Bank Passbook and Purse in Indonesia

Bank Rakyat Indonesia this month introduced SMARTBRI, a multi-application (electronic passbook and purse) banking card to provide nationwide off-line banking for its customers living or travelling through the entire archipelago stretching across 2,000 kilometres from east to west and consisting of 13,500 islands.

The Smart Card, from Gemplus Card Technologies Asia, acts as a banking passbook which holds the electronic equivalent of a hard copy passbook and can be used with the bank's ATM's. A purse application co-exists with the passbook application to hold the electronic equivalent of cash.

Continued on page 163

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 14 - Cryptography and Key Management continued.

CONTENTS

This Month

We have produced the first part of a special report on microcontrollers for Smart Cards. We will continue with part 2 next month.

Smart Banking in Indonesia

Continued from page 161

The SMARTBRI card is set to revolutionise banking in Indonesia because of the country's widespread geographical area and an overloaded telecommunication infrastructure. Indonesia does not have a card culture like the USA or European countries and its banking networks tend to be restrictive because of communication problems and often customers have to return to their local branches, where they hold their accounts, to effect even a simple withdrawal transaction.

Due to the security offered by the SMARTBRI card, the system is able to work without the need for on-line communication with the central host computer. Apart from the savings in cost, it allows banking services to be made available in places where it was not previously possible because of the lack of communication lines, and also allows transactions to be carried out at any branches in the system off-line.

The System

The customer can obtain a SMARTBRI upon successful application for an account with the bank and can use it as a traditional banking passbook and as a debit card. The chip in the card contains the current passbook data and a certain amount of electronic money that can be used for small payments such as public transportation, public pay telephones, and in cafeterias, retailers and vending machines etc.

The cardholder can transfer money from the passbook account to the electronic purse through an ATM or at terminals in bank branches. Service providers accept the electronic purse as a means of payment, and Bank Rakyat Indonesia assures clearing and settlement of all transactions between various service providers working in partnership with the bank.

Benefits

Benefits for BRI are seen as: additional fee revenue, new source of on-going interchange income, share of float pool, better customer retention, increased market share, new market opportunities, better customer service via the Smart Card, and value-added services for customers.

Service providers benefits are: enhanced customer service, new market opportunity from increased traffic, incremental sale volume, lower operating cost from cashless handling, reduced fraud risk, and differentiation from competitors.

Cardholder benefits are: added payment convenience, fast and easy payment process, reduced need to carry cash, availability of banking services, and added safety and privacy.

The project was implemented as a joint development involving BRI, Gemplus Technologies Asia and PT Askom (Gemplus local Indonesian agent).

Gemplus delivered 20,000 3K byte EEPROM Smart Cards to BRI for the launch. The card provides all the necessary security functions such as authentication of card, terminal and cardholder. Message authentication is also provided to ensure that transactions are not tampered with. Control functions like authorization of terminal, accumulated transactions limit and a log of transactions are also implemented with the help of the Smart Card.

One of the features of the card is that it can have up to three independent PINs, allowing different family members to share the card if necessary with each PIN having a pre-setable withdrawal limit per day.

Card details:

Type	Contact
Fabricator	Gemplus
Dimensions	ISO ID1
Contact location	Front
Chip type	Microcontroller
Memory type	EEPROM
Memory capacity	3K bytes
Standards	ISO 7816-1/2/3
Comms protocol	T = 0
Security	PIN
Cryptography	DES

Contact: Remey de Tonnac, Gemplus Technologies Asia, Singapore - Tel: +65 776 1989. Fax: +65 773 0648.

DirekteBanken Super Smart Card

Den Norske Bank has set up the first telephone bank in Norway, called DirekteBanken, which uses a Super Smart Card. The scheme was launched in November last year and so far 2,000 cards have been issued,

Speaking at the European Smart Card Applications & Technology (ESCAT) Conference in Helsinki, Finland, early this month, Ms Elin Sjodin Drange, General Manager, DirekteBanken, said the project began with a preliminary survey within the bank in the autumn of 1991 which concluded that there was a market for telephone banking services in Norway, and planning started in February 1992.

The concept was that all banking services required by customers would be made available by simply dialling a free call telephone number; and that banking hours would be suitable for customers with opening hours from 7 am to 8 pm on weekdays and from 10 am to 3 pm on Saturdays.

The service is presented as an option. Customers can either use the traditional branch network of Den Norske Bank or become a customer in DirekteBanken which is a complete bank with ATM cards, MasterCard, current and investment accounts, and loans established as DirekteBanken products. Customers also receive statements of account.

Customers "subscribe" for banking services by paying a fixed annual fee of 690 Norwegian Crowns (approximately £70) which covers the cost of obtaining and using ATM cards in both ATMs, EFTPOS terminals, bank and postal giro charges and the use of ordinary cheques in Norway.

Security

Security safeguards for customers and the bank are provided by a digital signature developed by NCR, the bank's EDP department, Intellect, and Bergen Data Consulting, an EDP consultancy.

