

SMART CARD NEWS

September 1992
Volume Number 1 1



British Gas Leads With UK National Network

British Gas has started to put in place the biggest Smart Card network in the UK with 6,000 points where cards can be recharged. Agreement has been reached with Newsagents Federation Services Ltd (32,000 members) and Post Office Counters (20,000) and contracts are in the process of being finalised. With more outlets available than currently planned recharging points, it is expected that there will be keen competition to be selected.



This is the project to watch in the UK. British Gas is a leading player in the use of Information Technology and has one of the most advanced computer networks in Europe. Now that it is turning its attention to Smart Cards we can expect some exciting developments. Of course British Gas needs a network to service its own customers, but the strategic thinking is that they can capitalise on this infrastructure and make it available to other interested parties.

Continued on page 3



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 2 - How the IC Card is Made

Highlights from European Smart Card Applications & Technology (ESCAT) Conference in Finland.

CONTENTS

NEWS

| | |
|---|---|
| NatWest.Experiment | 4 |
| NIST Developing Smart Card | 4 |
| PFPF Look at Smart Cards | 5 |
| SWIFT to Increase EFT Security | 6 |
| Boost for Contactless Cards in UK Transport Schemes | 7 |
| Book Review | 8 |
| Keeping Up With Standards | 9 |

CASE STUDIES

| | |
|---|----|
| Bull Smart Card Technology at Expo '92 | 10 |
| BSkyB The Biggest UK Users of Smart Cards | 12 |

TECHNICAL BRIEFINGS

| | |
|--|----|
| Smart Card Tutorial - Part 1 Introduction to Smart Cards | 14 |
| SGS-Thomson ST16623 Integrated Circuit | 16 |
| Smart Card Diary | 18 |
| The Berlin Card | 18 |
| Trials on London Buses | 19 |

British Gas Leads

Continued from page 1

Among its own objectives are to cut bad debts by making it easier for people on low incomes to pay, and to reduce fraud by replacing coin and plastic token meters. Other organisations have similar concerns, for example, the electricity boards and, with the increasing use of water meters, the water authorities.

Project manager Peter Stoddart said that the scheme had created a great deal of interest. "We are talking with a number of organisations in different fields who are interested in using the network, but I cannot identify them at this stage." In this area, he said, there are several potential uses for Smart Cards, for example to pay community charges or replace systems like buying stamps at a Post Office and sticking them on a cards. The card could also be used to pay for stakes in the planned UK national lottery.

Called The Quantum System, the British Gas project being carried out in association with Landis & Gyr, consists of specially developed meters called Quantum meters, Smart Cards (GASCARDs), a network of easily accessible charging units linked by telephone line through 100 co-ordinating computers in British Gas offices with access to 12 regional mainframe computers.

The GASCARDs, supplied by Gemplus and being manufactured at their plant in France, cost "in excess of £5 each" reflecting, says British Gas, the storage on the card, high security and an expected lifetime of between 5 and 10 years.

An ISO standard reusable Smart Card with a 2k EEPROM chip, it carries the credit purchased at a charger unit to the meter. It also receives information from the meter such as the reading and hardware status which is transferred to the charger the next time it is used. This information is passed daily via the unit's integral modem to the local PC, and then on to the regional mainframe.

British Gas claims that the system is "extremely secure and fraud resistant." Each card, for example, is unique to the customer and their meter and cannot be used by anyone else.

The charger unit has two card slots, one for the operator's card to activate the unit and one for the

customer's card. Security features include an operator pass card which activates the unit, remotely programmable credit limits and transaction limits.

More sophisticated cards, the Servicecard and Datacard are used by engineers and customer accounting personnel for system configuration and monitoring purposes. The Datacard records information stored in the meter for system interrogation and fault finding, and is also used in the installation of charging units. Most powerful is the Servicecard which allows engineers to install, remove and exchange meters without loss of data. It is self-powered with an extended memory capacity and a live data and time function for system configuration.

The system has been on trial, initially in Newcastle-upon-Tyne and then in three other areas. Now the project is going nationwide to cover all 12 regions.

The five-year project - which has about four years left to run - involves 6,000 charging units, a million meters and over two million Smart Cards. Each household will have two cards, the charging outlets will have three special cards each for activating the charging units, and there will be 25,000 "super" cards for use by engineers when installing the meters.

British Gas have not yet given any figures for the total cost of the project, but it has been reported that the development contract awarded to Landis & Gyr for 100,000 meters and supporting infrastructure was in the region of £25 million, while British Gas had expenditure of its own in the development process. As they are planning for one million meters, total expenditure over a five-year period is likely to be in the region of £125 million. Even for British Gas this is a considerable investment, but they see this not only providing benefits for their customers, themselves, and others involved in the scheme, but as the key to the future development and dissemination of Smart Cards in the UK.

Benefits

Customer benefits are seen as providing a safe way of paying for gas and helping them to budget, and pay off any outstanding debts by deducting a percentage of the input value. A logic unit provides the customers with a liquid crystal display on the

meter showing the amount of credit available and also the state of the gas account. There is also an "overdraft" facility - at present a £3 limit - for use in an emergency, for example if the gas runs out late at night or over a week end. The card can be recharged easily in multiples of £1 at Post Offices and corner shops locally, or at gas showrooms. Also customers do not have to be "at home" to have their meters read and there is no cash in the meter to attract thieves.

Post Offices and corner shops offering card recharging services will receive a small percentage of sales and will benefit from an increase in customers who may buy other items in the shop.

British Gas sees the Quantum meter as a way of reducing some of the problems associated with mechanical meters and a replacement for the 600,000 coin and 200,000 plastic token meters currently in service. This will save the expense of having to visit homes to read meters and empty them of cash or tokens, and resetting them if prices change. It will substantially cut losses through fraud and burglary.

But substantial savings are expected in reducing bad debts by making it easy for customers to "pay as they go." Results from the trials show that the average amount pre-paid on the card by customers is £3, but this is usually done twice a week. If this trend continues when the project is completed with one million cards in use, British Gas will be collecting £6 million interest-earning money in advance a week.

Information from Peter Stoddart, British Gas, Gateshead. Tel: UK 091 491 4245. Tom White, Landis & Gyr. Tel: UK 0952 677661.

NatWest Experiment

National Westminster Bank has issued some 5,000 Smart Cards to staff at its London computer centre at Goodmans Fields, and those working locally, for use in making purchases at its two restaurants, shop and coffee lounges.

The experiment started with about 100 cards in March and has now been extended to all staff who can pay for meals, refreshments and confectionery by simply inserting their Smart Card in a reader at

the cash till which deducts the amount required from the card.

Issued free to staff, the card can be topped up with funds to a maximum of £50 at the bank branch at the computer centre. But more interestingly, NatWest has adapted in-house ATM's at which staff can recharge their cards.

Leon Stelmaszyk, Implementation Manager for the project, said the specially adapted ATMs were only available at the computer centre and not anywhere outside NatWest premises. Staff insert their normal NatWest Servicecard or Cashcard into the ATM and enter their PIN. Screen instructions tell them when to enter their Smart Card in a second slot. Instead of dispensing notes, the ATM electronically transfers money from the customer's bank account onto the microchip in the card.

