Japan and USA to Push Smart Card Technology

Japan and the United States have formed Government-backed organisations to accelerate the development and widespread use of Smart Card technology in their own countries - strategic moves that should alert European countries to the need for closer industry co-operation, for example, as seen in the Open Multi-applications Card working group and the European Common Card Strategy group (ECCS).

The new organisations are the Japan IC Card System Application Council (JICSAP) and The Smart Card Forum in the US.

Continued on page 143

Mike McCourt (left) UK General Manager of Motorola's semiconductor operations, presents a framed wafer to

©1993 Smart Card News Ltd., Brighton, England. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, optical, recording or otherwise, without the prior permission of the publishers.

Stephen Barden, Chief Executive Officer and Managing Director of News Datacom to mark the supply of the seven millionth chip for Smart Card Pay TV systems.

Smart Card Tutorial Part 13
Cryptography and key management

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

©1993 Smart Card News Ltd., Brighton, England. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, optical, recording or otherwise, without the prior permission of the publishers.

CONTENTS

Japan and US Initiatives

Continued from page 141

The Japan IC Card System Application Council comprises representatives from the Ministry of International Trade and Industry (MITI), the Japan Electronic

Industry Development Association (JEIDA), New Media Development Association, Ministry of Post & Telecommunications (MPT), Japan Data Communications Association, Ministry of Health and Welfare (MHW), MEDical Information Systems (MEDIS), Ministry of Home Affairs (MHA), Local Authorities System Development Center, and private members from NTT, NTT Data, computer and communications products suppliers, and card makers.

Jicsap has two particular objectives. One is to popularise and promote activities in Smart Card technology, and three other councils have been set up with specific responsibilities for application development, popularisation and support activity, and public relations. The other objective is to study development activities through three other councils, the standardisation working group, the multi-purpose application working group and the contactless card study working group.

The Application Development Council currently has eight Working Groups dealing with specific applications such as healthcare, ID cards, networks, leisure and broadcasting.

The widespread support for the JICSAP organisation can be seen by the number of major companies represented on the various Working Groups.

Self-governing System and Medical System Working Groups

These two groups will work closely together and liaise with the Ministry of Healthcare and Welfare and the Ministry of Home Affairs who are studying future nation-wide expansion of IC card applications in this field. The Working Groups will gather information on related activities and look at new and future requirements to develop a new service model that can be introduced nationally.

Members are: Chairman, Jyuri Ozawa, NTT Data Communication Tel: + 81 3 5546 8337 ; Vice-Chairman, Toppan Printing Co.; Consultant Members - Medical Information System Development Center and Fujitsu; Public Relations - Local Governing Information Center and Hitachi Maxel. Members - Oki, Omron, IBM Japan, NEC, Japan Unisis, New Media Development Association, Hitachi, NTT Card System, C-Media, Syoei Printing Co., Tokyu Car Manufacturing and Tokin.

ID Card System Working Group

This group will examine ID card applications which, although they have a relatively long history compared with other applications, are independent as a system and of a "closed" type. The Working Group will gather information on the various systems and the services they provide and study the possibility of expansion from a closed system and of linkage and compatibility with other systems.

Members are: Chairman, Hiroshi Shogase, Toshiba Tel: + 81 3 5484 6272 Vice-Chairman, DNP; Consultant members - Matsushita Battery Industrial Co. Zexel; Public Relations - Mitsubishi and Japan Unisis; Members - NTT Data Communications, Omron, Oki, Toppan, IBM Japan, NEC, Hitachi, Hitachi Maxel, C-media, NTT Card System, Yamatake Honeywell, Shoei, Japan Construction Mechanisation Association, Tokyu Car Manufacturing, Tokin.

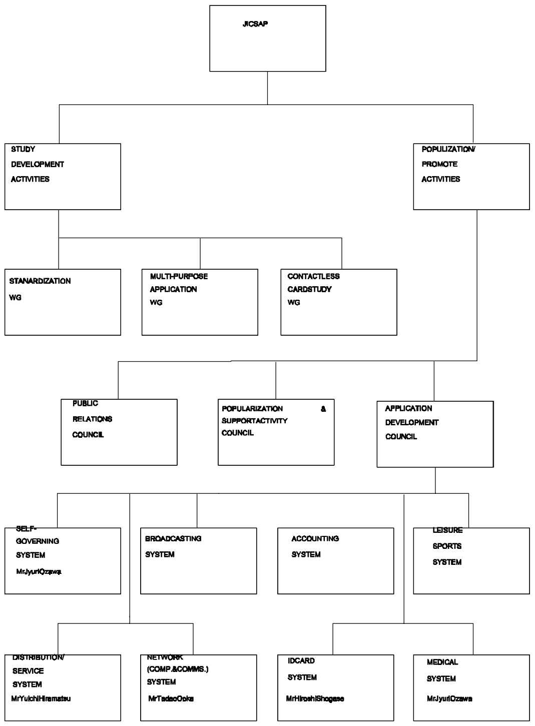
Distribution/Service System Working Group

The group will study current applications and problems and study the possibility of expansion and the application field.

Members are: Chairman, Yuichi Hiramatsu, Oki - tel: + 81 3 3454 2111

©1993 Smart Card News Ltd

Vice Chairman, JEIDA; Consultant Members - Omron and Hitachi; Public Relations - Sharp and IBM Japan; Members - NTT Data Communication, Oki, IBM Japan, NEC, Japan Unisis, Hitachi Maxel, Fujitsu, DNP, Toppan, C-media, NTT Card System, Teleka, Japan Diners Club, Tamura Electronics, Dynamic & Leading Co. Shoei, Tokyu Car Manufacturing, Transport Economic Research Center, Tokin.


