Jarvis, Chairman of the Inter Bank Standards Committee and General Manager of Information Technology at First National Bank, said: "We ran the risk of each bank developing its own systems at the cost of allowing customers common access to other banks' networks, ATMs, Smart Card readers and point of sale devices."

An inter-bank pilot project is currently in the planning stage and will be launched within a defined community to enable monitoring and control from a systems perspective as well as from a client/merchant point of view.

Major growth

Smart Cards will initially be targeted at those who do not qualify for credit, or at those who do qualify but do not wish to incur credit, as the technology is designed to replace cash, cheques and debits but not credit card transactions.

The major growth in the card industry is likely to come from debit and prepaid cards, bringing millions of South Africans into the formal banking net. It is estimated that one in three South Africans has a bank account and, of these, only 10% have credit cards. The promotion of Smart Cards has, therefore, significant opportunities for the South African financial industry and it is likely that debit card use will overtake credit card use by 1995.

It is also estimated that 80% of all transactions in South Africa are cash transactions, the majority of which could be effectively carried out with a rechargeable electronic wallet payment card or a throwaway prepaid card.

Mr Jarvis said: "With the myriad of possible applications, many of which will substantially improve the lot of the mass market in particular we banks now need to consult as widely as possible with other business interests and social organisations."

Benefits

Benefits of Smart Card technology as seen in South Africa are that it provides security for the customer with the convenience of a single card to pay for small to medium value purchases without the need to carry cash. In addition, unlike a normal purse, a new electronic purse can be issued after loss, theft or destruction, with the original balance restored. This has particular relevance to the South African mass market where theft of weekly pay packets is described as "rampant," so it would be possible for companies to give loaded cards to workers in place of weekly pay packets.

Benefits for the retailer include guaranteed settlement, increased turnover, and cash taken out of the system. There is also significant potential benefit for merchants, especially those in remote locations, who do not have convenient access to on-line point of sale terminals. For the banks there is the opportunity to extend card payment products to a much wider section of the population while at the same time controlling risk and reducing fraud - both major issues in conventional payment markets.

As South Africa has a significant number of electronic terminals in the marketplace, it is likely that Smart Cards will also carry a magnetic stripe for use in ATMs for the foreseeable future.

AFC Project in Oslo

One of the most comprehensive Smart Card Automatic Fare Collection (AFC) projects to be undertaken anywhere in the world will involve buses, trams, subway, trains and ferries in the region of Greater Oslo, Norway.

The region around the Capital city has a population of around 889,000, and public transport is the responsibility of three publicly owned transport authorities: the Norwegian State Railway, Greater Oslo Local Transport and Oslo City Transport which with about 27 transport operators carry more than 200 million passengers every year.

To implement a new integrated fare collection system, the three transport authorities set up a joint venture company called BAS which spent four years on testing and looking at existing systems, and a further four months evaluating 13 tenders for the project.

In November last year, Scanpoint Technology was selected as the turnkey supplier responsible for the delivery, installation, maintenance and support of the system.

Main objectives

BAS defined the main objectives of the new fare collection system as:

* Handling of the different and independent fare structures in the region: flat fare, zonal fare and distance related fare.

* Handling of multi-modal ticketing: bus, train, tram, subway and ferry.

* Distribution of revenues between all authorities, transport companies and operators involved.

* Minimising boarding times.

* Being user friendly to operators and users.

* Reducing the level of fraud.

* Integration with existing systems.

After examining the available card technologies, BAS chose the contactless Smart Card for reasons of security, its large capacity and long lifetime, plus the advantage in connection with a city transportation system of a transaction speed of less than 0.3 of a second depending on the card type.

Pilot project

A pilot project will start in November this year involving buses, trains, trams and on-station equipment, but not ferries at this stage.

Scanpoint has ordered 20,000 1K byte EEPROM microprocessor contactless Smart Cards from GEC Card Technology, England, for this trial. The card communicates with the card reader using standard data communications without any integral battery, and conforms with standard ISO dimensions.

Full implementation of the AFC system is scheduled to start in August, 1994.

Although cash tickets will still be available it is hoped that the vast majority of travellers will use Smart Cards. When the system has been fully implemented, BAS will look at additional uses for the card in providing other services.

System implementation

The budget for the AFC system implementation is 150 million Norwegian kroner (approximately £15 million).

The development involves a large amount of hardware and software:

Fare Computers	1,757
Portable Fare Computers	437
Contactless Smart Card Readers	1,803
Stand Along Contactless Card Readers	235
Contactless Smart Card Verifier	78
Passenger Operated Vending Machines	239
Depot Equipments	106

In addition a major data transmission system, and central and depot software, is to be installed. The number of contactless Smart Cards to be ordered for implementation is not yet known.