Balance enquiry devices are located at key points so that staff can check the funds available on their cards at any time by inserting the card in a slot and reading the display screen..

The card being used is the Gemplus card with a SGS-Thomson chip and 2K EEPROM. NatWest have customised it by calling it the Byte card because of its association with computing and eating.

NIST Developing Smart Card

The National Institute for Standards and Technology (NIST) in the United States is reported to be developing a multiple application Smart Card for secure access control to computers, departments and buildings.

It will be interesting to see if it incorporates the DSS algorithm developed by NIST as an alternative algorithm for RSA. The DSS algorithm is designed for digital signatures and not for data encipherment. Some critics suspect this may be a less secure algorithm. There has been considerable debate in the USA between the proponents of the different algorithms where it is clear that considerable commercial issues are at stake.

PFPP look at Smart Cards

Britain's banks and card issuers, concerned at plastic card fraud losses running at £165 million a year, are looking at Smart Cards as a means of cardholder verification at the Point of Sale.

In a major market research survey to test consumer reaction this month, 2,000 people will be interviewed and have the opportunity to state their preference from a choice of three verification methods - PINs, signature verification or finger scanning.

The project is being organised by the Plastic Fraud Prevention Committee under the auspices of APACS (The Association of Payment Clearing Services). Technical Director Barry Fergus, of Barclaycard, said the use of Smart Cards per se was not the issue. The issue was how best they could get cardholder verification at the Point of Sale within which there was the choice of doing it on-line or off-line. "If you do it off-line the only viable way is by using Smart Cards."

At present the Committee is carrying out the technical evaluations of the three options and the cost evaluations. When this and the market research is completed they will decide which method they want to use and then whether this should be done on-line or off-line.

"That is the point when the Smart Card becomes a crucial issue," said Mr Fergus. "The debate is what is the best means of verification. Until that is sorted out we cannot really address the on-line/off-line argument."

The market research involving four or five sets of verification equipment which will be used in different parts of the country, will start and complete during September. Pins will be self-selected by users in the tests, and the Committee have been looking at the Bull system of finger scanning used at Expo '92 (see pages 10 and 11) as well as other finger scanning methods and a range of signature verification systems.

Check Book Access Control

Multiple application Smart Cards are being used to control and monitor physical access to a high security building on Standard Check Book's 16-

acre site at Midsomer Norton, near Bath, England.

The company is the UK's largest manufacturer of computer forms and listing paper and over 400 Smart Cards have been issued to staff involved in the printing of continuous cheques and sensitive direct mail.

The system has been designed and supplied by McCorquodale Smart Card Systems and, following a trial period, is likely to be extended to a further two factories within the complex.

Authorised staff insert their Smart Cards and enter their Personal Identification Numbers (PINs) at one of the card readers placed at key locations and access points to gain entry.

Information is relayed from the card readers to a central computer providing a visual display of the site, immediately indicating unauthorised attempts to access a secure area of the building. Audit trails compiled by the micro-processor within the Smart card detail the movement of personnel and the amount of time spent in particular areas.

McCorquodale have incorporated traditional security features in the overall system design, including alarmed fire exits linked to the central computer, while several fire exits have built in microphones to broadcast a message if the door is opened without permission. The card can also be used for other functions such as time and attendance.

Information from Trevor Crotch-Harvey, Managing Director, McCorquodale Smart Card Systems. Tel: (0272) 308684.

NTT orders 6 million cards

NTT Data Tsushin Co has placed an order for six million IC cards with four suppliers - Gemplus Card International of France, Hitachi Maxell, Spom Japan and Toshiba agent Kyokkou Denki Sangyo.

The cards, to be delivered by 1994, will be 8Kb and 0.5 Kb IC cards. NTT anticipates it will be able to offer the cards to customers at around 1,000 Yen (approx. £4) and 600 Yen (approx. £2.40) respectively.

SWIFT to increase EFT security

SWIFT, the Belgium-based Society for Worldwide Interbank Financial Telecommunications, is introducing Smart Cards for the authentication of EFT (Electronic Funds Transfer) messages. This security enhancement will be mandatory for the 3,500 plus financial institutions around the world who use the SWIFT network.

The system has been subjected to a security review by a group of international security experts and has been passed to go to pilot testing starting in mid 1993 with 10-15 users in the first phase and, after three months, some 50-100 users in the second phase. It will go live in the first quarter of 1994.

Called USE (Users Security Enhancement), the system is based on Bull CP8 EPROM technology utilising their 8Kbyte Smart Card with an improved MP mask and a SWIFT-specified algorithm.

A Smart Card reader has been combined with a hardware security module to create the Secure Card Reader (SCR) which is tamper-resistant and sends commands to the card and reads data from it.

When an authorised operator receives his card from a supervisor, he uses it with his Personal Identification Code to log on to the network automatically. It eliminates the need for operators to read or type codes to log in to the SWIFT network, and cards can be programmed to allow them to log in any number of times over a fixed period determined by the supervisor.

Administering the procedure is easier as the card is personalised to the operator and protected by his or her PIN. For additional security a dual PIN can implement dual control.

The basic package to operate USE comprises the Secure Card Reader, a Basic Card Reader (which continues to allow access to the network should the SCR fail), and three sets of three Smart Cards - one set for immediate use, one in case of problems for when the lifetime of the first set has expired, and one for test and training purposes. This total package is available to financial users at BF 160,000.

SWIFT is not divulging the cost of the scheme but

it will recover over £10 million from equipping member user banks and financial institutions.

Information from Luc de Clercq, Manager, SWIFT Users Security Enhancement Project. Tel: Belgium +32 2 655 3111.

GIS Application Development

General Information Systems (GIS), of Cambridge, England, has announced the availability of a complete applications development system with its Open Smart Card Access Routine (OSCAR) designed around the OKI MSM62785-018 Smart Card microcontroller.

The system, costing £399, includes a card reader that fits into the 5.25 inch disc drive slot on a PC, a serial interface card to the PC bus, and two OKI 8Kbyte (64 Kbit) Smart Cards.

Software includes a set of utility programs for user familiarisation and a library of card access routines for rapid applications development. Programming manuals and an introductory guide for applications developers are also provided.

Applications include the storage of confidential medical data, financial transactions, electronic purse systems, and access control.

GIS say they will provide applications development if required. Enquiries to Christopher Curry - Tel: (0223) 462200.

Dancoin Launches Danish Trial

Denmark has started its six-month Dancoin prepaid Smart Card trial in the town of Naestved (population 45,000), 70 kilometres south of Copenhagen, and plans to implement it country-wide starting on 1 March, 1993.

The card will be used for a variety of services, for example, in launderettes, banks, vending machines, payphones, parking meters and on the local bus system. Other services will be added as the trial progresses.

Dancoin is an independent company set up specifically by Danish banks, telephone companies and the transit sector.

Boost for Contactless Cards in UK Transport Schemes

Contactless Smart Cards have had a major boost in the UK with Greater Manchester Passenger Transport Executive (GMPTE) last month adopting them in a £10 million automatic fare collection system that they say will be the biggest in the world. Close behind them is London Transport Executive which will also specify contactless Smart Cards for bus travel in the UK capital when it goes out to tender this month for a major trial scheme (page 19).