JICSAP
STUDY DEVELOPMENT ACTIVITIES
POPULIZATION/ PROMOTE ACTIVITIES
STANARDIZATION WG
MULTI-PURPOSE APPLICATION WG
CONTACTLESS CARDSTUDY WG
PUBLIC RELATIONS COUNCIL
POPULARIZATION & SUPPORTACTIVITY COUNCIL
APPLICATION DEVELOPMENT COUNCIL
SELF-GOVERNING SYSTEM MrJyuriOzawa
BROADCASTING SYSTEM
ACCOUNTING SYSTEM
LEISURE SPORTS SYSTEM
DISTRIBUTION/ SERVICE SYSTEM MrYuichiHiramatsu
NETWORK (COMP.&COMMS.) SYSTEM MrTadaoOoka
IDCARD SYSTEM MrHiroshiShogase
MEDICAL SYSTEM MrJyuriOzawa

Network System Working Group

The group will investigate the activities and trends in the field of telecommunication.

Members are: Chairman, Tadao Ooka, NTT - tel. +81 3 3509 4355; Vice Chairman, SPOM Japan; Consultant Members - NEC and Tatsuno Mechatoronics; Public Relations - New Media Development Association and Japan Data Communication; Members - NTT (five representatives), NTT Data Communication, Oki, Omron, SPOM Japan, Toppan, IBM Japan, Hitachi, C-media, NTT Card System, Teleka, U-card, KDD, DDI Corporation, Syoei, Tokin, and Tokyu Car Manufacturing.

A Further three Working Groups are in the process of being established. They are Leisure Sports System WG, Accounting System WG and the Broadcasting System WG.

Smart Card Forum

The Smart Card Forum in the United States is a Multi-industry initiative to accelerate the widespread use of Smart Card technologies in the United States, and has the backing of the financial services, telecommunications, entertainment, publishing, software, computer and health care industries and Government agencies.

The Forum's objectives include addressing compatibility issues across business applications as well as facilitation of market trials of multiple use cards.

Organisations involved include American Express, Apple Computer, ASI, AT&T, Bank of Montreal, Bay Bank, Bell Atlantic, Bellcore, CES, Citibank, IBM, Innovatron, MasterCard International, MicroCard, Microsoft, News Datacom, Philips Home Services, The Washington Post, Toshiba America, US Treasury, VeriFone and Visa International.

Catherine Allan, interim chairperson and Vice President, Corporate Technology, Citibank, says: "Our objective is to foster communications across industries and the public sector that will result in North American market trials of Smart Card based payments and information services within the next few years. The exploration of inter-operability standards by industry players will be a significant part of that effort."

In its formation stage, the Forum is focusing on user needs and analysis of business specifications for Smart Cards. Committees have formed to explore and define application specific requirements in several areas - payments, financial and information services, telephony services, electronic benefit transfer, and health care.

Key objectives defined by the Forum are to:address card-based applications and implementation: identify Smart Card inter-operability issues and facilitate market trials and identify inter-operability requirements consistent with, and drawn from, international standards organisations.

A Technology Committee has been established to provide advice on technology, systems, security and inter-operability issues to the various business applications work groups.

Rich Mandelbaum, Chief Scientist, AT&T Smart Cards Systems and Solutions, says: "The market needs exist, and the technology is proven. By expediting the implementation of this technology, the widespread use of Smart Cards in the United States."

The Forum offers various categories of membership from $1,000 to $15,000. A Board of Directors and Officers will be elected from the membership at the first annual meeting in late September.

Membership is open to public and private sector organisations with a user or business applications focus.

Little interest in the UK

A move to set up a Smart Card Forum with the Backing of the UK Government's Department of Trade and Industry met with little interest (SCN January 1993).Although some 40 representatives consisting of suppliers, bankers and end users attended a meeting at the invitation of the DTI, there was not enough support to progress the initiative.

The prime objective of the Forum was to achieve maximum benefit for the UK from the development and introduction of Smart Card technology with the promise of Government backing in providing research support, industry sponsorship and the promotion of innovative uses of Smart Card technology.

A spokesman for the DTI said: "This was a scheme which had to be developed by the industry if they wanted it, but there was very little interest." He described the scheme as currently being "on the back burner" and added that there was likely to be a meeting soon to finally end the initiative unless there was a strong revival of interest.

Contacts: The US Smart Card Forum - Susan Weeks, Citibank, New York - Tel: +1 212 559 0580. U.K Smart Card Forum. Ms Di Williams, Department of Trade and Industry, London, England - Tel: +44 (0)71 215 1902.

Philips Extending Capacity

TRT, the Smart Cards & Systems subsidiary of Philips, is to build a new Smart Card factory on its existing site in Caen, France, increasing its manufacturing capacity from 15 million to 60 million cards a year with enough space to go up to 200 million a year.

Philips will continue to concentrate mainly on microprocessor cards, a market in which they expect to handle much higher volumes, but they will also increase production of memory cards. The company already has a substantial market in supplying memory cards to the German healthcare programme and intend to break into the massive worldwide telephone card business.

The new factory is part of a re-industrialisation programme initiated by the French Government, Usinor Sacilor and the local communities and represents a FF 160 million investment over four years. The development will create some 300 jobs and reinforce the existing technological environment.

Contact: A J Selezneff, International Marketing Manager, TRT Smart Cards & Systems, France - Tel: +33 1 41 28 75 84.

Belgian Embassy Network

Belextel, the communications network linking all the Belgian Embassies in the world to the foreign ministry's central computer centre in Brussels, is nearing completion.

Installation in the embassies is in the final phase under the management of CSC Europe, UTIMACO Belgium, and Bull Belgium.Bull CP8 has supplied some 800 security packages (TLP 224 NV reader, PC integration kit, and cards).

Police Department

The same three companies are installing equipment during 1993 to protect computer workstations in the Belgian police department. Bull CP8 is supplying TLP 224 NV card readers and cards.

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

Rare Cards Auctioned for Charity

A rare set of limited edition telephone cards raised several thousand pounds at a charity auction to raise money for German Cancer Aid.