The Smart Card, which is supplied by Intellect, of Western Australia, is the same size as an ATM card but thicker and contains a 1 x 20 character display and a key pad (10 numeric keys and four functional keys), replaceable batteries and a microprocessor chip.

The system uses a challenge and response system to verify the identity of the customer. When a cardholder makes a free phone call to the bank, he activates his Super Smart Card by entering his secret PIN, and tells the service operator his customer number which is written on the card. At DirekteBanken the operator enters this number on the PC and reads a random number of four digits over the telephone to the customer who enters it on his card.

This number is encrypted into a unique six figure digital signature by the card using the DES algorithm. When the customer reads this number off the card's display, the operator enters it on the screen and sends it for verification by the bank's IBM mainframe computer operating under MVS and secured by the ACF2 security software package. The verification routine cannot produce a digital signature, it can only verify that the signature produced by the customer is correct.

Even if the line has been tapped or monitored, no other person can gain access and carry out transactions in the customer's name by giving an "over-heard code" because this would be recognised by the security system as an "already used code."

The card ensures that the bank is dealing with the right customer, but in addition a voice log is taped of conversations about the transactions as proof of what the customer ordered and for future reconstruction/documentation.

Future Card

The development of an "ordinary" Smart Card (0.8 mm thick) with a magnetic stripe is seen as more convenient as a multi-function card offering both security and standard banking services in one card as well as the ability to use it in smart pay phones and standard equipment supplied with Smart Card readers.

Contact: Ms Elin Sjodin Drange, General Manager, DirekteBanken, Den norske Bank AS - Tel: +47 55 22 34 40. Fax: +47 55 22 34 30.

German Banks Project

The German banking industry under ZKA - Zentraler Kredit Ausschuss - which deals with subjects of common interest to all the banks, are considering equipping their Eurocheque card with a multi-function chip.

ZKA have approached card providers to come up with concepts for discussion to see if they meet the requirements of the banks.

While there is much interest in an Electronic Purse in Germany, Goachim Fontaine, of ZKA, said: "We really cannot say whether a chip card in Germany will contain a chip for a purse or not. What we will do is to introduce a multi-functional chip which will obviously have the ability to bear a purse, but it need not."

The electronic cash system in Germany is an on-line debit system. It is an EFTPOS system using debit cards, especially the Eurocheque card, and every transaction is verified with a PIN and sent on-line to an authorisation centre.

Off-line Facilities

Based on that system, ZKA are planning to have off-line facilities for which they need a Smart Card to verify the PIN and to have some parameters within the chip to decide when on-line authorisation is necessary. The long term aim is to have 80 per cent transactions processed off-line.

Another objective is to have telephone functionality with the chip card and discussions are currently taking place with Deutsche Telekom.

Contact: Goachim Fontaine, ZKA, Germany - Tel: +49 221 166 3203.

La Poste EP Project?

La Poste, the French Post Office, is expected to announce shortly that it will go ahead with a nationwide Smart Card Electronic Purse project.

The plan has been under discussion for a long time with La Poste hoping for support from the French banks who have all adopted Smart Cards for their customers. However, it is believed that the banks have been reluctant to share their lead in Smart Card technology and that La Poste will launch an independent but compatible card scheme.

This move will further boost the penetration of Smart Cards in France as La Poste will be looking for service providers. A possible early alliance may be with France Telecom with whom La Poste has close ties and is a major outlet for the sale of Smart telephone cards.

Card and equipment suppliers will almost certainly be French. If La Poste is to take advantage of compatibility with the French banks it will have to take account of the BO′ card operating system developed by Bull CP8 with Groupement des Cartes Bancaires and licensed to a number of other French card suppliers.

Sovereign Payphone

The Sovereign Payphone system from Cambridge Telephones accepts most of the debit and charge cards available in either magnetic or chip card format. It was demonstrated at a Manchester card fair this month using prepaid Smart Cards from Delphic Card Systems, the recently formed joint venture company of TRT Philips Smart Cards & Systems and De La Rue Card Technology.

All card transactions, except prepaid chip cards, are sent to a Front-end Transaction Processor (FTP) for validation. Card numbers are checked against master hot lists and may be authorised locally or sent to a card authorisation centre for approval above predetermined floor limits.

Contact: Colin English, Sales and Marketing Manager, Cambridge Telephones, England
Tel: +44 (0)480 494900.

Amphenol Appointment

Dr Ulrich Meyer has been appointed Vice President Marketing/Engineering with the connector supplier Amphenol-Tuchel Electronics GmbH in Heilbronn, Germany.

Post Office Smart Card Plans

Post Office Counters plan to start offering Smart Card payment facilities at a substantial number of their UK offices starting in May or June 1994. They are aiming to attract and meet the demands of the major utilities - electricity boards, the privatised water companies and British Gas.