Dr John Baker, Managing Director of GEC Card Technology, whose company will be supplying the cards in the Greater Manchester scheme, said: "We believe once contactless Smart Cards are seen operating in large numbers, there will be a strong move from contact Smart Cards towards the contactless alternative. This is the way to go."

He added that contactless cards with no surface contacts to wear out or become contaminated, were more convenient, and did not suffer from the effects of static.

The GEC card will be tailor made from its standard design to do what was required of it and Dr Baker envisaged an interchangeable family of cards.

Announcing its plans to introduce the electronic ticketing system on public transport throughout the county, GMPTE said it will eventually be used to pay for journeys on buses, trains and the new Metrolink.

AES Scanpoint (UK) Ltd has been awarded the contract to deliver a total Automatic Fare Collection (AFC) system. This is a new 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.

GEC Card Technology will supply the cards to AES Scanpoint (UK) Ltd, and Strategic Imaging Systems (SISYS), specialist security and public transport division of Nibbles Systems Ltd, of Poole, Dorset, whose equipment will personalise the cards, is a nominated sub-contractor.

SISYS equipment will handle the personalisation and issuing of the cards. Advanced techniques capture images of people from live video cameras and print directly on the surface of the card

The scheme will be piloted in the Bolton area among concessionary bus passengers ie pensioners, children, blind and mobility impaired people. Two major bus operators - Greater Manchester Buses and Ribble Motors - will have equipment fitted in about 300 of their buses, and in their depots, paid for by the Executive. The cards will be issued in the first instance by GMPTE through 25 of their offices, including travel shops. The cards can then be recharged at Post Offices and newsagents to any value that the customer wants. Using a simple card reader the shopkeeper enters the amount into the card. Each point of charging is modem linked off-line to the clearing house.

The pilot study will involve 5,000-10,000 Smart Cards. Four months will be spent in designing and producing the equipment, three months on on-the-road trials, with a further month spent completing the evaluation after which the scheme should be ready for county-wide implementation. This will involve equipping 2,700 buses plus some 350 regional rail and Metrolink locations, over 1,000 card sales/card reissue locations over the next 18 months.

It is expected that over one million cards will be issued. The card base will be managed through a central clearing house and will be expanded into other applications outside automatic fare collection.

GMPTE says that each card will cost £3.95 with a card lifetime guaranteed for 10,000 transactions, while GEC say it will last for over five years.

Who will pay for the card is still under consideration, and will be a political decision. One of the options is that those who qualify for concessionary travel already pay £2 for a pass with their photograph on it and it may be decided to keep the charge the same.

Greater Manchester's present ticketing system was due for renewal and this was one of the spurs which has led to introducing Smart Cards. Cost benefits are seen as channelling money into a state of the art

technology scheme which would have been spent anyway in replacing an obsolete ticketing system due for renewal, and reducing ticket fraud, for example, young adults travelling as children.

One obvious cost benefit is that by using Smart Cards, journeys will be pre-paid by customers and this money will attract interest. In addition, once the system is operational it can be expanded to other applications outside public transport, for example, making calls from public telephones, paying for petrol at garages and for goods in shops. The Executive is already involved in discussions with other potential outlets. Part of the deal is that shops involved in recharging the cards will benefit from the customer being able to purchase goods in their shops using the same card.

This leads on to intriguing behind the scenes activity by the GMPTE who are negotiating a joint venture which will help to defray costs and perhaps even make a profit. This is another "political decision" but NKT Ltd, Danish parent of Scanpoint A/S is rumoured to be a favourite prospective joint venture partner.

Information contacts:

Mike Hill, Greater Manchester Passenger Transport Executive. Tel: UK 061 228 6400. Fax: 061 228 3291.

Dr John Baker, Managing Director, GEC Card Technology Ltd. Tel: UK 021 555 6280. Fax: 0922 25458.

Peter Fogarty, Chairman, AES Ltd. Tel: Australia 61 9 389 1500.

Morten Solling, Managing Director, Scanpoint A/S. Tel: Denmark 45 43 43 3999.

Tony Douglas, Managing Director, Nibbles Systems Ltd (for Strategic Imaging Systems). Tel: UK 0202 723277. Fax: 02-02 735398.

Book Review

The Case for Smart Cards, written by The Software Partnership, published by Eurostudy Publishing Co Ltd. ISSN 1-85271-223-6. 101 pages, priced £99/US\$198.

This book is intended as an introduction to the technology and application of Smart Cards and as such is lightweight technically. However, for readers new to the subject, it gives a useful overview of the available card technology and explains why Smart Cards can in many circumstances provide a more powerful and cost-effective alternative to current plastic cards.

To explain the differences between Smart Cards and alternative card technologies there is a section on magnetic and enhanced magnetic cards, optical memory cards and the Maxcard.

Section six details current and potential Smart Card applications grouped under physically closed environments, logically closed environments, finance and security, and general.

Examples of physically "closed" areas include leisure and holiday centres or hotels, while logically closed areas include health care and vehicle monitoring. In the finance and security area examples involve Electronic Funds Transfer (EFT) at points of sale, electronic banking, access control, home shopping and supermarket loyalty schemes. General applications include pay television, cellphones, civic schemes and toll and parking payments.

Here the author(s) look at the applications, for example, a holiday centre, and the typical facilities that could be made available on the Smart Card, how the card would work, and resources required before arguing the case for using Smart Cards and giving examples of current pilot schemes, existing projects or potential applications.

Another section looks at some Smart card projects in Europe, the USA and Japan. The book concludes with the view that the future of Smart cards in Europe is likely to lie in payment cards. Card issuers were starting to view Smart cards as a way of tackling fraud problems and it was likely that one or more issuers would soon conduct a relatively "open" trial of Smart cards as payment cards.

In addition to performing as more secure debit and card cards, Smart Cards were likely to emerge as prepayment cards for a range of products and services, and as retail loyalty cards.

Keeping up with Standards

There are a number of organisations working on standards for the IC Card through sub-committees and working groups and increasing activity, particularly in Europe where the number of topics under consideration continues to grow.

The principal IC Card standards bodies are:

| | |
|------|--|
| ISO | -International Organisation for Standardisation |
| IEC | -International Electronic Commission |
| CEN | -Comite Europeen de Normalisation |
| ETSI | -European Telecommunications Standards Institute |

This first article in a series aimed at helping people to understand what is going on and who is doing what, looks at the work of the International Organisation for Standardisation (ISO), which is a worldwide federation of international standards bodies.

The work on IC card standards in ISO is split into two areas. One is the inter-industry environment under Joint Technical Committee 1's Sub-Committee 17, known as JTC1/SC17, and its working groups (WGs). The other deals with the financial sector through Technical Committee 68's Sub-Committee 6, known as TC68/SC6, and its working groups.