The auction, took place at Europe's first Telephone Card Exhibition held in Berlin and the proceeds from the sale of the cards, which included the first Smart Card to be produced in ECU units, was presented to German Cancer Aid by Bernd Schafers-Maiwald, Marketing Manager of ORGA Kartensysteme GmbH, Germany.

Chris Jarman, Managing Director of ORGA Card Systems (UK) Ltd said: "Rare telephone cards are fast becoming a collectors' item with enthusiasts prepared to pay large sums of money for unusual designs or limited editions. We were delighted that ORGA could become involved in such a worthwhile cause."

Contact: Paul Hill, Marketing Manger, ORGA (UK) Ltd, England - Tel: +44 (0)491 410997.

Milton Keynes Stored Value Card

Milton Keynes, the new city created in rural Buckinghamshire, England, to meet the dreams and aspirations of the 1970s, introduced Smart Card technology for its City Line stored value ticketing system on buses and trains in April 1989, making it one of the longest running applications of its kind in the country.

While the system has proved to be successful additional services originally envisaged, such as using the same Smart Card for parking and for entry to leisure centres, have not yet materialised largely due to local authority budgetary controls. In addition, the Borough Council has decided to introduce a new card with less functionality.

This is good news for California-based US^3, who are supplying 4,000 cards through their UK representatives Crystal (UK) Ltd.

Steve Mortimer, Public Transport Officer for the Borough of Milton Keynes, said they had changed cards for two reasons. "Firstly," he said, "the existing bus cards we have are to a fairly high specification, in fact higher then we need at the moment, so we have gone for a lower specification which is cheaper and obviously cost is an important factor in these days of very stringent local government finance.

"That does mean that it is going to be more difficult to use the new bus cards for other purposes as was originally envisaged, but there may be ways round that. We may have to think again as regards future specifications for future orders. Currently ideas for using Smart Cards for other uses within the Borough are on ice.

"The second reason for changing supplier was that the cost of the original Smart Cards had gone up very substantially," he said, but declined to give any figures.

The Borough Council's interest in the scheme lies in the administration of concessionary fares, and they are responsible for processing applications and issuing the cards. All resident senior citizens, disabled people and children or students under the age of 19 are eligible for concessionary fares for travel on the buses and, in the case of the students, on trains as well within

©1993 Smart Card News Ltd

the Borough.

Smart Cards are used in conjunction with a permit and club cards which show the holder's photograph. After paying a registration fee of £5 senior citizens can purchase multiple journeys in advance, for example, they can buy 10 rides at a time. As the current concessionary fare for them is 20p a ride they pay £2. Each time they travel 20p is deducted from the card. This enables them to travel at a substantial discount as the average adult fare is about 95p.

Schoolchildren and students pay 50p per ride or they can have a time expiring ticket which costs £6.70 per week, or pay £25 per month for unlimited travel within the Borough.

Today there are some 22,000 Smart Cards in circulation although about 5,000 are not in use on a regular basis. It is estimated that about 16,000 senior citizens have bus cards and about 75% use them regularly. Around 4,000 students and schoolchildren use them, while the County Council have a small number in use for children attending special schools.

The cards can be revalued at three locations in the city centre and on buses. Currently five local bus operators have a total of some 140 buses equipped with electronic ticket machines and they will be joined shortly by another two new operators. Last year, passengers eligible for concessionary fares made a total of 2.8 million trips on the buses and trains.

In addition, Milton Keynes City Bus, one of the main bus operators, use bus cards for their own commercial purposes.

Development of the technology

Roger Slevin, County Passenger Transport Officer for Buckinghamshire, said the County Council is starting to look at the development of the technology into other fields and car parking is under consideration.

However, he said, a co-ordinated electronic pricing system for car parking is not without opponents. "My concern as a transport person is that the parking people may find the attraction of the cheaper magnetic stripe card system for their application too great to resist," he said. "That may cause problems for the bus operators."

He believes the new card will prove to be satisfactory in operation and significantly cheaper, and that the Electronic Purse function can be extended to cover other applications once they have the right protocols in place to protect each user of the system.

"The acid test to us will be more to do with the mechanical integrity of the chip embedding than anything else. We have not been over-impressed with that on the existing card."

The main application has been on the concessionary fare side where data has been very important to the Council.

Discount Card

It is up to each operator what they do on a commercial basis with their own passengers. City Bus, for example, has its Discount Card which offers passengers 10% less than they would be paying if using cash for each journey.

The main advantage of the concessionary fares scheme is that it is easier to administer because there is irrefutable information available for accurately reimbursing operators whereas sample surveys are expensive and unreliable as passenger movements vary on a day-to-day basis. Other benefits have been a saving on administration cost and a degree of loyalty encouraged by the Stored Value

©1993 Smart Card News Ltd

system.

In the Milton Keynes system the driver handles the card for the transaction. In a relatively low usage situation this has been found to be successful as it provides a reliable transaction whereas if the passenger is involved, bearing in mind the dominance of the concessionary passenger, there may have been much more of the "fumble factor" to contend with.

The system, supplied by ERG Australia through AES Prodata, uses Datafare 2000 Smart Card readers and ticketing machines, and contact Smart Cards. Currently the card has 4K bit of memory, but the new one has 1K bit. There are a range of other cards, typically 64K bit as the driver card which is used to record transactions and download them to depot systems which consist of a network of PCs connected to a host computer.

New card details:

Type	Contact
Fabricator	US^3 Inc
Dimensions	ISO ID1
Contact location	Front
Chip manufacturer	N/A
Chip type	Memory+ logic
Memory type	EEPROM
Memory capacity	128 bytes
Standards	Not compatable with
ISO	7816-3
Security	Secure memory
access	

Contacts: Steve Mortimer, Public Transport Officer, Milton Keynes Borough Council, England - Tel: +44 (0)908 682367. Roger Slevin, County Passenger Transport Officer for Buckinghamshire, England - Tel: +44 (0)296 383751.