Their £19.5 million investment programme to equip 5,000 sub post offices with multi-function Advanced Payment Terminals (APTs) and upgrade existing terminals in 700 Crown Offices (SCN April, 3) is on schedule. APTs have been installed in 620 offices in South Wales and Yorkshire, England, and work has started in Scotland where they expect to equip 700-800 offices before Christmas. The next area to be tackled will by North East England which will bring the total number of offices equipped to around 2,000 by the end of April 1994.

Ian Gair, National Sales Manager for Post Office Counters, said: "We are working with two suppliers to jointly develop two different technologies - a Smart Key and a contact Smart Card - which we expect to be able to offer to our major customers about May or June of next year."

Benefit payments

Meanwhile, Post Office Counters are discussing with the Department of Social Security the feasibility of using plastic card technology for the payment of Government benefits.

Claire Choudhury, Post Office Communications, said: "We are only at the discussion stage but we are installing new APTs which are able to take Smart Cards in our offices throughout the country."

Benefits payments make up a substantial part of the business of Post Office Counters with £13 million collected every week. Of this total, pensions account for around £7 million, and child benefit about £3 million. The use of Smart Cards to pay benefits electronically would speed up the service and offer convenience and security to the customer, but it remains to be seen if the DSS will favour Smart Card technology or opt for cheaper and less secure magnetic stripe cards.

Contacts: Ian Gair, National Sales Manager - Tel: +44 (0)71 922 1242; Claire Choudhury, Post Office Communications - Tel: +44 (0)71 320 7048.

European Pay-TV Joint Venture

News International Plc, the European subsidiary of The News Corporation Ltd, and Teledirekt, a wholly-owned subsidiary of PRO 7 Television GmbH, the third largest private television broadcasting station in Germany, have formed a joint venture company to provide one of the most advanced forms of pay television services in Europe and will run a subscriber management operation based in Munich, Germany.

News Datacom, UK-based subsidiary of News International, will develop and supply the technology and conditional access services

The joint venture company will provide subscriber management and conditional access services for foreign language television channels. Subscribers located in Germany, Austria and Switzerland will be able to receive these television channels from January 1994.

Contacts: Jane Reed, News Corporation, England - Tel: +44 (0)71 782 6018. Dr Georg Kofler, PRO 7, Germany - Tel: +49 89 95001-281.

Cristel Represents Racom

Racom Systems Inc., of Englewood, Colorado, USA, has appointed Cristel UK Ltd as the first European representative for its recently introduced contactless "In-Charge" Card which combines wireless data transfer technology with patented Ferroelectric RAM (FRAM) to achieve the faster memory access times needed for such applications (SCN June, 1993).

The "In-Charge" card, developed jointly by Racom Systems and Ramtron International, is seen as having wide ranging uses in applications such as public transport ticketing, access control and factory automation.

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

Smart Card Tutorial - Part 13

Cryptography and key management

The particular advantage of a Smart Card with its inherent processing capability is the opportunity to implement cryptographic mechanisms within the Smart Card. As we have mentioned previously the IC chip may be considered as a tamper resistant module which offers significant resistance to physical attack. In this part of the tutorial we are going to take an overview of cryptographic algorithms and mechanisms along with their attendant key management considerations.

Although a large number of cryptographic algorithms have been developed over the years, in practice only two are in common use for financial applications which is still the main customer for such security. The DES (Data Encryption Standard) algorithm was proposed in 1977 and the RSA (Rivest Shamir and Adleman) in 1978. These algorithms represent two different classes of operation, DES is a symmetric algorithm whilst RSA is an asymmetric algorithm. The difference is easy to understand by referring to fig. 1. The input message is enciphered by means of key 1 to produce a cipher. The original plain text may be recovered by means of key 2. If both keys are the same (i.e Key 1 = Key 2) then the cryptographic process is symmetric. This is the more obvious operation and means that the sender and receiver of secret messages must share a common secret key.

The asymmetric situation is a relatively new concept first proposed by Diffie and Hellman in 1976 and represents the case where the two keys are different (but clearly related) and where it is not practically feasible to derive one key from a knowledge of the other. This form of asymmetric algorithm is often referred to as public key cryptography where it is assumed that one of the keys may be made public. Thus referring to fig. 1 it would be possible to make key 1 public for a particular entity. This means that anyone could produce a cipher using key 1 but only the owner of key 2 would be able to recover the original plain text. It should also be noted that the entity that creates the cipher using key 1 is equally incapable of reversing the process.

This concept of public key cryptography is an intellectual delight because at first sight it seems impossible. However it actually brings the whole concept of modern cryptography into perspective in as much that it shows the principle of the work

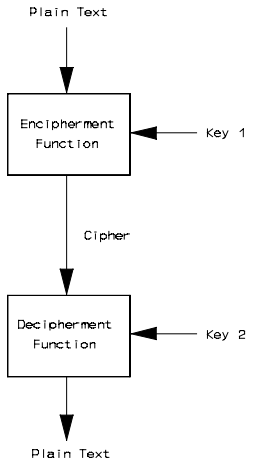

Fig 1. The Fundamental Cryptograghic Process

function. These cryptographic algorithms are not absolutely secure but offer a resistance to attack defined by the relevant work function. In the case of the symmetric algorithm which uses a simple (secret) key, an attack could be based on trying all the possible keys until a sample of plain text and cipher text produce a direct match. The work function is then based on the time required on average to exhaust the total key space.