Fare Computer

The Fare Computer is primarily installed in buses, trams, trains, ticketing offices or similar places and is used for sales, updating and validation of tickets and cards. All prices and validity periods are calculated automatically according to the fare description loaded in the Fare Computer. When a ticket is issued or a card is used, all data such as route, destination, driver ID, date and time, ticket or card type is saved for processing.

Portable Fare Computer

The Portable Fare Computer is used on trains and ferries and is meant for sales of tickets, and sales, updating and validation of cards. Like the Fare Computer it saves data for processing later.

Contactless Smart Card Reader

Most card readers are for buses, trams, trains, ticket offices or in connection with turnstiles on subway stations. The reader automatically validates a

contactless card according to the attached Fare Computer. It allows passengers to validate their cards without any staff involvement. The passenger presents the contactless card within 10 cms of the reader and the unit gives a visual and acoustic accept/not accept signal. At the same time relevant card information, for example, residual value, is displayed.

Stand Alone Reader

This unit is designed for installation outdoors on train and subway stations and is resistant to climatic conditions and vandalism. It is used for the automatic validation of contactless cards according to the fare description loaded in the unit. The card reader is equipped with a keyboard which allows the passenger to select the required journey before presenting the card to the reader. When the passenger presents his card the unit operates in the same way as the reader above.

Contactless Smart Card Verifier

These are for use by the transport authorities inspectors for checking validity of passenger cards. All data registered from the cards can be transferred directly to a personal computer.

Passenger Operated Vending Machines

Five different types of vending machines will be installed outdoors on train and subways stations, ferry berths and similar places. They will accept coins, notes, bank cards and contactless Smart Cards to enable passengers to buy tickets, validate and update their cards. A number will be equipped with touch screen and a special printer for issuing standard tickets. All data registered is saved for processing.

Depot equipment

Basically all drivers, ticket collectors etc have their own personal staff card which is used for transferring data between the ticket machines and the depot equipment and then to the central computer system network.

Data Transmission System

The Data Transmission System handles the data flow to run the fare collection system, for example, data between ticket issuing units and company depots or central computers.

Changes in the fare system and "black lists" can be transferred to the fare computers, or sales and transaction data from the fare computers back to the central computer.

Central and Depot Software

The three transport authorities have BUSPOS, an extensive administration and communication software package for handling the fare collection system, installed on their mainframe computers which are on-line to each other and form the central computer system network.

BUSPOS has several routines, for example, administration of all ticket issuing units in the system, collection of all transaction and financial data for processing, settling of accounts with staff, operators etc. It also has a card database with a status on all cards used in the system making it possible to create blacklist or reissue lost or damaged cards.

Contact: Hans Holmgren, Project Manager, Scanpoint Technology A/S, Denmark - Tel: +45 43 43 39 99.

Italian Moneta Card

One million retailers throughout Italy are members of the Confcommercio Association which, in 1989, formed a new company called SETEFI SpA to develop the Moneta electronic payments systems for which they adopted Smart Card technology. The Moneta multicard EFT system uses a multi-service microchip credit card.

Set up with capital of 5 billion lira, SETEFI is owned 30% by FINATER representing the Association's members, and 35% each by the Italian banks CARIPLO and BANCA di ROMA.

Confcommercio wanted to create a card product to overcome the problems restricting card utilisation in Italy which were identified as: Retailers unwilling to take cards because of high merchant commissions, unwieldy mainly paper-based systems; unreliable supply of terminals, connections and response times; unacceptable delays in applying transactions to accounts; and high levels of fraud due to stolen cards by organised crime.

The Moneta Card offers the cardholder two different accounts - the Conto Breve (short account) settled by paying the full balance monthly by direct debit 15 days after receiving the statement; and the Conto Lungo (Long Account) limited to transactions above a fixed limit at certain shops only. Settlement is by 6, 12 or 18 equal instalments including interest which is recalculated monthly to take into account new purchases.

The Smart Card handles all authorisations and purchases and security is through a PIN code chosen by the user. The card decides when PIN entry is required according to the sale amount, for example, all transactions above an agreed limit, or on a random basis allowing several small purchases to be made consecutively before PIN entry is requested.

The Moneta card encompasses all transaction types from newspaper and vending purchases to substantial items more usually associated with credit/debit cards.

Following pilot projects in 1990, the system is now established in several regions - Lombardy, Tuscany and Sardinia - and in important towns like Bari in the south east.

Growth statistics

In these areas the scheme has shown substantial growth. The following figures, given by Eugenio Casucci, of FINATER Confcommercio, Milan, show:

The installed base of EFT terminals has risen from 4,746 in 1991 to 9,767 in 1992, an increase of 105%

Payments accepted increased from 336,582 in 1991 to 2,370,745 in 1992, an increase of 604%

The total value of payments increased by 616% from 63,437 million lira in 1991 to 454,314 million lira in 1992.

Moneta cardholders rose from 124,253 in 1991 to 179,721 in 1992 - a 45% increase.