VeriFone (UK) Appointments

Tricia Carter has been appointed Regional Marketing Manager for VeriFone (UK) with responsibility for the marketing of all VeriFone's standalone and EFTPOS terminals and communications products in Northern Europe, the Middle East and Africa. She will continue to co-ordinate the international sales and marketing of the Gemstone EFTPOS terminal range, a position she has held since the launch two years ago.

The company has also announced the appointment of Steve Martin as Gemstone Sales Manager for the UK.

Cashcard Moves Offices

Cashcard Systems Ltd has moved offices from Newark, Nottinghamshire, England, to Welwyn Garden City. The address is Gate House, 37-43 Fretherne Road, Welwyn Garden City, Herts, AL8 6NS. Tel: +44 (0)707 396939,

Dialysis Patient Card

Smart Cards are being used to hold the records of patients suffering from kidney failure and who require dialysis treatment. The system is known as DIALYBRE and the software to operate the system has been installed by Circe SA in 150 French hospitals, 50 kidney self-dialysis centres, and the homes of many patients. So far more than 1,500 patients now carry their personal card.

The basis of the system is also installed in 25 hospitals in Spain, five in Switzerland and three in Canada, with the prospect of Germany and Italy joining the scheme this year.

The system was pioneered in France where it was tested for two years before

©1993 Smart Card News Ltd

being implemented on a large scale.

There are two types of cards in the system - the patient card, which is a 3K byte EEPROM card, contains identity, insurance and medical data; and the professional card, which is a 4K byte EPROM card, and enables medical staff (doctor, nurse, medical secretary) to access data contained in the patient card for reading and/or writing.

Patient mobility

With patient mobility increasing in Europe, the DIALYBRE card is an efficient means for secure data communication and patient follow-up, especially for patients using self-dialysis units at home or in specialist centres.

The card is regularly updated at each medical check. The patient completes his or her follow-up form directly on the display of his personal computer or telematic terminals. The data is updated in his hospital medical file secured by the health professional access card. Then the specialist prescribes in the patient card, the treatment and medical visits to come.

Complementary functions

Complementary functions are being investigated, including a follow-up programme for patients who have had a kidney transplant operation.

Each patient card can be accessed (read and/or write) at different levels depending on whether the dialysis centre is the patient's usual one or another medical centre, and on whether the medical professional is a doctor, a nurse or a medical secretary.

The DIALYBRE card memory has three main areas - identification of the patient in compliance with insurance specific requirements of each country, the coding of the medical files in accordance with the World Health Organisation and the European table of emergency codes, and the dialysis file which complies with the EDTA (European Dialysis and Transplantation Association) standards.

Card details:

Patient Card

Type	Contact
Fabricator	Gemplus
Dimensions	ISO ID1
Contact location	Front
Chip type	Microcontroller
Memory type	EEPROM
Memory capacity	3K bytes
Standards	ISO 7816-3
Comms protocol	T=0
Security	PIN
Cryptography	DES

Professional card

Type	Contact
Fabricator	Gemplus
Dimensions	ISO ID1
Contact location	Front
Chip type	Microcontroller
Memory type	EPROM
Memory capacity	4K bytes
Standards	ISO 7816-3
Comms protocol	T=0
Security	PIN
Cryptography	DES

Contact: Dr Bruno Lassus, Health Applications Sales Manager, Gemplus International, France - Tel: +33 42 32 51 21. Fax: +33 42 32 52 79.

Smart PIN-Pad from VeriFone

VeriFone, Inc., has announced the CM450 PIN-pad which reads and writes Smart Cards for retail, healthcare and other point of sale applications, enabling merchants to easily add Smart Card transaction capabilities to their existing VeriFone systems.

The device features a two-line 16 character display that can show both a prompt and the response entered by the user, and operator efficiency is enhanced by six colour-coded function keys that can be programmed to perform the most frequently used operations in a single keystroke.

The CM450 can communicate via an RS232 serial interface with VeriFone transaction automation systems, plus a variety of other devices, including PCs and electronic cash registers. For mobile applications, such as taxis, it can be powered from the car battery.

The CM450 supports a wide variety of industry-standard asynchronous microprocessor cards and synchronous memory cards from companies such as Gemplus, Bull, Schlumberger and DataCard.

Installations

Certified in France by Groupement des Cartes Bancaires for operation on the national Electronic Funds Transfer network, the CM450 is installed with TRANZ 460 EFT terminals and the system processes magnetic and Smart Card-based credit and debit transactions.

Takashimaya Singapore Ltd has selected the units for their new Smart Card-based retail payment system now being installed in their new department store. The system, which has been developed in conjunction with DBS Bank and Visa International will use Smart Cards from Gemplus International, France, and is the first system of its kind in Asia to incorporate Smart Card technology. The payment system will be expanded in early 1994 to include 120 other retailers in the Takashimaya shopping centre.

Contact: Tricia Carter, Regional Marketing Manager, VeriFone (UK) Ltd - Tel: +44 (0)895 824031. Fax: +44 (0)895 822473.

Table Top Terminal

A portable payment terminal from Bull, the QUESTAR 10, has been approved by Groupement des Cartes Bancaires.

Bull has now started marketing the product which will soon be seen on store counters and restaurant tables.

The terminal features a two-line LCD display of 16 alphanumeric characters and accepts both microporocessor and memory cards as well as magnetic stripe cards. It runs with EFTPOS software produced by Bull CP8, and security features include recording of the last 400 transactions and the capability of holding 4,000 black list entries.

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

Italian Electronic Wallet

The Italian Portofoglio Elettronico, or Electronic Wallet project, was developed by Olivetti and the Italian PTT, particularly the Post Bank sector, and is expected to involve the issue of 1.6 million contactless Smart Cards in the first phase of development.

