Denmark to Launch First Country-wide Scheme

Denmark will be the first country in the world to adopt Smart Cards nation-wide when it's Danmont (Dancoin in English) project - currently under trial - is launched in March next year.

In the trial town of Naestved, 70 kilometres south of Copenhagen, some 54 card sales outlets have been organised and Smart Card holders among the 45,000 residents can use them to make calls from 20 card payphones, pay for journeys on buses, use them in laundries, buy drinks and snacks from vending machines - and use one of Naestved's two parking meters!

The scheme has attracted attention from observers all over the world, and many are asking the same question: Can this relatively small country, with a population of just over five million, succeed in such a massive and costly undertaking? This is a particularly pertinent issue when the scheme is aiming at very small transactions of between 3Kr and 7Kr.

Continued on page 3

Smart Card News

Editor: Jack Smith

Technical Advisor: Dr David B Everett

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 3 - Physical Characteristics of the Contact Card.

An update on GSM.

CONTENTS

NEWS

Bull Calls for Harmonisation 25

Campus Management System 25

Who will accept this scheme ? 26

Banks still "testing the water" 28

JerseyCard Launches Cash Purse 29

TECHNICAL BRIEFINGS

NIST Advanced Smart Card
Access Control System (ASACS) 31

Smart Card Tutorial - Part 2
How the IC Card is Made 33

Smart Card Diary 38

A smart way to travel 38

Gemplus offering public key 39

Electronic toll collection 40

Danish Smart Card Scheme

Continued from page 1

The Danmont system consists of the Danmont cards (at present non-rechargeable cards which will later be superseded with multi-function Smart Cards), a network of service payment terminals, several concentration points where transactions from different service providers are collected and forwarded to the single clearing system. It is interesting in the Danish system that the transactions will be posted as a total and not individually.

So far 20 service providers have issued cards for the test trial, including the top six Danish banks -Den Danske Bank, Unibank, Bikuben, Jyske Bank, GiroBank, and Arbejdernes Landsbank, the two local banks Haandvaerkerbanken A/S and Naestved Diskontobank, and the Copenhagen Telephone Company (KTAS).

The cards are being supplied by Danish card suppliers dz danmark Ltd and ID Kort Ltd with a Siemens SLE 4404 M2 416 bit chip. Service payment terminals authenticate the cards using a Secure Application Module (SAM) which is implemented as a single chip microprocessor card. The SAM program is based on a Hitachi H8 chip, and the German company, Giesecke & Devrient/GAO has developed an operating system called STARCOS with, among others, the block protocol T=1 and an encryption system based on the DES algorithm. The Hitachi H8 chip is configurated with an 8 Kbyte EEPROM, 10 Kbyte ROM and 256 byte RAM. The processor is 8 bit.

Implementation

The implementation of the DANMONT system is planned to take place in five phases.

1. test of the system in the town of Naestved (started 1 September)
2. nation-wide expansion from 1 March 1993.
3. introduction of a rechargeable, prepaid card from 1 April, 1994
4. introduction of a multi-function card with limited functionality, and
5. extending the multi-function card using the full functionality.

Significant features

There are three particularly significant features about the scheme:

* Danmont is securely based on full co-operation between the banks and telecommunications industries.

* The Danes have decided on an "open system" with one "system operator."

* The implementation is taking place in five distinct stages with success viewed in the long term.

In June 1991, KTAS (Copenhagen Telephone Company Ltd) on behalf of all the Danish telephone companies, and PBS (Danish Payment Systems Ltd), on behalf of the Danish banks and savings banks, set up Danmont A/S for the purpose of introducing a prepaid plastic card based on IC card technology to be used for the payment of small amounts, with the ultimate intention of upgrading the card to a microprocessor-based card suitable for use as a multi-function card.

There is no doubt that the strength of the scheme lies in the fact that the financial and telecommunications industries - two of the biggest potential users of Smart Card technology - have joined forces to implement the scheme.

Thus, instead of fighting over who gets the icing on the cake, each party has a predetermined share in a unique arrangement which could provide a role model for other countries.

Henning Jensen, Managing Director of Danmont, says: "If you cannot co-operate you cannot get low cost. So even the biggest bank and the smallest savings bank are theoretically having the same unit cost in Denmark on their payments. because you are not killing your competitor on payment systems."