JTC1/SC17 has two Working Groups of particular interest - WG4 dealing with contact cards, and WG8 with contactless cards as follows:

JTC1/SC17/WG4 - Contact Cards

ISO 7816

- 1 Physical characteristics
- 2 Dimensions and location of the contacts
- 3 Electronic signals and transmission protocols
- 4 Inter-industry commands for interchange
- 5 Number system and onticketing procedure for application identifiers
- 6 Inter-industry data elements for interchange

JTC1/SC17/WG8 - Contactless Cards

ISO 10536

- 1 Physical characteristics
- 2 Interface arrangements

Financial Sector

TC68/SC6 has three Working Groups developing standards for the financial sector -Working Groups 1, 5 and 7 as follows:

TC68/SC6/WG1 ISO 8583 Financial transaction card originated messages- interchange message specifications

TC68/SC6/WG5 - Messages and data content

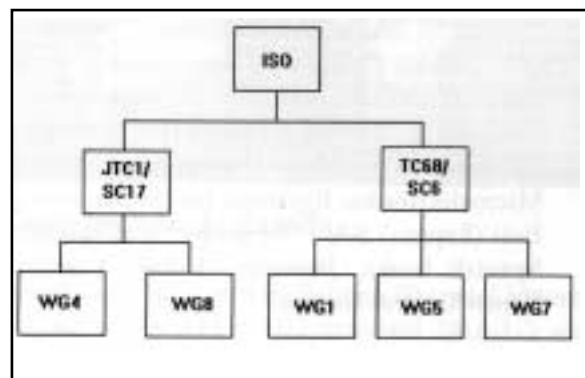
ISO 9992

- 1 Concepts and structures
- 2 Functions
- 3 Messages (commands and responses)
- 4 Common data for interchange
- 5 Organisation of data elements

TC68/SC6/WG7 - Security

ISO 10202

- 1 Card life cycle
- 2 Transaction process
- 3 Cryptographic key relationships
- 4 Secure application module
- 5 Use of algorithms
- 6 Cardholders verification
- 7 Key management



Case Study - Bull Smart Card Technology at Expo '92



The organisers of Expo '92 in Seville, Spain, chose an advanced technology solution to control access for thousands of season ticket holders and staff. The scheme cost £6 million pounds and involved the world's first major public application of a biometric Smart Card solution to access control. But how did it work in practice? What were the benefits to the parties involved? How did the public react to a system which involved fingerprint recognition? Expo '92 closes its door next month after a six month run, and Smart Card News looks at the results to date.

The recognition system was supplied by the Temporary Union of Companies (UTE), created for that purpose by the State National Mint (FNMT) and Bull (Espana) SA. The National Mint has the sole right to manufacture Bull CP8 cards in Spain. The fingerprint reader terminals were developed by Telesincro SA, a Bull subsidiary. Specifications and design of the application were the responsibility of Excel Data SA formed by Fabrico Nacional de Moneda y Timbre (the National Mint), Telefonica Sistemas (telephones subsidiary), Microelectronica Espanola (microelectronics) and Bull (Espana) SA. The project was sponsored by Spanish banks, Banestro, Bilbao Vizcaya, and Banco Central Espano.

Enrolment

Two visually different cards were involved - one for season tickets and the other for Expo personnel. Those requiring season tickets went to a branch of one of the sponsoring banks where they filled in a

simple application form and paid for the ticket. A few days later they were given an appointment to attend a central enrolment office, taking with them proof of their identity.

At the office, their card was personalised with each individual's unique biometric data, in this case a fingerprint. Enrolment involved placing a finger, normally the first finger on the right hand, on a small aperture where a camera captured its image. This was digitised and stored inside the secure EEPROM memory. Registration took about three minutes to take three fingerprint readings. The second and third readings were taken at slightly different angles to allow for mismatches on presentation. The fingerprint system came from Identix in the United States, a partner with Telesincro SA. It took up 1.2Kbits, about half of the EEPROM.

A trouble-shooting desk was manned by Bull personnel and provided a neat solution to familiarising ticket holders with the use of the card and ensuring that it worked correctly. To leave the enrolment centre, users had to pass through a turnstile using their new card. They simply entered the card in the reader and placed their finger on the finger scanning device. This process took less than a second and on verification the gate was opened. Failure rates at this stage were less than one per cent and were quickly rectified.

It was sometimes necessary to use another finger if the other was bandaged, the print rubbed smooth through working with chemicals or through mountaineering. Problems encountered included people who forgot which finger they should use, and an elderly gentleman whose hand shook when the template was being prepared.

The system on site

Entry to Expo '92 was through 12 main entrances with 120 turnstiles operating on a tidal flow basis which automatically provided more entrance turnstiles in the morning and more exits in the evening.

There were between 50 and 60 Bull TCA 200 access terminals (Smart Card and Fingerprint readers) at the entrances linked through an RS485 network to PC based concentrators connected to two Bull DPX/2 360 systems. Communications systems were duplicated and the DPX systems

could run back to back providing high resilience to failure.

The DPX systems acted as servers to the concentrators and provided on-line updating of a blacklist of lost or barred cards. They also polled the concentrators to collect information on how many visitors were attending and how frequently. The system was based on the Bull CP8 card with a Motorola chip 6805 (CMOS technology) called the Mask Scot 100. 128 bites of RAM, 4Kb of ROM and 3K EEPROM.

Statistics

Over 450,000 cards had been issued by August - 250,000 day and 100,000 night season tickets, 55,000 to Expo staff, and 50,000 to VIPs as identity and access cards.

Bull said that the failure rate was less than one in 1,000 with the false rejection rate set higher for a point of entry system than it would have been for a point-of-sale outlet. The main reason for failures was the problem of reading the fingerprint. For people between the ages of 15 and 65, the system worked very well, but with young children, particularly in the 5-7 age group, their fingers were too small to get the fingerprint correctly on the card so they had difficulties when they arrived at the turnstyle. With older people, for example with arthritis, they had difficulty in keeping their finger still. However the parameters for the application could be moved to allow for people with problems.

Besides the problem of people having physical problems with the fingerprint, another problem was to obtain a correct fingerprint the first time for such a large number of people.

As a back-up, a guard at each gate had a hand-held reader to read personal details of the user if there was a problem about entry. In addition there was a re-enrolment area near the gate.

Benefits

Customer benefits were seen as having a card, which if lost or stolen had a nil street value as it could not be used by anyone else. Indeed some 500 cards went missing but the organisers were getting a few returned every day.

Organisers could be sure that the person using the

card was the rightful owner and could gather statistics on use. For example, season tickets holders were using each card on average 16-17 times.

In addition, because Expo '92 was attracting visitors from all over the world and the theme was "Discovery", the organisers wanted to present a state of the art project.

The greatest benefits for those involved were probably in the worldwide publicity achieved by showing the first large-scale public use of the new technology of biometric verification combined with a Smart Card in the high profile showcase of Expo '92.

One of the biggest doubts hanging over the project was how the public would react to the use of fingerprint scanning - often labelled as an invasion of privacy and said to be unpopular because of the connotation with crime. This doubt was quickly dispelled as the users were satisfied that their fingerprint was held only in the card and not stored elsewhere.