Called the Postcard, the project started in 1989 with an initial supply of 1,600,000 contactless Smart Cards, 20 issuing centres, 210 ATMs, and 3,650 Card reader/writer terminals and involved 2,000 Post Offices.

Objectives

The objectives of the project are to automate a number of transactions at Post Bank (Bancoposta) offices, including the payment of pensions, and to improve the level of services to customers during and outside the normal bank opening hours; reduce cash sums in the transfer between users and the postal service, cut costs and reduce paper work, and increase the appeal of the Post Office as a bank.

Postcard is an electronic wallet and it works as a savings book, a cash withdrawal card and a credit card. It offers cardholders facilities to make cash deposits and withdrawals, full or partial credits or debits of postal, telegraphic and Bancoposta operations, pension payments (for those entitled to state pensions), and non-cash operations such as requests for balance statements, cash movement printouts, PIN changes at cash dispensers etc.

Banks, companies and other institutions can make special arrangements with the postal service to enable the cardholder, for example, to carry out withdrawal and payment operations.

Benefits

General user benefits include the availability of service in every Post Office, cash withdrawal facilities out of normal working hours, and security of data held in the card's memory. For pensioners the card allows them to make withdrawals on actual needs in Post Offices at any time, plus reducing the risk of being mugged.

The PTT administration sees a fall in cash sums in the transfer between users and the postal service, and a decreasing risk on uninvested funds and on cash handling. There is a decrease in transaction times and paperwork and an economy of management.

To guarantee compatibility with others systems, the card has a magnetic stripe which enables it to be used with the Bancomat (bank cash card) system.

The system uses Olivetti's C-less contactless Smart Cards under license from AT&T Smart Cards and Systems in the United States.

Contact: Maurizio Malinverni, Marketing Director, Olivetti Sixtel, Milan, Italy - Tel: +39 2 125 521704.

Singapore CashCard Project

Singapore's CashCard project using stored value Smart Cards aims to have nine million cards in circulation by the year 2000, and the way in which the scheme has been devised with the support of seven banks gives it a sound base on which to build success.

It has been planned by NETS, or the Network for Electronic Transfers, whose seven shareholder banks are Development Bank of Singapore (DBS), Keppel Bank, Overseas China Banking Corp. (OCBC), Overseas Union Bank (OUB), Post Office Saving Bank (POSBank), Tat Lee Bank, and the United Overseas Bank (UOB).

The project will build on the financial, technical and operational resources of the banks and thus already has a strong infrastructure in place. Collectively, the banks have a network of over 1,000 ATMs, more than 320 bank branches, and existing relationships with over 4,000 NETS retail outlets to provide consumers with convenient points for CashCard services and transactions and provide the foundation for expansion.

Cards will be available in values of $20, $50 and $100. The first card to be issued will be the bearer card which will support the basic CashCard functions. It will have a preloaded value and can be revalued at customer service centres, bank branches and service providers, CashCard vending machines and ATMs. The basic card will be used without a Personal Identification Number (PIN) allowing faster transactions.

At a later stage each of the banks will introduce their own composite cards, which in addition to acting as a CashCard, will function as an ATM card, NETS EFTPOS card and credit card. This card will have a magnetic stripe as well as a chip and a PIN will be required to activate debit functions.

When the system is fully implemented consumers will be able to use their cards at retail shops, taxis, fast food outlets, vending machines, telephones, car parks and cinemas throughout Singapore instead of paying cash.

The tender was awarded to Singapore Computer Systems Ltd who will be responsible for the development, installation and delivery of the system.

The estimated cost for the system over the next five years is said to be $12 million which seems a rather conservative figure for such a large-scale project.

SCS will act as the main contractor in the pilot project. Tandem Computer will supply the Cyclone R RISC-based computer system.

Gemplus Technologies Asia, the Asia-Pacific subsidiary of Gemplus Card International, France, will supply the Smart Cards.

Ingenico International are providing card readers and Information Sciences will supply Connex application software.

The NETS Steering Committee that examined the feasibility and implementation of the project were assisted by Anderson Consulting who have been retained to advise the committee in the development of the pilot system.

Pilot system

The system will be tested in a six-month pilot project starting in February 1994 and involving more than 200 service providers in the Ang Mo Kio district, one of the most heavily populated housing estates, and in the downtown financial district. It is planned that more than 40,000 cards will be issued by the banks by the end of 1994 and that around 500 CashCard Point-of-Sale terminals will be installed at both sites by the end of the trials.

Nation-wide launch

A full-scale nation-wide launch is targeted for 1995. By the year 2000 it is envisaged that all Singaporeans will carry at least one CashCard.

It is also planned to use the CashCard in the Electronic Road Pricing system when it is introduced in 1996.

Ernest Wong, Chairman of the CashCard Steering Committee said he hoped that the card would also be used to pay for travel on trains and buses.

He saw the Smart Card as helping to fulfil Singapore's vision of becoming an "intelligent" island, taking it a step closer to a cashless society.
Contact: Peter Hong or Mrs Nancy Lai, UOB, Singapore - Tel: +65 5393980/ Fax: +65 5393986. Tye Beng Hong, Gemplus Technologies Asia Pte Ltd - Tel: +65 7761989.

Seven Millionth Chip for Pay TV

Motorola's European Semiconductor Group has presented a commemorative wafer to News Datacom to mark the seven millionth microcontroller chip supplied for News Datacom's Smart Card-based Conditional Access and Subscriber Management Systems for Pay TV.

News Datacom supplied systems to BSkyB in the UK. Other contracts include the supply of systems for a direct digital satellite transmission network with up to 100 million subscribers, and Conditional Access and SMS for a satellite-based pay-TV system for up to five million subscribers.

Contact: Valerie Gopthal, News Datacom, England - Tel: +44 (0)628 74774.