Open system

Danmont admits that its "Open System" concept demands large initial investments, and has a longer development and penetration time than closed systems. But what is unique about the Danish system is the decision to establish a single "system operator" and a single clearing centre, giving complete independence between the card issuers and the service providers. This makes it possible to be a service provider without also being a card issuer at the same time, enabling small merchants to obtain access to the system.

Danmont has also made strenuous efforts in all stages of the project design to keep costs down. On the card side, for example, the card issuer pays for the card himself but Danmont has advised on the opportunities to sell both sides of the card for corporate or promotional advertising, thus substantially reducing or removing card costs. In fact one of the banks involved is now planning to issue three new series of cards.

Since the start of the project Danmont has said that the cost of the card accepting device had to be between 3,000Kr and 5,000 Kr and now they can be bought from three different suppliers today in this price range.

While there is an additional cost to the service provider for integrating the device into the various machines, such as telephone or vending machines, this is a one-time outlay. The cost of the device is about the same as for a coin handler but with the advantage of removing vandalism which costs between 5 and 10 times the amount of cash stolen.

Long term success

The owners of Danmont have allocated £8 million to finance the scheme. Income will consist of interest on the money floating around in the system (the float), the remaining value left on unused pre-paid cards which Danmont conservatively estimates at one per cent of the turnover, plus the clearing charges on collections.

Mr Jensen said: "Whenever a card is sold we get the money so the bank, for example, gets neither the settlement nor the float and none of your readers in banking will understand why the banks are doing this because they are not used to co-operating. In Denmark the banks are saying okay if our contribution is that the float is paying the Danmont we don't mind because we own half the company. Service providers like Copenhagen Telephone, for example, is saying maybe we will have to pay for the transactions, maybe we will even have to pay more than we believe but if that is our price to get moving with a uniform card all over the country then we own half the company. The question about prices and float and so on is diminished because you are a shareholder. There are many people who do not understand this. They are very narrowly looking at 'what is my bank's interest'. Doing that no system can ever work."

Looking ahead to the introduction of the multi-application card, he says the prepaid is only one application and Danmont is not making the multi-application card, and is not pushing any other application to the multi-function card.

If prepayment is only one of the applications for the multi-functional card, what are the others likely to be? Strong possibilities are GSM as one of the GSM operations in Denmark is owned by the telecoms, pay-tv in which telecoms are also deeply involved, home banking and new products to the banking and finance industry.

It is envisaged that a new company will run the multi-function card and that Danmont will be a partner. Mr Jensen said: "We are securing our own application to be ready for the multi-application card because it is an important application.

"More and more international observers who are talking to us," said Mr Jensen, "can see that if you ever want to get into this you have to find ways of co-operation, maybe not as complete as Danmont but at least there has to be co-operation between the major parties behind the card because if a bank issues it or the banking industry they will not succeed.

If public transportation do it they will not succeed - only in their own sector. But by having everybody selling the same basic card they are gaining more than they are losing on co-operation.

"It is difficult in big countries but I know there are people saying it must be possible."

Robin Townend, Research Manager at Barclays Bank, UK, who was one of the observers visiting Naestved to see the trial in action, comments: "If they don't do it nobody else will."

NEWS

Bull Calls for Harmonisation

Europe, and particularly France, held the lead in the field of card operating systems, but they had to be wary of potential products which were appearing, in particular from Japan warned David Stephenson, Director, International Operations and Business Development, Bull CP8.

He told delegates at ESCAT (the European Smart Card Applications & Technology) conference in Finland last month that he believed that Europe still had a significant lead both technically and conceptually with regard to the security features in the chip and in the operating system. The Japanese S card used a non-standard block protocol (T=14) and most likely a Japanese algorithm (FEAL). The S card would not bring anything new either to the marketplace, or to the numerous customers who used cards such as TB100 today.

The TB100 card was the result of a joint project between Bull CP8 and TRT-Philips, aimed at producing a multi-service provider/multi-applications European operating system which met ISO standards.

"This object was achieved, and I believe that it is not too late for the European card manufacturers to rally around an operating system such as TB100 which meets the ISO standards, rather than dispersing our efforts and resources to develop additional new general purpose operating systems," he said.