Card technical details

Smart Card fabricated by Fabrica Nacional Moneda y Timbre (FNMT) to ISO Standard 7816-1-2 with Motorola chip 6805 CMOS memory plus logic/CPU. Non-volatile memory EEPROM. Memory capacity Mask ROM 4Kb, EEPROM 3Kb, Ram 128 bites. Communication protocol TO. Security - PIN (2 bytes) and Bull Telepass proprietary crypto algorithm.

Case Study - BSkyB The Biggest UK Users of Smart Cards

BSkyB dominates the market in the UK as the biggest users of Smart Cards with over one million in current use and a potential market of 20 million. They are a vital tool in the management and control of pay-TV programmes and services and the vehicle for:

- * Collecting revenue
- * Restricting programmes to designated countries or regions, and
- * Preventing fraud.

Because of its use by BSkyB, the VideoCrypt system has established itself as the de facto standard for encryption of television signals in the UK and assured its dominance in the market.

The importance of VideoCrypt and Continental Europe competitors such as Eurocrypt and Nagravision, is that they have foiled the pirates who have been unable to break the encryption system to date, thus safeguarding the revenue from the customer base and from advertising - which is directly proportional to the viewing figures. Importantly too, it has kept programmers happy by protecting copyright.

The VideoCrypt system adopted by BSkyB was the result of a joint venture between NewsDatacom and Thomson Consumer Electronics using the French Gemplus Smart Card.

A highly sophisticated and virtually hacker-proof system, it is the largest application of Smart Card Technology in the UK, yet for the paying customer it is a simple matter of inserting his or her card in a decoder to unscramble the picture for viewing.

Behind this user-friendly operation lies a complex system for secure end-to-end broadcasting. It is made up of a number of components:

The Subscriber Management System is a comprehensive database and management system supporting customer service and billing, for example it holds customer records and their subscriptions. It is here that data for the production of viewing entitlements is prepared and routed to the Authorisation Centre.

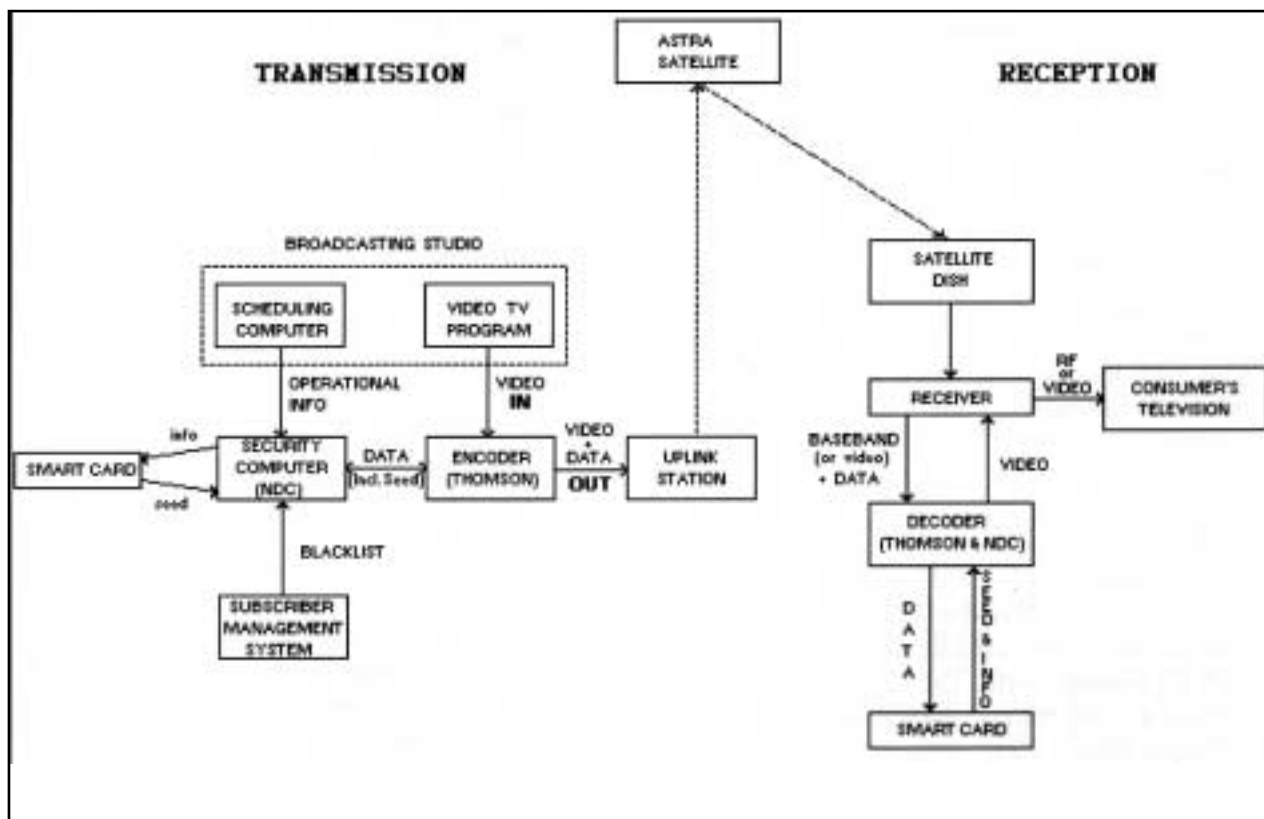
The Authorisation Centre organises the signal for transmission using its own Smart Cards to provide scrambling instructions to the encoder. The Centre can automatically determine different access conditions for different programs, for example, it can restrict viewing to a specific country, countries, or region according to programme scheduling requirements. It also collects and processes over-the-air addressing data. This data is sent over the air in lines of the video vertical blanking interval. It includes the descrambling seed and synchronisation pseudo-random number generator (PRNS).

VideoCrypt uses a video line rotation method for scrambling the signal to prevent unauthorised viewing. The Encoder scrambles the video signals by digitising the video for cut and rotate scrambling and converts it back to analogue form for transmission having inserted over-the-air addressing data into the vertical blanking interval. Transmission can be by any signal medium - satellite, cable, terrestrial, MMDS, and signal type PAL, SECAM, NTSC, MAC, and D-MAC. This signal is digitised to 10-bit accuracy, for high broadcast quality.

Line cut and rotate scrambling destroys the structure of the picture which cannot be re-assembled without knowledge of the encryption algorithm. Successive video lines are cut randomly and transposed ie swapped over. These cut points are generated by a PRNS. In order to know the sequence it is necessary to know the seed number used to generate the cuts. To prevent this being discovered the VideoCrypt system generates a new "seed" every few seconds.

The audio signal is intentionally left "clear." Although it is possible to scramble the audio signal this can be expensive and the argument is that there is little value in watching an undecipherable picture on the television screen even if you can hear the sound track.

As far as the viewer is concerned the key components are the Decoder and the Smart Card. The Decoder unscrambles the signal for viewing according to entitlement information received from the Smart Card which also processes any over-the-air data directed to it, for example, updating or stopping entitlements.



Sky Television VideoCrypt System

Decoders used 8-bit digitisation and sample the signals at a rate of 14 MHz.

The microprocessor chip in the card is physically secured utilising techniques such as “buried Bus” architecture while a special high security mask was developed for the card operating system.