Schlumberger Buys US Company

Schlumberger Ltd has acquired the privately-owned Global Tel*Link Corporation in Mobile, Alabama, USA, which designs, manufactures and markets public pay telephones and related equipment.

The US company will be managed by Schlumberger Technologies' Transactions Systems business group which includes Smart Cards and Systems, and the acquisiton of the US Company indicates that Schlumberger sees this as another opportunity to promote Smart Card pay phones in the North and South America markets. The group has allready supplied 80,000 pay phones to more than 40 countries.

Contact: Bertrand Dussauge, Communication, Schlumberger Technologies Transactions Systems, France - Tel: +33 1 47 46 62 47.

Vodafone to Launch EuroDigital

Vodafone, the UK-based operator of the largest cellular telephone network in Europe, is to launch its new pan-European GSM service with the name EuroDigital on 1 September.

The service is aimed at subscribers who want to roam throughout the UK and into Europe and who require enhanced speech security. Existing users of the Vodafone network will need a new cellular handset to use the EuroDigital service but will be able to transfer their current mobile phone number.

Hand portable phones are expected to be available shortly from Alcatel, Ericsson (2), Mitsubishi, Motorola (4), NEC, Nokia, Orbitel, Panasonic, Philips

©1993 Smart Card News Ltd

and Sony. For an introductory period, Vodafone is offering its service providers a £125 incentive payment to enable them to retail the new digital phones at competitive prices which they say is likely to be around £399.

Roaming facilities are now available in Germany, Sweden, denmark, Finland, Italy, Switzerland and Norway, to be followed shortly in France, Greece, Ireland and Luxembourg.

Vodafone MetroDigital

In another development, Vodafone will launch its MetroDigital Service on 1 October in London and the South East of England. Subscribers will be able to make local calls at rates lower than today's standard cellular call charges. They will be able to roam to all countries that offer a GSM service and will be able to make and receive calls using their digital GSM mobile phone in those countries.

The GSM system uses a Smart Card known as a Subscriber Identification Module (SIM) for authenticating the user and providing the data necessary to access the network and bill the cardholder. Vodafone SIMs are supplied by GAO (Gesellschaft fur Automation und Organisation) based in Munich, Germany.

Contact: Mike Caldwell, Manager, Corporate Communications, Vodafone, England - Tel: +44 (0)635 33251.

Visiopass From France Telecom

Visiopass conditional access system for Pay-TV from France Telecom is based on the D2MAC/Eurocrypt system with the subscribers' access rights recorded on a Smart Card enabling them to watch descrambled programmes.

The system is based on three principles:

* Encoding-scrambling where the programmes broadcast by the programme providers are encoded in D2MAC and scrambled under Eurocrypt control. Authorizations to access programmes are transmitted within the television signal.

* Descrambling in which the Visiopass terminal, which is both a decoder and descrambler, restores the signals corresponding to the access rights registered in the Smart Card.

* Transaction management which consists of registering access rights on cards associated with the terminals.

"PC" Smart Cards

France Telecom has developed a series of "PC" (Porte-Cle) cards and currently uses the PC2 cards in the Visiopass system. Each card bears an identification number and provides high security storage of Entitlement Management Messages (EMM) which are sent to it via the Subscriber Authorisation System.

©1993 Smart Card News Ltd

The card contains secret operating and management keys enabling it to activate descrambling and provide the terminal with the required information. Its microprocessor is divided into several zones allotted to the various providers so that each can manage its service autonomously, create new programmes and develop their own commercial strategy.

A feature of the card is that viewers can have a confidential code which they can set to prevent their children from watching unsuitable programmes, or to limit use of their card during their absence. The personalised card can be used by the subscriber, with all of his rights, on all terminals using the Eurocrypt standard.

France Telecom is currently developing two new types of cards. One is a less expensive, non-reusable card, for purchasing event-related programmes in pay-per-view. The second, called PC2.2, is re-usable and will allow "preview" in the case of impulse pay-per-view.

Visiopass is being used by the four main French cable operators (Lyonnaise des Eaux, CGV, Com Dev and France Telecom); for optional movie channels like Canal+, Canal+ 16/9, Cine-Cinemas and Cine-Cinefil. Recently France Telecom introduced pay radio services. All of these services are available with one Visiopass terminal and one Smart Card.

Contact: Alain Michelet, Direction de Programme Visiopass, France Telecom, Paris, France - Tel: +33 1 44 44 45 27.

D2-MAC/Eurocrypt Services

Channel	**Country**	**Satellite**	**Subscribers**
TV3, TV1000 Film Max (Kinnevik)	Sweden	Astra	400,000

Filmnet	Sweden	Astra	210,000
Canal+	France	TDF1/2	50,000
16/9 bouquet	France	Telecom 2	2,000
Optional programs	France	Cable	50,000
Pay-per-View	France	Cable-St Germain	3,000
BBC World Service TV	Europe	Intelsat	5,000
TV-Plus 16/9	Netherlands	Eutelsat	3,100
Business TV	Europe	Satellites	3,000
Kabel Kanal	Germany	Eutelsat	-

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.

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.

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.

Smart Card Europe, SAS Portman Hotel, London, England, 13/14 December.

Practical sessions, for example, on Smart Card security and requirements for an electronic purse, and case studies of current applications. Contact: Juliet Coe, IBC Technical Services - Tel: +44 (0)71 637 4383. Fax: +44 (0)71 631 3214.

Restaurant Loyalty Application

Cashcard Systems has developed a restaurant loyalty scheme that could significantly increase turnover. The application can run in a single restaurant or across whole chains, rewarding frequent diners with discounts, free dishes from the menu, or wines, and other incentives based on the frequency of visit or level of expenditure.

Similar schemes have been running in the United States for a number of years. In the California Cafe Restaurant Corporation's 11 restaurants, over 40,000 members were generated in less than two years, and more than 50 per cent of those remained "active" i.e. the member used his or her card within the last two months. Turnover is expected to increase by at least 15 per cent.