It is planned to extend the system throughout Italy, but this expansion has been slower than anticipated when the Moneta Card was first launched.

Mr Casucci explains: "There is a real problem of implementation of the project because it is based on EFT terminals and we do not have EFT terminals to cover all over Italy." Eventually, he says, there will be a mass distribution of terminals and cards when they can include all of the Association's one million members.

Benefits

Benefits to the retailers are that the system accepts all the most important credit cards - Visa, Master Card, American Express, Diners and Cartasi, and the Bancomat debit card. There is also the opportunity to issue co-branded cards which has been taken up, for example, by several hypermarkets and some retail chains. Other advantages include less commission on transactions, low or no cost EFT terminal lease, quicker payment and paperless transactions.

Cardholders need only one card as a credit card, can arrange long term payments, and withdraw money at ATMs.

From the issuers' point of view there is growing multicard acceptance, an integrated payment system with automated payment collection. The Smart Cards also offer high security against fraud and can be used off-line, reducing costs.

Card details:

Type	Contact
Fabricator	Gemplus
Contact location	Front
Chip type	microcontroller+memory
Memory type	EPROM
Memory capacity	4K bytes
Standards	ISO 7816-1-2-3
Comms protocol	T=0
Security	PIN
Cryptography	DES

Contact: Eugenio Casucci, FINATER Confcommercio, Milan, Italy - Tel: +39 2 332 00411.

New Card has FRAM Memory

A new type of card, called the "In-Charge" card, allows money or information to be exchanged on-the-move without contact. It combines the transaction card technology of Racom Systems, Inc., based on wireless data transfer via radio waves, with a new type of computer memory from Ramtron International Corporation called FRAM (Ferroelectric Random Access Memory) able to store data in the absence of power.

It is designed to provide a rugged contactless, cost-effective alternative to contact Smart Cards in low-value financial transactions and/or to expand the capabilities of read-only RF ID applications by providing a write function with the same performance as the read function.

The card contains a single chip radio frequency transponder with 256 bits of non-volatile ferroelectric RAM (FRAM) with high-speed read/write capability at a range of up to 15 cms (six inches). It conforms to ISO ID1 dimensions but is thicker at 1.65mm

In use, a cardholder would present the card to a Racom RF Communications Controller (connected via an RS-232C interface to an IBM compatible PC host computer) within the system range of 15 cms. The controller generates a 125 kHz powering signal to power the card transponder. The card transponder and the communications controller create an RF interface for reading and writing the card's internal memory. The system processes the requested transaction, records it, and updates the card's memory.

Applications

The system, known as the DSS 1000 RF Proximity Communications Subsystem, is seen as ideal for applications such as electronic fare payment in mass transit systems, ski resorts usage, or student ID campus cards.

Richard Horton, Racom President, says: "We designed the DSS 1000 system to replace coins and tokens in low-value

(less than $20) prepaid financial transactions such as fare collection on buses and subways. But we are also finding significant demand in applications ranging from electronic ski lift tickets, to recording maintenance and inspection records on containers of hazardous waste."

Demonstration kit

A preprogrammed version of the DSS 1000 intended for evaluation, applications development, and demonstration is available directly from Racom Systems at a price of $1,800.

The system includes four RFM 256 CC Transponder Cards, an RFC 100 AA 20 Communications Controller with antenna and power supply, cables, instruction manual, carrying case, and a Windows-based menu-driven operating software package for installation on the user's IBM-compatible PC. Additional cards can be purchased for $9.72 in orders of 1,000.

The kit can be ordered from Racom Systems, Inc., 4840 Pearl East Circle, #301E, Boulder, Colorado 80301, USA. Fax: +1 303 447 2033.

Contacts: Wayne Baker, Director of Business Development, Racom - Tel: +1 303 447 2474; Lee Brown, Manager of Corporate Communications, Ramtron Int. - Tel: +1 719 481 7011. In the UK, David Sherwood, Managing Director, AM&T Tel: +44 (0)272 237594.

GiroVend Contactless System

GiroVend's cashless vending system using contactless Smart Cards or keys has been designed to also handle a wide range of in-house applications such as security access control, parking, time attendance and personnel identification all on one card.

Among the first customers for the contactless vending system when it was launched last year was Lloyds Bank in the UK.

Now Group Chairman Richard Smart says the Group anticipates that the new system will attract 30 per cent of GiroVend's business sales in 1993.

Easy to upgrade

The system is designed to eliminate the expense of on-site cash-handling. It is quick and easy to upgrade from GV magnetic-based cashless equipment. The system's interchangeable media reader is designed to accept either an iC contactless "GiroCard" or, for more robust working conditions, the "GiroKey" fob. System transactions are activated through media proximity to the reader. Other transaction technologies such as magnetic stripe and watermark, can also be incorporated with the GiroCard for use with existing on-site systems.