If we refer to the asymmetric case then we can show the concept of the work function by means of a simple analogy. Let us consider a message encoding and decoding system that is based on the use of dictionaries. The plain text message is represented by the English language whilst the cipher text may be represented by French (we conveniently ignore any similarity between some English and French words). The public key encoding process is implemented by giving all participants a dictionary that defines English to French only. This means that everyone can produce a cipher by turning an English message into French. However without the other side of the dictionary (French to English) there is a significant but not impossible work function to recover the original message. For each French word the whole dictionary would need to be scanned in order to find the English equivalent. In

this simple analogy the intended receiver of these messages would be given the French to English dictionary. Clearly we can also build up a system by having other dictionaries (e.g English to German, English to Italian, etc) where all

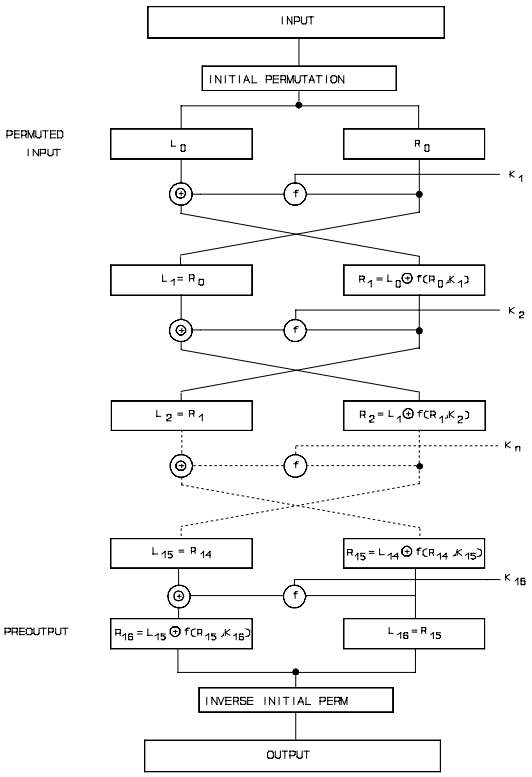

Fig 2. The DES Algorithm

participants have the forward dictionary but only one has the reverse dictionary.

This conveniently leads us to a further concept of the one way function (OWF). This is very important in modern cryptography and underlies the use of many modern mechanisms. The principle is very straightforward and may be considered analogous to the lobster pot. The design of the pot is such that it is very easy for the lobster to enter the pot through the entry tube but the reverse process is practically infeasible (to even the most athletic lobsters). It is the next stage that is also important, the fisherman recovers the lobster by means of a trap door in the bottom of the cage for which only he has the key. This is just another way of looking at the public key algorithm as a one way function with a trap door. In all cases of course we can show an appropriate mathematical representation. The DES algorithm is shown in fig. 2.

The DES Algorithm

The DES algorithm was initially published as FIPS publication 46 (USA Federal Information Processing Standards) in 1977. The algorithm is designed to encipher and decipher 64 bit blocks of data using a 56 bit key. The process is shown in fig.3. The block to be enciphered is subjected to an initial permutation (IP). The output of this operation is then iterated 16 times by the following operation,

$$L' = R$$
$$R' = L \oplus f(R,K)$$

Where L = left most 32 bits of previous step
R = right most 32 bits of previous step
$f(R,K)$ = function of key and R

at the end of this loop the result is put through a final inverse permutation (IP^{-1}) to produce the 64 bit output.

The decipherment process operates in the same way except the key function is used in reverse order.

The RSA Algorithm

The RSA algorithm has an attractive elegance about it, probably because of its apparent simplicity as shown below,

$$C = M^e \text{ Mod } N$$

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

Where:

M = Message Block; C = Cipher Block
e = Encipherment key; d = Decipherment key
N = Modulus (product of two primes p and q)

and
de = 1 Mod lcm(p-1, q-1)

Like all cryptographic algorithms there is much

under the surface and there are a number of conditions that must be met in order to implement the algorithm correctly. This need not concern us here but we can look at an example using trivial numbers just to see the algorithm in operation,

let M = 4
p,q = 5,11
N = 55 (p*q)
choose e = 3
d = 7 (de = 1 mod 20)

Encipherment
$C = 4^3 \bmod 55 = 9$

Decipherment
$M = 9^7 \bmod 55 = 4$

(note: $9^3 \bmod 55 = 14$)

In practice the size of N and d are typically 2^{512} which is about 154 decimal digits. These numbers are difficult to process quickly with the 8 bit CPU's commonly found in the Smart Card microcontroller. We will return to this subject in more detail later in the tutorial.