He added that standards could be used in a positive way to accelerate market growth, but they could also be manipulated in such a way as to stifle and retard the development of a technology and its market.

When correctly developed, standards served to reassure future users of the technology. However standards could have a serious effect in slowing down the development of a new technology and its related applications "when the industrial companies of one country or another believe that it is justified to change perfectly adequate and established standards simply to further their own interests."

"With the benefit of hindsight, one cannot find any other reasons for past conflicts in the IC card industry in determining standards, or the appearance of new standards to cohabit with, and stand alongside perfectly adequate existing ones.

"This has been demonstrated in the past by the adoption the block protocol, spurred only by national interests and the interests of one or two individual companies, as an alternative ISO standard, but which provides no distinct advantage for 95 per cent of card applications, whilst requiring increased, and consequently more costly, resources."

One could always find more than one way to skin a cat, he said, but he was disappointed that a united European approach could not be found to the card protocol question, so as to defend the interests of both customers currently using IC card applications and technology, and the interests of the European industry in general.

Campus Management System

DataCard Corporation is to start marketing a new Smart Card-based All-in-ONE-Card Campus Management System to colleges and universities. Designed to meet the demand for a single student ID card which can be used for identification, transaction processing and access control applications, the system will be available for installation in the summer of 1993.

Students will only need to have one card carrying their identity and allowing them to access food services, debit tuition and bookstore accounts, and make convenience store and off-campus retail purchases and small value transactions such as at vending machines, laundries and copy machines. DataCard says the security features eliminate the potential for fraudulent use or duplication and safeguard the student's prepaid accounts while minimising the school's exposure.

David Tushie, President and General Manager, Smart Cards and Systems Division, says the All-in-ONE -Card Campus Management System is positioned for use by a larger non-campus constituency.

Contact: Mark Iverson, Director, Marketing, DataCard Corporation. Tel: +1 612 931 1763.

Who Will Accept This Scheme?

Cambridge, one of the most attractive cities in England and known all over the world for its famous university, may have its traffic problems eased in a revolutionary Smart Card scheme scheduled to begin testing next year.

However, the electronic congestion metering system planned for the city is likely to exasperate vehicle owners, particularly resident drivers, and turn tourists away.

A charge will be levied on drivers for a unit of congested road, a unit being .5 km or one third of a mile. Three basic elements of time, distance and inertia have been combined to trigger payment above a threshold.

The system will target congested conditions only and if applied at 20p per unit it would increase the marginal cost of motoring in congested conditions from 6p per mile (petrol costs) to 66p (60p congestion plus 6p petrol). This increases the marginal cost in congested conditions by a factor of 10 whilst leaving the costs unchanged in all other conditions.

The threshold has been provisionally set at four stops within any half km, or alternatively when the time taken to travel any half km is above three minutes.

State-of-the-art

Technically this is a clever scheme using advanced state-of-the-art technology, but if drivers feel they are going to be penalised every time they are caught up in a traffic jam or fail to cover a predetermined distance within a certain time, some may be tempted to speed when they have the opportunity, jump traffic lights and pedestrian crossings and fail to give way at roundabouts.

If the result is an increase in road traffic accidents, the Council will have to think again about the plans.

So far reactions from residents have been muted, but as one prominent opinion former commented: "This scheme is so bizarre that people have not bothered reacting. They think it is so crazy that it will never happen."

Prepaid Smart Card

The method of payment is by a prepaid Smart Card which will contain a certain number of units, say 50, and would be purchased for £10 if the price per unit is 20p.

However, a-self policing control mechanism is needed, and this will be in the form of a meter installed in vehicles. The Smart Card will energise the car when inserted, and de-energise it when removed. An "overdraft" will be allowed, say 50 units, at which point the card must be recharged and the overdraft paid off before the onboard unit will accept the card for the next journey.

The City will be controlled by beacons on all 17 radial roads which will "switch on" the in-car meter by microwave. All journeys made in the City will be metered and switched off again on exit.

The County Council says that metered vehicles will form the vast majority of all vehicles entering the City, especially at peak hours.