Both the card and the key are rechargeable and the system software enables a wide range of user entitlements and special instructions to be programmed on the card, from discounts, subsidies and free vends, to differential pricing, quantity restrictions and even stock control.

The card used is a 1K byte EEPROM

Contactless Smart Card from GEC Card Technology.

GiroVend chose contactless technology because, unlike magnetic stripe based transaction systems on the market, it does not need surface contacts for reading and processing data. Where other card reader-write products are vulnerable to data corruption from dirt lodging in contacts or on exposed electromechanical moving parts, data transferred on the contactless card is by RF (radio frequency) induction.

The company says that as the card is protected from wear and tear, it lasts longer than other data carriers, and the system readers, with no slots, contacts or exposed moving parts to go wrong, are not only more reliable and robust than current transaction technologies but much faster and service efficient.

Contact: Richard Smart, Group Chairman, GiroVend Holdings, London, England - Tel: +44 (0)71 738 0616. Fax: +44 (0)71 738 0331.

Mercury One-2-One

Mercury One-2-One, owned by Cable and Wireless and US West, is currently Beta testing its Personal Communications Network (PCN) service with around 1,500 business customers before the commercial launch, later this year. Initial coverage will be the heavily populated London area bounded by the M25 motorway, with coverage extended to around 24% of the UK population by April 1994, and progressively throughout the country by the end of the decade.
The Smart Card is the phone owner's personal key to the service and Mercury has ordered cards from two suppliers - Datacard Corporation and Orga Card Systems (UK).

The customer gains access to the service by inserting a personal Smart Card into the phone and keying a PIN.

Using the card in another compatible mobile phone means that any calls made are charged to the owner of the card, rather than the owner of the phone. Similarly, you can let business colleagues, family members or friends use their own Smart cards in your phone and call costs will be billed to their account.

The One-2-One service offers various pricing options, a monthly call limit, itemised billing, and a VoiceMail service that records messages when the customer is unable or unwilling to take a call. Handsets will cost around £300 and are compact enough to slip into a pocket or handbag.

Security system

It is estimated that in the London area alone, 10,000 mobile telephones were stolen in the last year, but the new One-2-One service security system identifies both individual customers, with their PIN held on the Smart Card, and individual phones with a unique

identification code burnt into the handset. Either number can be "blacklisted" by the network rendering stolen phones or Smart Cards worthless to thieves.

As an extra security measure, the subscriber can programme an additional PIN access number to be entered before calls can be made.

Alan Hadden, Head of Business Policy, says: "We can't stop our customers from misplacing handsets or prevent people from stealing them, but what we can do is make the theft of those phones a completely worthless exercise. That is precisely what we have achieved by combining Smart Card technology and secure handset identification codes with an all new digital phone network."

Scandals

Scandals over the taping of Royal mobile phone conversations should never happen again. It is almost impossible to eavesdrop on digital calls, unlike the mobile networks which were allegedly intercepted to give rise to the "Squidgy" and "Camillagate" tapes.

A Mercury One-2-One spokesman said: "Not only will the new system transmit signals in a digital format unrecognizable as a voice conversation to anybody tuning in, the transmissions themselves are encoded in a form making them virtually impossible for eavesdroppers to decipher."

To find out more about Mercury's One-2-One service, call on Freephone 0500 500 121.

Harmonisation Move

A single Smart Card that can be used internationally for a wide variety of purposes is the aim of a working group composed of representatives of many of the leading companies in the chip card industry.

At the second meeting of the Open Multi-applications Card working group in Cologne, Germany, last month their view was that current contact card technology was insufficient as a basis for the development of a single card for multi-applications usage. The market itself was divided over this question with various non-compatible cards presently employed in different projects.

It is envisaged that the working group will start on a large-scale project with contactless card as its basis (named Contactfree Multi-Application Card," (C-MAC) driven by an internationally standardised operating system.

Representatives at the meeting included Bosch, Deutsche Bundersbahn, Eurocard, Giesecke & Devrient, Lufthana Airplus, Philips, Siemens, Deutsche Telekom, Visa and various banks.

ECCS Group

Later in the month, the European

Common Card Strategy group (ECCS), met in Caen, France, to review the practicality of developing a joint strategy aimed at establishing a MAC for world-wide usage.

The meeting convened by Mr H D Kreft, Managing Director, ADE, Germany, felt that the ISO standard 7816 (Part 4) was insufficient as it allows variations in the construction of card operating systems which can lead to the development of different ISO compatible cards. Whilst these, by definition, are compatible with the relevant ISO standard, they need not be compatible with one another. Also it is highly unlikely that 200 pages of standardisation description will lead to uniform results from hardware and software developers.