Security Mechanisms

There are a number of security mechanisms that can be used in Smart Card applications but of particular interest are those mechanisms that relate to data integrity and authentication. The cryptographic check values (CCV) and digital signatures are the most widely used mechanisms, sometimes the term signature is applied to both mechanisms.

Cryptographic Check Values(CCV)

The use of the DES algorithm to calculate CCV's is well established. The often used MAC (Message Authentication Code) was originally defined by the ANSI X9.9 standard and subsequently adopted as the ISO 8730 standard for finacial messages.

This check value is generated by using the DES algorithm in cipher block chain mode as shown in fig.3. The standards referred to above use the most significant 32 bits of the final output as the check value or MAC. If necessary the final message block is padded out with zeros, so that each input block is always 64 bits. The receiver checks the cryptographic check function by applying exactly the same operation.

The primary purpose of the CCV is to provide a data integrity function that ensures that the message has not been manipulated in any way. This includes both the modification, addition and deletion of data. In itself this function does not provide any such assurances on the addition or detection of whole messages. The necessary security can be acheived however by the use of sequence numbers which are incorporated within the CCV.
The cryptographic check value also supplies some assurance of source authentication depending on the key management architecture. As a trivial example where two correspondents (only) share the secret DES key then the receiver can be assured of the authentication of the sender. The CCV does not however provide the property of

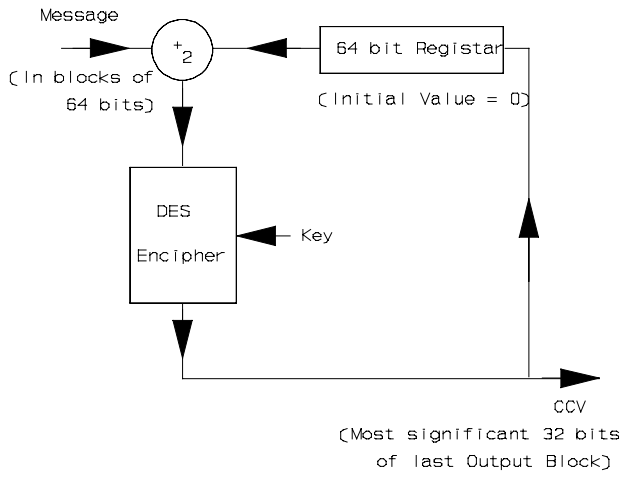

Fig 3. The Cryptographic Check Value (CCV)

non - repudiation. In the example shown here the receiver has the same secret key as the sender of the message and clearly is capable of modifing or inserting a new message. Under such an arrangement it is difficult to prove the source authenticity of the message to a third party. This is better provided by the use of an asymmetric cryptographic algorithm.

David Everett

Next month. Part 14 - continued.

Dr SIM from ORGA

ORGA Card Systems UK has launched Dr SIM, a new PC-based solution for testing and diagnosing problems associated with Smart Cards used as SIMs (Subscriber Identity Modules) in the GSM (Global System for Mobile Communications) network and in PCN (Personal Communications Network) services.

The new product, which allows users to test Smart Cards and then either repair them or load them with specific customer oriented service functions, has already attracted orders for several thousand of the units from mobile phone service providers and dealers in Germany.

Key components

It comprises two key components - a card reader and PC software. The card reader comes complete with a two line alpha-numeric display and a keyboard, and the software, which is available in either DOS or Windows, has a user friendly interface which allows all existing Smart Card SIMs as well as plug-in SIMs to be handled.

Dr SIM software supports the following functions: card testing, card repair; editing of short dial numbers, data service parameters, preferred networks, preferred languages; display of short messages, IMSI (International Mobile Subscriber Identity), service profile; changing, disabling and enabling the PIN; copying subscriber data from one GSM card to another; printing subscriber data; transferring predefined short dialling number data in the card; entering the secret number on the card via the card reader or PC keyboard.

The system requires an IBM PC or compatible, minimum 560Kb RAM for the DOS version and 2MB RAM for Windows, free COM1 or COM 2 interface, 286 processor for DOS and 386 processor for Windows, Hercules EGA or VGA graphics card, DOS 3.3 or higher or Windows 3.0 or higher.

Marketing Director, Paul Hill, says: "Dr SIM allows GSM/PCN network operators and service providers to ensure optimum customer service on all SIM cards. Several thousand of these units have already been ordered by service providers and mobile phone dealers in Germany for the D1-Netz and the concept looks set to take off in a big way in the UK."

Contact: Paul Hill, Marketing Director, Orga Card Systems UK - Tel: +44 (0)491 410997.

New Chipcard Acceptor

Amphenol-Tuchel Electronics GmbH, of Heilbronn, Germany, has released its Superflat Chipcard Acceptor with manual card eject.