The Smart Card is the key security device because it contains all of the system’s security algorithms, retrieves the descrambling seed number for the decoder and decrypts the data.

As a further refinement the microprocessor in the Smart Card employs Public Key cryptography in the form of the Fiat-Shamir zero-knowledge identification test which forces the decoder at regular intervals to test that the card is authentic. It is mathematically impossible for a forged card to pass this test.

Cards are changed periodically, and, if necessary, the Smart Card security algorithms can be changed making hacking attacks difficult and clearly not

viable. BSkyB does not commit itself to a public timetable for sending out new cards, but recently completed a reissue.

In some earlier systems, the user’s decoding key was in the Decoder. When pirates cracked the code, as they did with alarming success, the security of the system was compromised. Security could only be restored by replacing each subscriber’s Decoder - an expensive and time-consuming operation.

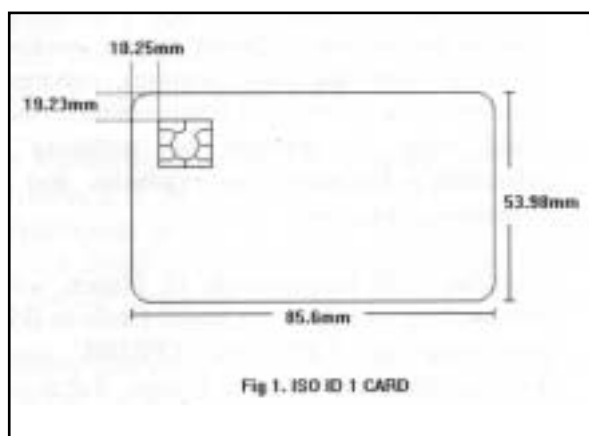
Gemplus Card International, of France, was the first supplier of subscriber Smart Cards to BSkyB, fabricating its COS 8K EPROM card to VideoCrypt specification in France. Subsequently News Gem Ltd, formed by Gemplus and NewsDatacom, opened a production plant at Livingston, Scotland, with plans to manufacture one million cards a month. Unfortunately this venture ended in disagreements and the factory was closed. The current Smart Card issued by BSkyB is fabricated in the United States and uses a Motorola chip.

Smart Card Tutorial - Part 1

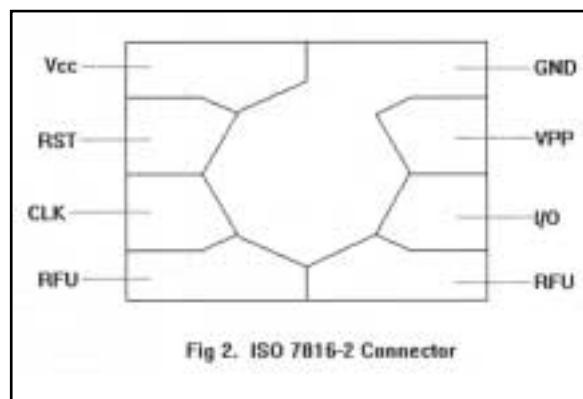
Introduction To Smart Cards

Even the name Smart Card captures the imagination, however such a term is ambiguous and is used in many different ways. ISO uses the term, Integrated Circuit Card (ICC) to encompass all those devices where an integrated circuit is contained within an ISO ID1 identification card piece of plastic. The card is 85.6mm x 53.98mm x 0.76mm and is the same as the ubiquitous bank card with its magnetic stripe that is used as the payment instrument for numerous financial schemes.

Integrated Circuit Cards come in two forms, contact and contactless. The former is easy to identify because of its gold connector plate (fig 1). Although the ISO Standard (7816-2) defined eight contacts, only 6 are actually used to communicate with the outside world. The Contactless card may contain its own battery, particularly in the case of a "Super Smart Card" which has an integrated keyboard and LCD display. In general however the operating power is supplied to the contactless card electronics by an inductive loop using low frequency electronic magnetic radiation. The communications signal may be transmitted in a similar way or can use capacitive coupling or even an optical connection.



The Contact Card is the most commonly seen ICC to date largely because of its use in France and now other parts of Europe as a telephone prepayment card. Most contact cards contain a simple integrated circuit although various experiments have taken place using two chips.



The chip itself varies considerably between different manufacturers and for a whole gambit of applications. Let us consider first the purpose for the 6 contacts used by the ICC (fig 2)

Vcc is the supply voltage that drives the chips and is generally 5 volts. It should be noted however that in the future we are likely to see a move towards 3 volts taking advantage of advanced semiconductor technology and allowing much lower current levels to be consumed by the integrated circuit. Vss is the substrate or ground reference voltage against which the Vcc potential is measured. Reset is the signal line that is used to initiate the state of the integrated circuit after power on. This is in itself an integral and complex process that we shall describe later in more detail.

The clock signal is used to drive the logic of the IC and is also used as the reference for the serial communications link. There are two commonly used clock speeds, 3.5795 MHz and 4.9152 MHz. The lower speed is most commonly used to date in Europe but this may change in the future. One may be tempted to ask why these strange frequencies were chosen, why not just a straight 5 MHz. The reason lies in the availability of cheap crystals used in the television world. For example the American NTSC colour subcarrier frequency is exactly 3.579545 MHz. The Vpp connector is used for the high voltage signal that is necessary to program the EPROM memory. Last, but by no means least is the serial input/output (SIO) connector. This is the signal line by which the chip receives commands and interchanges data with the outside world. This is also a fairly complex operation and will be the subject of a more detailed discussion where symbols such as T0 and T1 will be fully explained.

So what does the chip contain, well the primary use

of the IC card is for the portable storage and retrieval of data. Hence the fundamental component of the IC is a memory module. The following list represents the more commonly used memory types,

| | |
|--------|-------------------------------|
| ROM | Read only memory (mask ROM) |
| PROM | Programmable read only memory |
| EPROM | Erasable programmable ROM |
| EEPROM | Electrically erasable PROM |
| RAM | Random access memory |

A particular chip may have one or more of these memory types. These memory types have particular characteristics that control their method of use. The ROM type of memory is fixed and can not be changed once manufactured by the semiconductor company. This is a low cost memory, in that, it occupies minimum space on the silicon substrate. The use of the silicon is often referred to as real estate because clearly one wants to get as much as possible into the smallest possible space. The snag however is that it cannot be changed and takes several months to be produced by the semiconductor company. There is also effectively a minimum order quantity in order to achieve this low cost.

In order of increasing real estate the PROM comes next. This memory is programmable by the user through the use of fusible links. However high voltage and currents are required for the programming cycle and such devices are not normally used in Integrated Circuit Cards. The EPROM has been widely used in the past but the name for this application is something of a misnomer. Whilst the memory is erasable, by means of ultra violet light, the necessary quartz window is never available in the ICC and the memory is really used in one time programmable mode (OTP). Getting pretty heavy in real estate terms is the EEPROM. This memory is indeed erasable by the user and can be rewritten many times (between 10,000 and 1,000,000 in a typical implementation) All of these memories described so far are non volatile. In other words when the power is removed they still retain their contents. The random access memory (RAM) is a different kettle of fish, this is volatile memory and as soon as the power is removed the data content is lost.