Non-metered, non-regular users such as business callers, visitors and tourists, will have to pay to enter the City by car. It is envisaged that all visitors entering by vehicle will purchase a daily pass at automatic machines at City entrances.

A research grant awarded in 1990 by the Science and Education Research Council to a consortium, including Newcastle University and Newcastle Polytechnic, has enabled a laboratory prototype meter to be produced, and as part of the ADEPT (Automatic Debiting and Electronic Payment for Transport) consortium under the DRIVE project of the European Commission, sufficient resource is available to allow a miniaturised onboard unit to be produced. This is expected to be available in the summer of 1993 for demonstration including the microwave beacon technology and the Smart Card application.

Field trials

Cambridgeshire County Council propose to carry out full field trials on at least 100 vehicles starting in 1993. This will give them the opportunity to evaluate their time, distance and inertia formula and decide how it stacks up in practise against traffic lights, pedestrian crossings, roundabouts, and road works.

However, before full implementation of the scheme in 1995, the Council will require legislation to charge for the use of certain roads by congestion metering, and to give the Council powers to insert meters free of charge to all vehicles owned by residents or companies within a designated area.

It is estimated that some 250,000 vehicles in a 15-mile radius of Cambridge, and in the City itself, will be equipped with the meters.

The County Council is funding research into the scheme and has allocated £100,000 for two years, and hope to attract contributions from unnamed other sources.

The Cambridge congestion metering scheme is one of five field trials within the ADEPT project. The other pilot sites and trials are:

Trondheim, Norway	Integrated payment and multi-transponder services
Lisbon, Portugal	Parking pre-booking, guidance and debiting
West Sweden	Multi-lane road use pricing and integrated RTI (Road Traffic Informatics) services
Greece	Multi-lane and mono-lane automatic toll collection and driver information (Malagra Highway).

Contact: Robert Tuckwell, Project leader and Group Engineer for Cambridge Transportation Planning. Tel: +44-(0)223 317724.

McCorquodale agreement

Siemens has signed a long-term agreement with McCorquodale Smart Card Systems to license its Smart Card operating system software for distribution throughout the world, including former Eastern Bloc countries.

McCorquodale said that the two companies were working together to develop new chip technologies specifically for Smart Card use. An integral part of the contract is a new microcontroller line designed by Siemens, using submicron CMOS technology and fast encryption techniques for chip card applications.

Doscar Smart Card Security

Doscar, an MS-DOS device driver for OKI standard Smart Cards using the OSCAR operating system, and providing 8Kb of secure memory (16Kb cards are planned for the end of this year) has been announced by Smart Card Solutions.

The user can treat the Smart Card as just another floppy disk. It can be used to control and monitor the use of a range of products and services, protect data files from unauthorised users, and hold data which needs to be both portable and safe, for example, financial transactions, medical records or company confidential files. The Doscar cards are read by a reader unit which fits into the PC like a conventional disk drive.

Contact: Owen McLaughlin, Director, Smart Card Solutions Ltd, 71 High Street, Earith, Huntingdon, Cambridgeshire, PE17 3PP, England. Tel: +44-(0)487 740865.

SWIFT Smart Card

Further details are now available on the new SWIFT (Society for Worldwide Interbank

Financial Telecommunications) Smart Card to be mandatory for Electronic Funds Transfer messages by financial institutions from the first quarter of 1994.

Called USE (Users Security Enhancement) the system goes to pilot testing in mid-1993. The card being used is the Bull CP8 standard ISO ID1 with a Motorola chip, 4Kbytes of Mask ROM, 8Kbytes of EPROM, and 128 bytes of RAM. The communication protocol is T=0, and security is provided by a six-digit PIN and a proprietary crypto algorithm. The card design is shown on page 21 without the chip embedded in the plastic.

Banks still "testing the water"

The UK banks have been experimenting with Smart Cards for a number of years now in what has amounted to "testing the water," but so far they seem reluctant to commit themselves to what many regard as the inevitable adoption of Smart Card technology.

The dilemma of the banks is that there is no straightforward business case to replace their existing card systems based on magnetic stripe cards, and they recoil from the massive expenditure involved in attempting to substitute another system. At the same time they desperately seek new business in the fiercely competitive financial markets and view with mounting concern the aggressive activity of the European PTTs who appear to be driving the use of Smart Cards (albeit small memory cards at the moment, but with the potential to expand into multiple applications and scoop up business at the expense of the banks).