Designed to accept cards compatible with ISO 7816, the unit has a compact profile and features a revolutionary card ejection system. The Smart Card is inserted into the acceptor until flush and latched behind the card entry lip. To eject the card, the user simply lifts upwards on the eject tab on the underside and the card springs out towards the user.

Envisaged applications are for mobile telephones, portable terminals, Point of Sale, and banking.

Contact: Ralf Stegmann, Amphenol - Tel: +49 7131 486303. Fax: +49 7131 486400.

Smart Loyalty Terminal

The Stellar Smart Card Loyalty Terminal, announced by HTEC, of Southampton, England, uses either memory or intelligent Smart Cards and offers the option of an operator Smart key.

The Stellar reader/encoder terminal employs encryption and security techniques developed by HTEC which they say allows the lowest cost memory-only cards to be used with confidence for loyalty or payment schemes. It will also handle microprocessor Smart Cards with on-card security access, optionally using PIN protection. The terminals will retail at around £500 with discounts according to quantity ordered.

Contact: Mike Moody, HTEC, England - Tel: +44 (0)703 581555. Fax: +44 (0)703 671173.

ESCAT Award for Gemplus

The ESCAT (European Smart Card Applications & Technology) Conference prize for the most innovative Smart Card accomplishment of the year (1992) has been awarded to Gemplus Card International, France, for the "Interface of 7816 Smart Card to PC Memory Card Interface," known as the Gemplus Pocket Reader.

The unit plugs into the PCMCIA slot on any portable PC turning it into a Smart Card reader allowing access to the card to collect data. Data stored in the reader can later be processed into a PC or printed out.

ESCAT chairman, Juhani Saari, presented the award to Gemplus representative Tim Baker at the ESCAT banquet dinner in Helsinki, Finland, early this month.

Smart Card Microcontrollers Part 1

Manufacturer	Atmel	Hitachi	Hitachi
Type Number	AT88SC54C	H8/310	H8/3101
Microcontroller Core	80C31	H8/300	H8/300
Architecture	8 bits	8 bits	8 bits
ROM	None	10K bytes	10K bytes
EEPROM	8K bytes data 8K bytes program	8K bytes	8K bytes
ECC	Yes	No	No
Page Write	Program Area	32 bytes	32 bytes
EPROM	-	-	-
Write cycles endurance	100K Data area 1K Prog area	10K (70C; 5V)	10K (70C; 5V)
RAM	768 bytes	256 bytes	256 bytes
OTP memory	Any data area All Prog area	Any page	Any page
Voltage	5V	5V	5V
Max clock speed	11 MHz	5 MHz (Internal)	5 MHz (Internal)
Max current	200mA	40mA	20mA
Sleep mode	-	Yes (reset to clear)	Yes
Special functions	Modular arithmetic coprocessor	None	None
Die size	N/A	N/A	N/A
I/O ports	1	1	2
Availability	Q1 1994	Now	Now

Motorola	Motorola	Motorola	Motorola
MC68HC05SC11	MC68HC05SC20	MC68HC05SC21	MC68HC05SC24
MC68HC05	MC68HC05	MC68HC05	MC68HC05
8 bits	8 bits	8 bits	8 bits
6K bytes	4K bytes	6K bytes	3K bytes
-	128 bytes	3K bytes	1K bytes
-	No	No	No
4 bytes	4 bytes	4 bytes	4 bytes
8K bytes (15V Vpp)	-	-	-
10K (70C; 5V)	10K (85C; 5V)	10K (70C; 5V)	10K (70C; 5V)
128 bytes	128 bytes	128 bytes	128 bytes
EPROM	16 bytes	16 bytes	16 bytes
5V	3-5V	5V	3-5V
5MHz (ext) 2.5MHz (int)	5MHz (ext) 2.5MHz (int)	5MHz (ext) 2.5MHz (int)	5MHz (ext) 2.5MHz (int)
4.5mA	TBD	5mA	5mA
Stop/wait 150uA	Yes	wait 450uA stop 30uA	wait 450uA stop 30uA
-	Watchdog system	-	-
3.5mm X 5.6mm	N/A	2.9mm X 5.1mm	3.4mm X 4.1mm
1 (additional 4 bit I/0)	1(additional 4 bit I/O)	1 (additional 4 bit I/0)	1 (additional 4 bit I/0)
Now	Q1 1994	Now	Now