Members hand over their personalised Smart Card each time they pay a bill and points, awarded according to the cost of the meal, are written onto the card.

Points are also awarded for private parties, banquets and off-premises catering orders as well as restaurant meals.

In addition to being able to check their points totals, members can be sent regular statements summarising their totals. These can be used to remind members of their current entitlements and also to introduce new promotional offers.

While members have the benefits of their loyalty, the restaurateurs gain information on their sales and individual customers preferences which can be used to devise further tailor-made incentives.

"The California Cafe experience illustrates the potential of Smart Card-based loyalty schemes," says Cashcard's Chief Executive, John Kelly, who has already introduced loyalty schemes into pubs and family entertainment centres, including those at EuroDisney.

"We are currently talking to a number of major UK restaurant chains, and anticipate announcing significant pilot installations very soon," he said.

Contact: John Kelly, Chief Executive, Cashcard - Tel: +44 (0)707 396939.

©1993 Smart Card News Ltd

Smart Card Tutorial - Part 12

IC Card Security Life Cycle

The London Evening Standard reported this month of a new technique used in note counterfeiting of the US dollar. The method called "washing" refers to the concept of cleaning $1 notes with solvents to remove all traces of ink and then photocoping a $100 note onto the clean paper. Previously the task of creating paper with the right feel and appearance was considered far more difficult than the printing function. The modern colour laser photocopier has already become a serious counterfeiter's tool which is readily available at relatively low cost.

What is really apparent here is the problem of maintaining security throughout the life cycle of the $1 bill. The ability to work the paper for subsequent reprinting is clearly a major weakness. In our consideration of the Smart Card it is important to look at all stages in the life cycle of the card from conception to eventual destruction.

For the purpose of this part of the tutorial we will describe a hypothetical application for a finished Smart Card and will consider the complete life cycle and the appropriate steps to preserve the necessary security.

As we have mentioned previously security is a pervasive attribute and should encompass the complete application process. In any secure application there will be a mixture of security mechanism and procedural controls. Both are important for clearly the use of the strongest cryptographic mechanisms will be totally invalidated by insecure handling of the keys.

Let us consider a Smart Card with a single application that is used as a financial post payment card. This card will be used by the consumer to buy goods from the retailer. The card will check the users PIN and generate a certificate to authorise the transaction process. This will enable the retailer to receive funds from the card issuer who will correctly debit the customers account. Each of the stages in the card life cycle is shown in figure 1.

There are of course many variations for the IC card life cycle depending on the requirement of the particular application. In this example we are more concerned to show the principles rather than describe any particular scheme. Also for the purpose of this discussion we have simplified the cryptographic key management which we will describe in more detail in the next part of the tutorial.

In figure 1 we show a number of stages described by the role of an entity in the card life cycle. One of the key principles to be achieved is security segregation such that no one party can break the security controls.

The first stage in the process relates to the design of the operating system and the application. Although it would be possible to put the complete application in the ROM mask we will consider here two separate components. The operating system might even be general purpose but in any event it is clear that our life cycle must take this into account since it forms the base upon which the security of the application depends.

The chip design is of course fundamental to the overall security of the IC card. Much has been written about the physical security offered by a Smart Card. Anyone who doubts the sophistication of the technology required to manufacture integrated circuits would be advised to spend a day with one of the major semiconductor suppliers. You really cannot make a modern chip in your back bedroom. In fact you would find it very difficult to establish a semiconductor manufacturing operation

©1993 Smart Card News Ltd

without dealing with one or more of the small number of specialized equipment manufacturers. The environmental controls for such a facility are in themselves an extremely sophisticated operation where costs are calculated in the millions of dollars.

For the design and manufacture of the chips we are concerned with a complete material audit. Given the assumption that the attacker cannot make the chips then he will be obliged to steal them if he wishes to mount any form of counterfeit operation. The concept of "washing" will be referred to later. It is accordingly a requirement upon the chip manufacturer to account for all the chips that are made, some of which, due to yield failures, will need to be destroyed.

©1993 Smart Card News Ltd

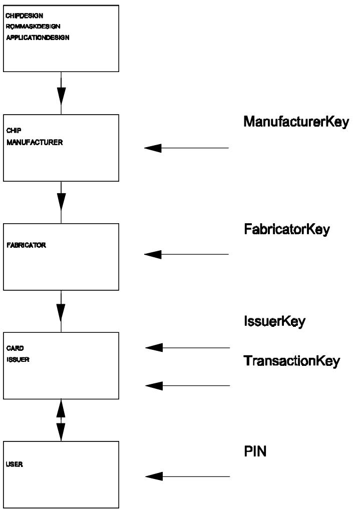


Fig.1.FinancialPostPaymentCardLifeCycle

The design and development of the ROM mask operating system and the application software need to follow the usual principles for any software to be used in security applications. This is in itself a non trivial task but at least the memory available in Smart Card chips is relatively small which forms a limit on the eventual size of the software. The integrity and correctness of software code is a major subject in its own right but it is clear that the design methodology and subsequent testing must allow for both positive and negative testing. By positive testing we refer to checking that the functions defined in the specification are processed correctly. In the case of negative testing we are concerned to know whether the software does anything in addition to that defined in the functional specification. It is readily apparent that this negative testing is a difficult problem and in general cannot be guaranteed complete.

When the ROM mask software has been developed and tested the code is given to the chip manufacturer usually on an EPROM chip or on a floppy disk. He will then return an implementation of the code for cross checking before manufacturing the batch of chips. This is in itself a useful integrity check but clearly one normally requires this code to be kept confidential and therefore its distribution should be carefully controlled by the appropriate procedural measures.