In order to pursue our studies further we must note that the cost of the IC at saturation (i.e when development costs have been recouped) is

proportional to the square area of silicon used (assuming constant yield). The ISO connector is so designed to constrain the silicon die size to about 25mm² (although it is possible to handle 35mm² or more). However the important point is more concerned with reliability where clearly the larger die will be more prone to mechanical fracture. There is another bi-product that we will consider later where the cost of testing and personalisation are considerably altered by the complexity of the particular chip. It is clear however that we should attempt to minimise the contents of the chip on both cost and reliability grounds commensurate with the particular application.

Well of course you cannot have something for nothing and although a telephone card may operate with a little EEPROM memory (128 - 512 bytes) and the memory control logic, more sophisticated applications will demand ROM, EEPROM, RAM and a CPU (Central Processing Unit) to achieve the necessary business. It is the addition of the CPU or micro-controller that really leads to the term "Smart" although we will not be rigorous in our use of the term.

The control logic should not be overlooked as this is necessary not only for communication protocols but also to offer some protection of the memory against fraudulent use. The ICC is probably the security man's dream because unlike most electronic storage and processing devices it has security intrinsically built in. The ICC really does provide a tamper resistant domain that is difficult to match with the somewhat larger security boxes that handle cryptographic processes.

So now we can differentiate the different types of ICC by their content,

- Memory only
- Memory with security logic
- Memory with CPU

The security logic can be used to control access to the memory for authorised use only. This is usually accomplished by some form of access code which may be quite large (64 bits or more). Clearly the use of EEPROM memory must be strictly controlled where fraudsters can obtain a financial advantage by unauthorised use. This applies as much to telephone cards as applications using ICCs for cryptographic key carriers.

The security advantage of the CPU device is of course more significant because the CPU is capable of implementing cryptographic algorithms in its own right, but we will discuss this in more detail in due course.

In the Smart Card world the term application is widely used to describe the software or programs that the IC implements. In the simplest case the application may be just a file manager for organising the storage and retrieval of data. Such an application may be totally implemented in the logic of the chip. Similarly the chip must contain the communications logic by which it accepts commands from the card acceptance device (CAD) and through which it receives and transmits the application data. The ICC which contains a CPU can handle more sophisticated applications and even multi applications since the CPU is also capable of processing the data and taking decisions upon the various actions that may be invoked. The subject of multi-applications and particularly the implementation of security segregation is another subject for more detailed discussion in subsequent parts.

Next month: Part 2 - How the ICC is made.

Technical Review: SGS-Thomson ST16623 Integrated Circuit

SGS-Thomson have produced a range of chips (ST16 xyz) for Smart Card use of which the ST16623 is the newest in the series. This family is used by Gemplus as the basis of the COS and MCOS devices.

Security is the name of the game with the ST16 family through the implementation of a number of detection features designed to thwart the counterfeit artist.

The ST16623 block diagram is shown in Figure 1. It is based on an 8 bit CPU with a 16 bit address bus. It has on-chip memories with the following capacities,

| | |
|--------|-----------|
| ROM | 6K byte |
| EEPROM | 3K bytes |
| RAM | 224 bytes |

The CPU is able to address 64K bytes of memory of which 9K bytes are implemented with the

ST16623. The microcontroller has a special security logic block which is used to achieve a high level of security against both software and hardware fraud. The ST16623 interfaces with the outside world using five of the standard ISO connections, Vcc, Vss, Clock, Reset and I/O. The high voltage for driving the EEPROM write cycle is implemented by means of an internal charge pump. The device also incorporates its own internal dual register (2 X 8 bytes) random number generator. The chip also incorporates a low power standby mode which is becoming an important feature of the ETSI standards as a means of reducing battery consumption in portable telecommunications equipment.

Memory access control

An attractive feature of the ST16623 is the memory access matrix which can be set by the user in the mask ROM. This matrix controls the memory types that can be accessed from programs operating in the same or other memory classes as shown in the table,

| Data Accessed Program Location | RAM | ROM | EEPROM |
|-----------------------------------|-----|-----|--------|
| RAM | C | C | C |
| ROM | X | X | X |
| EEPROM | C | C | C |

X =Access Authorised; C=Access Defined By User

This means that programs operating in the EEPROM can be denied access to data stored in both the ROM and EEPROM. This is an effective way of achieving security segregation necessary for multi-application environments.

Hardware security features

The memory circuits include two features designed to thwart dynamic and static reverse engineering. The address bus of the memory cells are scrambled for both the ROM and EEPROM busses. In addition dummy cells have been included to prohibit analysis of the IC current drain under dynamic operation.

However it is the physical security control logic which is of particular interest. The IC contains a security register (accessible by the programmer) that gives the status of a number of analogue/digital

attack sensors,

- Vcc low voltage detection
- Low Clock frequency detection
- Test fuse status sensor
- Light exposure and passivation sensor
- High temperature detector
- Standby mode status sensor

The Clock frequency sensor inhibits the attacker from attempting dynamic analysis at low speed. The light and passivation layer sensors make it difficult to reverse engineer the chip by removing the encapsulation and passivation layers which is necessary in order to place electronic probes on the address and data busses. The high temperature detector is debatable since one of the likely attacks might be an attempt to freeze the RAM memory status prior to probing. Ideally the sensor should detect temperature gradients rather than an absolute temperature threshold.

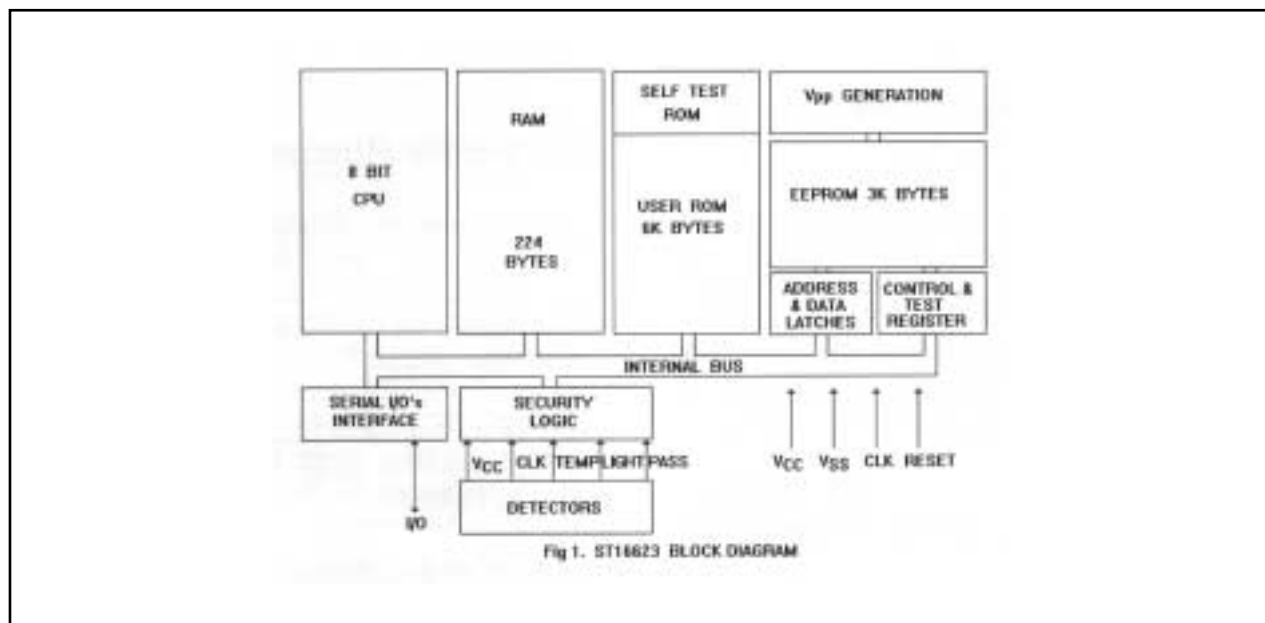
Software features

The ST16623 CPU has five registers,

- Accumulator (8 bits)
- Index register (8 bits)
- Program counter (16 bits)
- Stack pointer (6 bits)
- Condition code register (5 bits)