Manufacturer	Motorola	Motorola	Motorola
Type Number	MC68HC05SC25	MC68HC05SC26	MC68HC05SC27
Microcontroller Core	MC68HC05	MC68HC05	MC68HC05
Architecture	8 bits	8 bits	8 bits
ROM	4K bytes	6K bytes	16K bytes
EEPROM	1K bytes	1K bytes	3K bytes
ECC	No	No	No
Page Write	4 bytes	4 bytes	4 bytes
EPROM	-	-	-
Write cycles endurance	10K (85C; 5V)	10K (85C; 5V)	10K (70C; 5V)
RAM	128 bytes	128 bytes	240 bytes
OTP memory	16 bytes	16 bytes	16 bytes
Voltage	3-5V	3-5V	3-5V
Max clock speed	5MHz (ext) 2.5MHz (int)	5MHz (ext) 2.5MHz (int)	5MHz (ext) 2.5MHz (int)
Max current	TBD	TBD	5mA
Sleep mode	Yes	Yes	wait 900uA stop 50uA
Special functions	Watchdog system	Watchdog System	Watchdog System
Die size	TBD	4.2mm X 2.83mm	4.2mm X 5.0mm
I/O ports	1(additional 4 bit I/O)	1(additional 4 bit I/O)	1 (additional 4 bit I/0)
Availability	Q1 1994	Q1 1994	Now

Motorola	OKI	OKI	OKI
MC68HC05SC28	MSM62705	MSM62780	MSM62725
MC68HC05	627XX	627XXX	627XX
8 bits	8 bits	8 bits	8 bits
12.5K bytes	2 K bytes	6 K bytes	8 K bytes
8K bytes	0.5 K bytes	8 K bytes	2 K bytes
No	Yes	Yes	Yes
4 bytes	none	32 bytes	16 bytes
-	-	-	-
10K (70C; 5V)	10K (70C; 5V)	10K (70C; 5V)	10K (70C; 5V)
246 bytes	64 bytes	192 bytes	192 bytes
16 bytes	N/A	N/A	N/A
3-5 V	5 V	5 V	5 V
5 MHz (ext) 2.5MHz (int)	5 MHz	5MHz	5 MHz
5 mA	10 mA	16 mA	10 mA
Wait N/A Stop N/A	No	No	No
Watchdog	-	-	-
TBD	-	6.03mm X 6.83mm	-
1 (Additional 4bit I/O)	1	1	1
Imminent	Now	No longer promoted	Now

Manufacturer	OKI	OKI	OKI
Type Number	MSM62785	MSM62786	MSM62715
Microcontroller Core	627XXX	627XXX	627XXX
Architecture	8 bits	8 bits	8 bits
ROM	8 K bytes	10 K bytes	6 K bytes
EEPROM	8K bytes	8K bytes	1K bytes
ECC	Yes	Yes	Yes
Page Write	32 bytes	32 bytes	8 bytes
EPROM	-	-	-
Write cycles endurance	10K (70C; 5V)	10K (70C; 5V)	10K (70C; 5V)
RAM	192 bytes	192 bytes	128 bytes
OTP memory	N/A	N/A	Yes
Voltage	5 V	5 V	5 V
Max clock speed	5MHz	5MHz	5MHz
Max current	16mA	16mA	10mA
Sleep mode	No	No	No
Special functions	-	-	-
Die size	4.91mm X 5.6mm	-	-
I/O ports	1	1	1
Availability	now	now	now

OKI	OKI	OKI	OKI
MSM 62745	MSM 627160	MSM 62880	MSM 62840
MSM 627XXX	nx -8/50	nx - 8/50	nx-8/50
8 bits	8 bits	8 bits	8 bits
8 K bytes	14 K bytes	12 K bytes	10 K bytes
4 Kbytes	16 K bytes	8 K bytes	4 K bytes
Yes	Yes	Yes	Yes
32 bytes	32 bytes	32 bytes	32 bytes
-	-	-	-
10K (70C; 5V)	10K (70C; 5 V)	10K (70C; 5V)	10K (70C; 5V)
192 bytes	448 bytes	384 bytes	320 bytes
Yes	Yes	1K bytes	1K bytes
5 V	5 V	3-5 V	3-5 V
5 MHz	5 MHz	5 MHz	5 MHz
10 mA	20 mA	10 mA	10mA
No	No	Yes (200 uA)	Yes (200 uA)
-	-	-	-
-	43.68mm^2	-	-
1	1	1	1
Now	On request	On request	On request

Changes in Manchester Project

Major changes have been made in the development and management of the automated fare collection system for the Greater Manchester area.

Originally the contract to deliver the AFC system was awarded to AES Scanpoint (UK) Ltd, a joint venture company formed in equal partnership between AES, a subsidiary of ERG Australia Ltd, and Scanpoint A/S, a subsidiary of NKT Ltd, of Denmark. At that time, Greater Manchester Passenger Transport Executive (GMPTE) were looking to a joint venture to help reduce the cost of the scheme in which they are investing £10 million, with NKT Ltd, Danish parent of Scanpoint A/S rumoured to be the favourite prospective partner.

Later it was proposed that ERG Electronics Ltd (ERGE), the fare collection subsidiary of ERG Australia Ltd, would form a 50/50 joint venture for the project.

That proposal has now been replaced following the formal signing of contracts between ERGE and GMPTE giving ERGE total responsibility for the design, supply, maintenance and management of the system.