The harmonisation process requires, for example, the establishment of a reference system to ascertain whether a MAC or a MAC terminal behaves in an ISO-compatible manner. This software, called the Reference of International Card Harmonisation (RICH), ensures that programmes in both the card and the card terminal conform to ISO 7816. It is envisaged that RICH will set the international standard for the MAC in the same way IBM determined PC compatibility standards in the computer industry. The concept also proposes a RICH coupler device capable of operating both contact and contactfree cards through a single slot.

As no single international card producer clearly dominates the market at present, RICH can only be realised via the co-operation of various producers with market representation. This union of companies, in conjunction with contactfree chip card technology, is seen as providing the international breakthrough which could make RICH the world-wide standard for the MAC.

There were 21 delegates at the ECCS meeting including representatives from ADE, Credit Lyonnais, GEC, Gemplus, Motorola, Idesco, Amphenol-Tuchel, SEPT, and Schlumberger.

Contact: H D Kreft, ADE, Germany - Tel: +49 4151 8891-O. Fax: +49 4151 8891-29.

Dudley TEC Project Ends

Dudley Training and Enterprise Council (TEC) has ended its TECFUTURES Smart Card project (SCN, November 1992). The cards were used to replace money vouchers given to unemployed people to receive professional advice and guidance on job seeking and retraining.

Yvonne Peers, of Dudley TEC, said the TECFUTURES project was now finished. The idea was to test the technology and it worked very well with an off-the-shelf system which turned out to be cost-effective. It they had intended to go beyond the project it would have meant having a system tailored to the TEC's needs, but the cost was prohibitive.

The Smart Card system was supplied by JerseyCard and used cards from Gemplus.

Contact: Yvonne Peers, Dudley TEC, England - Tel: +44 (0)384 485000.

Philips DX ETEBAC 5 Approval

The French Groupement des Cartes Bancaires CB has approved the ETEBAC 5 security package presented by Philips, using standard readers, the new Philips DX microprocessor Smart Card operating the RSA public key algorithm, and software libraries of its catalogue.

The package is aimed at being integrated into available EDI (Electronic Data Interchange) application packages handling the ETEBAC 5 environment (Telematics Exchanges Between Banks and their Customers). Philips view this

package as a practical application that many companies will want to use with their banking partners and expect to deliver several hundreds of units this year and probably several thousands in 1994.

It offers the full set of security functions required in this environment: mutual authentication of each party to the electronic exchange, guarantee that information content is not altered during transfer, guarantee of the confidentiality of the exchange, irrefutable proofs to both parties of the existence and proper execution of the exchange.

The solution is already integrated into the ETEBAC application of CERG Finance, and has been qualified in the real environment of the ETEBAC server of Credit Lyonnais.

Other ETEBAC applications suppliers like SAARI, SYBEL, CONCEPT, and PLURIEL DCI are integrating the Philips' package into their offer, and will shortly be ready with the corresponding full ETEBAC 5 solutions.

Philips say their DX Smart Card-based package is in line with international standards, and complies with the most recent recommendations of the security working group on EDIFACT (Electronic Data Interchange For Administration, Commerce and Trade). They see it as a sound basis for further international standardisation, since the core security part is separate from the ETEBAC application software, and complies with EDIFACT recommendations on security.

Contact: A J Selezneff, International Marketing Manager, Philips Smart Cards & Systems, France - Tel:+33 1 40 94 75 84. Fax:+33 1 40 94 79 68.

Advanced Card Association

Plans to set up an Advanced Card Association based in the UK are now underway following an inaugural meeting to produce a framework to formalise the Association. The meeting discussed an interim constitution, a committee structure and invited elected representatives.

It was announced that the Department of Trade and Industry will provide the venue for the first full meeting for interested industry members wishing to join and that their will be direct liaison with invited government representatives through a joint speaking form which will cover specific vertical markets.

Over 15 offers for country representation in Europe have been received and discussed and it is planned to utilise these representatives to set-up similar government and trade links within their own countries.

The Association has also received requests to consider co-operation with the US Smart Card Industry Association (SCIA) and the International Card Manufacturers' Association (ICMA) to allow representations across a united front.

Any interested parties who wish to become involved should contact Chris Stanford or Simon Reed, c/o Charta Associates, The Court, Freepost, PO Box 301, Hemel Hempstead, Herts, HP1 1BR, England - Tel: +44 (0)442 231844.

Quality Certification for SOLAIC

SOLAIC, the Smart Card subsidiary of Sligos, has been awarded the ISO 9002 certification and its European equivalent, EN29002, for the manufacture of PVC integrated circuit memory cards and Smart Card micromodules.

The certifications were awarded by the French Quality Improvement Association (AFAQ) and the European Network for Quality System Assessment

and Certification, respectively.

SOLAIC's three core businesses - card manufacturing, card personalisation and memory card systems engineering - cover the entire Smart Card cycle from engineering to final delivery.

Smart Card Telephone Adaptor

A new telephone adapter for AT&T's contactless Smart Card, allows any touch-tone telephone to be used for banking transactions, ticket purchases and other services from a home, office, hotel room or other location where previously it would have required a personal computer or similar product.