Perhaps the most unusual feature of the CPU architecture is the stack which operates in the middle of the RAM address space. The stack is also limited to 63 bytes. As with most microcontrollers the register flexibility is limited. The index register can, however, be used as an additional accumulator. There are 63 basic instructions with up to 10 addressing modes. Bit manipulation is covered by the instruction set which also includes an 8 X 8 bit unsigned multiplication to give a 16 bit product. An 8 bit multiply takes 10 clock cycles.

The ST16623 is clearly optimised for Smart Card applications and is limited to a maximum clock speed of 4 MHz which is consistent with the widely used ISO clock of 3.58 MHz. It should be noted however that the chip would be out of range of the 4.92 MHz clock which is becoming more widely used, particularly in Japan. The real strength of this chip lies in the integral security features which appear not to be addressed in the same depth by other Smart Card IC manufacturers.



Smart Card Diary

Danmont - and the Future IC-Card Applications, Copenhagen, Denmark, 17/18 September.

Danmont presents its technical solutions, strategy and development while several speakers deal with aspects of IC-Card technology, European standardisation and future applications. On day two delegates visit Naestved which is being used as the test town for the Dancoin prepaid card system before being implemented throughout Denmark. Contact: Lotte Carl Tel: (+45) 43 44 99 99. Fax: (+45) 43 90 30.

Cartes '92, Palais des Congres, Paris, 22-24 September.

The 7th. International Plastic Card Forum Conference and Exhibition. Contact: Cartes 92 2 bis, avenue Desfeux 92100 Boulogne, France.

European Payments 92 (EFTPoS & Home Services), Sheraton Hotel, Edinburgh, Scotland, 17-19 November.

This eighth annual conference and exhibition organised by the Scottish Electronics Technology Group offers an Introductory Tutorial to Smart Cards on the afternoon of 16 November chaired by Bob Carter, Senior Consultant, Orchard International. Enquiries to Paula Biagioni, Tel: +(0)41-553 1930, Fax: +(0)41-552 0511.

Managing European Plastic Cards, Hotel Melia, Madrid, Spain, 19/20 November.

Covering the card industry with sessions on smart cards including the topic "Has the issuance of Smart Cards deterred the level of fraud in France?" from Christine Woillez, Directeur de l'Exploitation Interbancaires, Groupement des Cartes Bancaires (France). Programme from IIR, UK Tel: +44 71 412 0141, Fax: +44 71 412 0145.

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

Six conference streams covering communications, market overview and marketing systems, finance and security, medical, technology and innovations,

and transport and travel. In addition there will be a half-day seminar on 15 February providing a practical introduction to Smart Cards for new and potential users. A second hall has now been opened for exhibitors. Contact Conference Secretariat Tel: +44(0)733 394304.

The Berlin Card

Passengers on buses and trains in the Metropolitan area of Berlin will soon be able to pay for journeys using a multifunctional Smart Card.

A trial starts soon on the buses and trains of the Berlin Public Transport Company (BVG) who will run the system and distribute the cards which will contain a reloadable cash account with a value up to DM 999.00 (approximately £360).

Siemens-Nixdorf, who are implementing the project, said that the organisational and technical concept enable its expansion to an unlimited number of service providers of the payment system, for example, taxis, shopping centres, museums, and department stores etc.

Among the initial conditions necessary to the setting up of the system, are an accounting and clearing system for the Smart card payments.

The Smart Card will carry a high level of security through its cryptographic procedure for crediting and optional debiting.

Award for Buscom

Finnish company, Buscom, has been awarded a prize for the most innovative Smart Card accomplishment of the year 1991 for its "Leadership in non-contact Smart Card fare collection systems."

The award was for its transit fare collection project using contactless cards in the first system of its kind in Finland.

Buscom Smart Cards and card readers are currently being used in a trial by London Transport (see page 19).

Trials on London Buses

Continued from page 19



Smart Cards rather than pay cash. The reasoning is that people who use buses infrequently do not purchase, for example, a weekly ticket because they are not making enough journeys to justify the cost, but with the Smart Card they can use it whenever they like as long as there is still value on the card. People will not lose because of holidays. It is also a secure form of cash as if the card is reported missing the customer can be refunded for the value held on the card less an administration charge. The card is disabled if stolen. It is also more convenient to use as the card can remain in a wallet or handbag and still be read.

For LT there will be better checks on validity and valuable information on the number of passengers carried and travel patterns. Extensive use of Smart Cards could speed up journeys, and if it is feasible to provide the required level of service with fewer buses there are substantial savings to be gained.

Other perceived benefits are that the cards will lower the amounts of cash being carried on buses and, hopefully, assaults on drivers. A reduction in fraud is expected as it will be extremely difficult to pass an expired ticket when the card reader will alert the driver.

But the real bonus which LT hope to achieve is to persuade more people to travel by bus. 70-80 per cent of passengers use passes, including those who qualify for concessionary passes - senior citizens travel free - but numbers have been falling in recent years. Latest available figures show 1,149 billion journeys in 1991/92 and LT are targeting the 20-30 per cent who pay cash. There is a vast amount of money being paid in cash and a substantial proportion of this could be collected by pre-

payment and earn interest. The cards are expected to cost between £3 and £5 and travellers will have to buy them, but LT are considering incentives for regular travellers and discounts to attract people to use the card.

The card will be available at travel inquiry shops and pass agents who will not have to carry a high value of stock as there is no value on the card until it is issued.

As LT is specifying contactless cards, those tendering are likely to be companies like ADE, AT&T, Buscom, GEC and NEDAP.

Buscom Proximity Card Specifications

| | |
|--------------------------|--|
| Construction | EEPROM chip and coil, moulded in plastic resin |
| Dimensions | 86 x 54 x 1.6 mm |
| Mould material | PVC |
| Signal | RF |
| Interface | Inductive |
| Access speed | Special duplex coms up to 10,000 baud |
| Number of rewritings | over 10,000 times |
| Environmental conditions | Operating temperature -40 to +50 degrees C |
| Safety | Password Specific coding Safety counters |

Information from London Transport Stored Value Ticketing Project. Tel: +44 (0) 71 -918- 4123.