The contract involves the supply of an AFC system for use in all public transport operating in the Greater Manchester region comprising buses, trams and trains in one of the first major city systems in the world involving contactless Smart Card technology. Initially, over 500,000 cards to be supplied by GEC Card Technology, will be issued to passengers for use in the system.

Fifty per cent stake

In addition to the design, supply and maintenance of the system, ERGE will have a 50% stake in the management company that is responsible for issuing and recharging of cards and overall management of the central clearing system. The management company will also manage the expansion of the card system to other public transport authorities and a broader range of users.

ERGE say that revenue handled through the management company is expected to be in the order of £60 million a year, growing substantially as other users are added to the system.

Contact: Peter Fogarty, Chairman, ERG Australia - Tel: +61 9 273 1100. Fax: +61 9 273 1208.

Smart XS-Card from Nedap

Nedap NV will be introducing their contactless Smart XS-Card at the Security ’93 exhibition from 4-8 October in Utrecht, The Netherlands.

The card, which is ISO standard size (thickness 0.76mm), is said to have a reliable reading distance of up to 70 cms. Applications include access control, public transport, parking, paying, automatic machines, and telephone. If required, the card can be delivered with a magnetic stripe.

Contact: J B Haleber, Nedap NV, Groenlo, The Netherlands - Tel: +31 5440 71111. Fax: +31 5440 64255.

TRANZ 460 from VeriFone

VeriFone, Inc., has announced the TRANZ 460 transaction system for credit and debit card authorisation and electronic data capture at the Point of Sale. The system can accommodate a variety of peripheral devices, including Smart Card readers, PIN, and bar code readers.

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

Gemplus US Appointment

Dan Cunningham, Vice President of Sales & Marketing at Gemplus Card International Corporation has been appointed President and Chief Executive Officer for its US operations.

Prior to joining Gemplus Mr. Cunningham was US sales manager for MicroCard Technologies Inc. the US Smart Card subsidiary of Group Bull.

Gemplus US was launched in the Washington DC area in 1989 and has sales offices in Gaithersburg, Maryland; and in Dallas, Texas.

Smart Card Diary

Advanced Card Association meeting, Department of Trade and Industry, London, 11 am 29 September. Contact: Simon Reed, Charta Associates - Tel: +44 (0)442 231844.

ICMA (International Card Manufacturers Association) Annual Convention and Trade Show, Cascais, Portugal, 12-15 October. Contact: ICMA, New Jersey, USA - Tel: +1 609 799 4900. Fax: +1 609 799 7032.

CarteS 93, Palais des Congres, Paris, France, 20-22 October. Contact: CarteS 93 - Tel: +33 1 49 68 51 00.

1993 Plastic Cards Conference, Karos Indaba Hotel, Johannesburg, South Africa, 8/9 November.

A chance to hear about Smart Card developments in South Africa. Contact: Ms Babette van Gessel, AIC Conferences - Tel: +27 11 803 9680.

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.

Maxcard Cashless Vending

Maxcard is an easy and convenient way to pay for drinks in a new cashless payment system from Maxpax International, a leader in drinks vending in the UK.

The scheme uses rechargeable cards and eliminates the need to carry cash or look for exact change for the machine.

Maxpax has ordered 150,000 2K bits memory cards from Gemplus for the Maxcard system which is already installed in large and small sites across the country.

A maximum value of £5 can be loaded on the card which can be pre-programmed to offer cardholders up to 14 free drinks per day with the following options - 1, 2, 3, 4, 5, 10 or 14. This allows the issue of free drinks to be controlled and budgeted. Drinks can also be subsidised by offering discounts of 10%, 25%, 50% or 75%

These are useful features where some users are required to pay for their drinks and others are given complimentary or discounted ones. The machines will also accept cash.

Snack and food vendors supplied by Maxpax can also be equipped with the Maxcard system, allowing staff to use the same card at all vending machines on site.

The system enables the operator to keep a check on costs through direct control over the number of free or discounted drinks given to staff, and as staff pay for their drinks up front by loading value onto their cards, this income can be used to pay for the next drinks order.

A daily and cumulative audit of drinks vended and cash collected may be accessed using an ancillary hand-held printer.The cards can be signed by the cardholder in waterproof ink so that they can be returned if lost.

Maxpax provides the first 25 Maxcards free with the system. After that they cost £4 each.In one of the trials at a major office complex, the senior catering manager commented that the cost of the cards could prove to be a problem and it would cost a lot for the company to buy a card for each of its 250 staff members, but, she added: "Judging by the enthusiastic response we have had to the card system so far, I suspect most would not mind paying £4 for the convenience - and of course the cards last for as long as you keep them."

Card details:

Type	Contact
Fabricator	Gemplus
Dimensions	ISO ID1
Contact location	Front
Chip type	Memory
Chip manufacturer	SGS-Thomson
Chip reference no.	24CO2
Memory type	EEPROM
Memory capacity	2K bits
Standards	ISO 7816-1/2

Contact: Richard Suthons, Maxpax International, England - Tel: +44 (0)295 264433.