The prototype adaptor, which is about the size of a small paperback book, was demonstrated at the American Bankers Association National Operations and Automation Conference in New Orleans last month. Applications shown included the purchase of an airline ticket over the phone with the transaction recorded electronically on the card.

The adaptor contains a Smart Card reader/writer and a modem. When plugged into a standard telephone line, it allows a Smart Card to be used to verify the user's identity and as a storage medium on which the transaction can be securely recorded. A single telephone line is used for both the voice connection and the data link.

A major concern with home banking has been security, but AT&T says it has developed a verification system that substantially reduces the possibility of fraudulent access to a bank account. Although the user only has to provide a simple password, the Smart Card and the bank's computer carry out a security check to make sure the card is valid.

Diane Wetherington, President of AT&T Smart Cards, says: "Until now, many of the promises of the information age, like home banking, have been a reality only for people who can afford expensive home computer systems and were willing to learn how to use them. This device will let anyone perform transactions from anywhere, without the need for expensive computer hardware as an interface."

AT&T's 3K byte EEPROM contactless Smart Card can be used for multiple applications such as banking, and also act as an "electronic ticket" for airline travel, sporting events etc.

Contact: Michael Jacobs, AT&T, USA - Tel: +1 908 582 4767.

De La Rue and TRT Joint Venture

De La Rue Card Technology, a subsidiary of De La Rue PLC, and Philips Smart Cards & Systems subsidiary, TRT, have set up a joint venture to sell their Smart Card systems in the UK and Ireland.

Called Delphic Card Systems EEIG, it has been formed through the European Economical Interest Grouping (EEIG) structure and is headquartered at Tewkesbury in England. It will provide Smart Cards (microprocessor and memory cards) and associated readers and terminals, develop Smart Card solutions for business applications, and provide Smart Card personalisation services.

Delphic aims to be the leading payment card in industries such as banking, loyalty/leisure, utilities, pay TV and telecoms. The range of masks offered by Philips covers security cards, like D1, D2, or DX, the first RSA Smart Card on the market, or dedicated masks like GSM or BO' (for French banks), or general purpose masks like TB100. TB100 and BO' have been developed in co-operation with Bull CP8.

Contact: Darrell Barnes, General Manager, Delphic Card Systems,

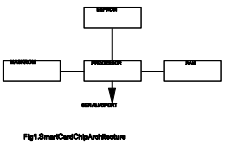
England - Tel: +44 (0)684 290290. Fax: +44 (0)684 290111.

Chip Card Reader from Safeware

Cardman, the new and compact card reader from Safeware AG, of Austria, can be used to read and write all chip cards compatible with ISO 7816.

Costing DM 240 (one-off price) the device can be connected to the serial port of a PC and can therefore be used under a variety of different operating systems.

Safeware says the open architecture permits OEMs, system houses and applications developers to offer the



inexpensive use of chip cards in the areas of electronic banking, access control to host systems and health insurance cards, amongst others. Evaluation kits are available.

Contact: Lars Sandell, Safeware AG, Linz, Austria - Tel: +43 732 301630-400. Fax: +43 732 301630-75.

Smart Card Tutorial - part 10

Security from the Bottom End.

Previously we took a look at the security of the Smart Card from a top down point of view. In other words we looked at the principles that we were trying to achieve without delving into the practicalities. This month we are going to start at the other end, looking at some of the practicalities to see what can be achieved. This bottom up approach should allow us to meet somewhere in the middle. This is a compromise between what is required and what can be achieved.

In order to consider security further we need to recap on the basic components of the chip in the Smart Card. This architecture is shown in fig. 1. The processor has four peripherals,

- MASK ROM
- EEPROM
- RAM
- SERIAL I/O PORT

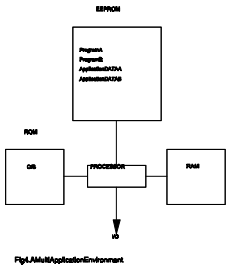
The mask ROM contains the operating system of the chip and is made as part of the chip fabrication process. This memory is read only and cannot be changed once the chip is made. The ROM may contain programs and data but in both cases the code and data are constant for all time. By the very process that the chips are made it is not practical to have any form of unique code or data in ROM. Thus the ROM memory is constant for a batch of chips (thousands). Each wafer at the end of the manufacturing process results in the die (apart from fabrication failures) looking identical.