The application software will normally be designed and developed by a separate path. The resultant code having been tested will be loaded into the PROM memory by a subsequent process. The chip manufacturer will produce a batch of chips containing the supplied ROM code (a test batch is normally produced for initial testing). The last part of the chip manufacturing process involves a test of the chip. At this stage the chip manufacturer would insert a secret manufacturing key into the EEPROM memory. The software in the ROM will have been designed to inhibit all functions without the correct presentation of this key. As such the chip is effectively locked.

The batch of chips is distributed to the fabricator whose task is to embed the chips into the plastic card. As we have discussed previously this involves a number of processes, where there will be some (nominal) failure rate. The role of the fabricator varies considerably between the various customers for their services. As a very minimum the fabricator must test the complete IC card to ensure its operational state. In some cases the fabricator completely personalises the card to the requirements of the issuer. For simplicity we will assume this latter position. In order to undertake this software identification and personalisation process the fabricator needs to `unlock' the chip by entering the manufacturer's key. As the last step in the personalisation process the fabricator will reset the manufacturer's key with a fabricator key before distribution to the card issuer.

The card issuer on receipt of the personalised cards will unlock the card using the fabricator key and will set the PIN for the user and the transaction key that will be used as part of the final application. The issuer will also reset the fabricator's secret key to the card issuer's secret key. The card is now enabled for operation and is distributed to the user.

The customer may use this card in a point of sale environment where the correct entry of the PIN is necessary before the Smart Card will generate an authentic transaction certificate. The retailer provides the transaction details (which will include the consumers account identifer) and the certificate to the issuer who will credit the retailers account and debit the customers account accordingly.

If the customer fails to enter his PIN correctly for a predefined number of trials then the application on the card will lock up. When the customer returns the card to the issuer then the application can be reset by means of the issuer key. Under normal operation the card should continue functioning until the expiry date set in the card data file is reached. At this stage the card will cease operation.

Now we can return to the `washing' concept. Can an attacker take the card at any stage and reprogram the data to his advantage. At each point in the life cycle the data on the card is protected by a secret key. Without knowledge of this key it is not possible to modify any of the card data in an unauthorised way. So here we have changed the attacker's work function to that of obtaining a security key held in the EEPROM memory compared with that of using chemicals to wash the $1 bill. I know which I would find easier to do!

Next month. Cryptography and key management.

David Everett

Correction

In last months newsletter we incorrectly published the telephone and fax number for Card Systems (UK) Ltd. The correct numbers are as follows; Tel: +44 (0)273 495034 Fax: +44 (0)273 495123.

Bell-Fruit Patent Judgement

In the Patents County Court in London last month, Bell-Fruit Manufacturing Co. Ltd, of Nottinghamshire, England, was granted an injunction restraining Twinfalcon Ltd (formerly known as Feature Electronics Ltd) from infringing their patent on the use of pre-paid credit or debit cards with amusement machines.

The court also ordered Twinfalcon to give BFM all physical materials offending against the injunction, along with details of all the company's sales contacts and prospects for its "System Gold." Damages, still to be assessed, were awarded to BFM, and Twinfalcon was ordered to pay costs in the case.

©1993 Smart Card News Ltd

The patent was granted to BFM more than 15 years ago, and has been licensed to leisure industry Smart Card specialists Cashcard Systems Ltd, since 1991.

"We are obviously delighted with this emphatic result," said BFM Technical Director, Dale Chadwick.

John Kelly, Chief Executive of Cashcard Systems, commented: "This rids us of an unauthorised competitor and sends a clear message out to any other organisation thinking of infringing BFM's patent."

Contact: Dale Chadwick, BFM, England - Tel: +44 (0)602 706707.

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

□ UK £375

□ International £395

□ Please invoice my Company

□ Cheque enclosed

□ Please charge my credit card

Visa/Mastercard/Eurocard/Access

Name____________________________________

Position__________________________________

Company_________________________________

Address__________________________________

____

Tel.______________________________________

Name________________________________

Address______________________________

____

Card No.______________________________

Expiry date____________________________

Signature____________________________

Fax.____

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

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

©1993 Smart Card News Ltd

ORGA Launches SIM-Simulator

Smart Card specialists, ORGA, has announced the SIM-Simulator, a PC-based tool used in the test and type approval of handsets for GSM (Global System for Mobile Communications).

A key component in the GSM service, currently being introduced throughout Europe and parts of Australasia and Africa, is the SIM (Subscriber Identity Module), a Smart Card which is inserted into the mobile phone when the user is making a call.

Paul Hill, Marketing Manager for ORGA UK, says: "Type approval of handsets has become quite a hot topic in GSM over the last few months. Handsets have been undergoing interim type approval for some time, however, the interim approval has not tested the interface between the handsets and the SIM. Errors at the interface between the card and the terminal can cause irrevocable damage to the SIM. We have designed the SIM-Sim to specifically test the logical and electrical characteristics of the interface and thereby identify any problems with the handset's design."

The SIM-Simulator incorporates a high speed optical fibre link to a transputer controlled measurement unit and is capable of (200MHz) timing measurement and electrical characterisation. It simulates the functional behaviour of GSM SIM chip cards with the T=O transmission protocol and the application defined in GSM Recommendation 11.11. The simulation includes the definitions of the data fields and data structure, monitoring the low level data transmission, manipulation of the command set, error logging and automatic go/no-go testing.

The unit has been developed in accordance with the requirements of GSM Recommendation 11.10 and is now undergoing formal approval. It has already been supplied to a number of network operators including Cellnet, Detecon, Vodafone, Danish Telecom and France Telecom and approved GSM testing facilities including BZT and RW-TUV.

Jon Twigg, Technical Marketing Manager at ORGA UK, comments: "The SIM-Sim is an exciting new product for ORGA and with the new GSM network starting to come into full operation we are confident that it will become a vital, if not mandatory, component in the type approval of handsets."

Contact: Paul Hill, Marketing Manager, ORGA UK Ltd, England - Tel: +44 (0)491 410997.

©1993 Smart Card News Ltd