The EEPROM memory is the non-

volatile storage area of the chip that allows data to be written and read under program control. This data is preserved even after the power to the chip is switched off. By writing data into the EEPROM we can give each chip a unique identity. The Smart Card chips from most semiconductor manufacturers have the facility to make parts of the EEPROM memory `write once only'. This is sometimes called OTP (One Time Programmable) or occasionally as EPROM memory in the sense that it cannot be overwritten. The latter term is ambiguous in that although EPROM memory requires ultra violet light for erasure, in the general sense the memory cells are always capable of being set to the final state. Thus if the initial state is all `ones' then any bit can be overwritten to `zero'. If this situation is allowed to arise then in some circumstances you may be subject to a security violation. Under these conditions going from a `1' to a `0' must increase the security for every bit used. A reverse situation may allow an attacker to decrease the security by over writing a `1' to a `0' which is an inherently possible process.

The random access memory (RAM) forms the memory working space to be used by the processor whilst executing programs either in ROM or EEPROM. This memory is volatile and all data will be lost (there are some security subtleties here that we will return to in a subsequent part) when the power to the chip is removed.

This RAM is no different in concept to that contained in our PC. However there is some difference in the amount of memory available. The modern PC usually starts at 1 million bytes and commonly has 4MB or more. The lowly Smart Card chip rarely exceeds 256 bytes. We mentioned previously that this is due to the square area of silicon taken by the RAM cells and the need to limit the size of the die for both cost and reliability considerations. Clearly the processor has total read/write control of the RAM. It is also important to note that the total RAM space is unlikely to be available to the application. At the very best it is necessary to invoke a



stack memory area for the processor to transfer control between the various software modules and to handle the interrupt structure of the processor.

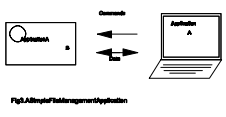
The serial I/O port should be considered as just another peripheral to the processor which may be read and written under software control. The most important point to notice here is that the hardware sophistication often found on general purpose microprocessors has been removed to optimize the space available on the silicon. Thus the ubiquitous UART (Universal Asynchronous Receiver Transmission) which buffers bytes of data to and from the serial port is replaced by a single register that the programmer must manage on a bit by

bit basis. Further more the timing of data transmission which is handled by the UART must now be managed by the program in the Smart Card.

For the purpose of our security analysis we will now consider two application scenarios. In the first case we will look at the Smart Card as a file management system as considered under ISO 7816-4. Then we will develop the situation further and look at the problems of managing two application programs in the IC.

In fig.2 we show the arrangement of programs and data for the Smart Card used as a file management system. We will simplistically consider two applications each with a file of data. We will also assume that these applications wish to control access to the data for authorised users only. It is important to note that the terminal acts as the application driver and completes the security link. Let us now consider that the Smart Card is brought into contact with a terminal containing the application as shown in fig. 3. In this discussion we will ignore the electrical and communication protocol handling and will assume it meets the ISO standard.

From the terminal's point of view there are four primary steps in the process of executing the application,



- Select the application in the card
- Prove the authorisation of the terminal user
- Read/write the application data
- De select the application (e.g power off)

In this very simple example we are only considering PINs as our security tool and the authorisation is therefore that of the terminal user (which may be delegated to the terminal by the application provider)

The application in the terminal thus proceeds to select the application using the commands of ISO 7816-4 as discussed previously (select file; verify; read/write).

Even in this simple example we run into problems straight away. Does each application have a separate PIN? From a security point of view it is clear that this must be the case and yet this contradicts the often held approach (with its obvious practicality) that this should be a single PIN for the card. There is a second problem even more fundamental than the first. How does the terminal know that the card is genuine? Giving a yes/no to the verify command is totally inadequate and hence the need for the authentication command. This allows the terminal to check the authenticity of the card but requires both the terminal and card to share the appropriate cryptographic mechanisms.

However it is clear that sufficient functionality exists to control these applications separately. Here the operating system is in control and can easily restrict access to the application data to authorised users in the sense that the correct PIN is provided). The application program in the terminal has no access to the data in the EEPROM directly and must invoke the commands available in the MASK ROM.

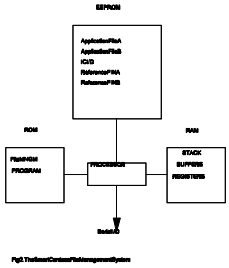
Let us now consider the more

interesting case where there are two application programs in the EEPROM as shown in fig. 4. Now the security game changes because the processor effectively transfers control to a program running in EEPROM. In the general case (some IC chips can constrain the memory partitioning; see vol. 1, No 1) the processor can read and write any data in the EEPROM whether it belongs to its own application or another. What this means is that a particular application must be restricted from reading and writing data in the EEPROM. All data accesses must be referred to a program that executes from the operating system in the MASK ROM. By this means the operating system can assure the correct partitioning of the data to its own application. Whether this is achieved by software (i.e an interpreter type of approach) or hardware control of the memory accesses results in a more sophisticated view of the architecture of the ICC.
We have shown in this part of the tutorial that there is a fundamental security difference between a file management structure (as envisaged in ISO 7816-4) and the more general case of a multi application environment. We have also made the point that a PIN check (supplied by the terminal) by an IC card is a one way process which does not take account of the authentication of the card itself. This is clearly not acceptable in the majority of applications and requires therefore the additional process of the terminal authenticating the card. This requires an additional overhead of cryptographic mechanisms and the appropriate key management hierarchy.

In a subsequent part we will explore the life cycle of an IC card from a security point of view including the implications of cryptographic key management. We will also attempt to answer that difficult question `Is a Smart Card secure?'

Next month. The Smart Card development environment.

David Everett



Smart Card Diary

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

This 3rd international card conference focuses on recent developments in the card industry. Contact Hopenstedt & Wolff - Tel: Germany +49 40 271 3323. Fax: +49 40 270 8066.

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: 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.

Brewers Test Cashcards

Two major brewers, Allied Lyons and Scottish & Newcastle, are to test cashcards in selected managed houses following the successful introduction of cashcards into a number of Whitbread pubs last year. Allied Lyons subsidiary, Taylor Walker, is installing the system in two of its Mr Q's specialist pool pubs in North London, while Scottish & Newcastle is introducing cashcards into three pubs in Gosforth, Sunderland and Whickham in north east England.

The Schlumberger cards can be bought at the bar and credited with the customer's choice of value. They can then be used for food and drink purchases and on non-payout amusement machines. Both brewers are tying rewards into card usage by writing bonus points to the card memory.

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

Cryptography Update

In April the President of the U.S.A announced a new initiative designed to bring together industry and the Federal government to improve security of telephone communication whilst meeting the needs of law enforcement.

The U.S government engineers (NSA) have designed a new cryptographic chip called `CLIPPER'. This chip has nominally been designed for attachment to an ordinary telephone. This chip may be used to protect both voice and data transmissions. The chips (MYK-78) will be supplied by MYKOTRONX of California. The silicon is fabricated in one micron technology by VLSI Technology Inc.

A novel feature of this new scheme is the establishment of an escrow system. Each chip will have two special keys, knowledge of which will allow the holder to decode messages generated by the chip. These keys will be stored in separate escrow databases access to which will be restricted to government officials with legal authorisation.

The CLIPPER chip contains a classified 64 bit block encipherment algorithm with a single 80 bit key called `SKIPJACK'. Apparently the algorithm has 32 rounds of scrambling (DES has 16) and runs at 12 Mbits/second. In volume the chips are expected to cost about $30.

A successor to the CLIPPER chip called `CAPSTONE' has already been developed. MYKOTRONX call this the MYK-80. This chip implements the SKIPJACK algorithm but also includes the DSA (Digital Signature Algorithm) and SHA (Secure Hash Algorithm) proposed by NIST. The CAPSTONE chip will not implement the RSA algorithm. These chips are expected to sell for about $85.

The SKIPJACK algorithm is intended to replace the DES algorithm which will cease to be certified in five years time. Some concerns have already been raised concerning the classified nature of the SKIPJACK algorithm and the escrow arrangement. The mechanism by which authorised agents may obtain the keys is still not clear whilst it would appear that once obtained then the subject's communications become insecure forever.

However it is clear that the US government would prefer SKIPJACK to be the new symmetric algorithm with DSA as the asymmetric algorithm. Whether the finanical industry will happily give up DES remains to be seen whilst the battle on RSA versus DSA continues. At the very least the patent position on DSA would appear to give Public Key Partners (PKP) and the RSA camp a distinct advantage.

Name_____

Position_____

Company_____

Address_____

_____

Tel._____

Fax._____

Name_____

Address_____

_____

Card No._____

Expiry date_____

Signature_____

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

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

Gemplus Fifth Anniversary

Gemplus has marked five years of successful trading at its anniversary celebrations in Gemenos, France. The company, formed on 2 May, 1988, employed just 12 people working in an old "garage" in Aix-en-Provence and had one client, France Telecom, who wanted one million Gemplus pay phonecards in circulation before the end of the year!

Now the Gemplus Group employs 700 people working at 13 locations in eight countries -

France, USA, Singapore, UK, Germany, Italy, Spaine and Taiwan - and supplies products to more than 50 countries around the world.

Smart Card production is now running at 10.5 million cards per month and the group has a turnover of 700 million French francs, 65% of which comes from exports.

The company has been able to grow because of the attention it has given to research into new products, technology and services, dedicating about 10% of its turnover each year to research and development. It has filed some 98 patents since it began operations.

From the original 300 sq.m in Aix-en-Provence in 1988, industrial facilities have been expanded to approximately 10,000 sq.m at the Gemenos, La Ciotat, Saracelles and Stuttgart plants.

This year, Gemplus obtained ISO 9002 quality certification making it an approved supplier of several major international clients.

Marc Lassus, Chief Executive Officer of Gemplus, (right) receiving the ISO 9002 quality certification from Charles Rozmaryn, General Manager of France Telecom