Banks in general tend to cater for the needs of the As, Bs and Cs of the world, but there are many, many thousands of people who do not have bank accounts and to whom an "electronic purse" type of card would be attractive. While the banks have managed very well without this business they must be anxious that the multi-million pound collective spend of this group could be attracted to some new money handling system which could make inroads into their own business.

Banking dilemma

The ESCAT (European Smart Card Applications & Technology) Conference in Helsinki, Finland, last month gave an interesting insight of the banking dilemma and the momentum of telecommunications activity in Smart Cards.

Roger Alexander, Assistant Director of Barclays Bank Central Retail Services Division in England, said that in-house studies at Barclays in the mid-eighties formed some basic conclusions about Smart Card technology that still held good today - that current magnetic stripe technology had (and still did have) security and data storage capacity limitations, that international standardisation would be required to ensure interoperability, that Smart Cards were expensive, that migration would take a long time in view of the existing investments in magnetic stripe cards.

However, the Smart Card offered a high level of security both in terms of authenticating the card and verifying the cardholder, it could support multiple applications, and it could function securely off-line providing savings on communications costs.

"Importantly," he said, "the technology was firmly recognised as that which would ultimately become the next generation of financial transaction card."

Costs of the Smart Card, little interoperability and the lack of international standardisation had been the principle arguments why financial institutions, outside France at least, had not embraced the technology. To a limited extent this was still true today, particularly if viewed as a magnetic striped card replacement.

No cost justification

"Put simply," said Mr Alexander, "today there is no cost justification, no infrastructure and standards are still being developed, a situation that has not changed since the early 80s. This does not mean, however, that there is no place for the

Smart Card in retail banking. On the contrary, the card business is very competitive, in the UK alone we have over 100 different Visa and MasterCard products. So, how can card issuers differentiate their products? How can card issuers ensure that their card is the preferred card and the one which is taken from the wallet or handbag at the Point-of-Sale?

"What the chip can offer over and above the magnetic stripe is the provision of Value Added Services, and these can be the differentiators. Ideally, they should be fee-based to offset the incremental cost of adding the chip and for generating new income streams. The card would therefore be a hybrid card, the magnetic stripe would manage the payment functions and the chip would offer new and valuable services for the cardholder. Ultimately, I see the chip managing the electronic payment functions but only when there is a critical mass of hybrid terminals in the market place.

"The successful implementation of this concept in retail banking applications is the dependence upon selecting the right Value Added Services!"

The most promising Value Added Services must be those that had universal appeal to ensure substantial market penetration thereby helping establish the critical mass of terminals to assist migration for payment system applications.

There were several case studies such as the French Banks offering payphone services. Public payphones were currently the most popular Value Added Service but other telecommunications applications were under development, most notably videotext services. Global System for Mobile Communications (GSM) and Personal Communications Network (PCN) - the next generation of mobile communications which would be Smart Card driven. All this indicated the growing importance and influence of the telecommunications operators in the market development of Smart Cards.

Other Value Added Services included motoring services, health care, travel, cashless parking, vending, fast food, and frequent shopper programmes.

What had been described, he said, was a typical bank card with an embedded chip giving access to a range of Value Added Services from which the cardholder could select those most relevant to their lifestyle. With this concept the primary function of the card remained a payment card, with the logo and features relating to the issuer and payment system. Some services could be provided free to the cardholder, for example, frequent shopper where the supermarket or oil company would pay the card issuer a rent for the space on their chip, or would be fee based as in the case of the medical applications.

Telephone based applications

Jerome Svigals, Inc., USA, had some interesting figures to give to conference delegates. PTT national level organisations headed the list of large volume Smart Card orders during the past year with 21 orders compared with 5 orders for national/social programs. In terms of volume, France had ordered 155 million cards for telecom coin replacement, and Germany 70 million.

JerseyCard Launches Purse

JerseyCard, the IC Card system on the self-governing duty free island of Jersey in the English Channel, is expanding its services with the launch this month of a pre-payment cash purse facility. It has also extended its services to the neighbouring island of Guernsey where they will be marketed under the name "GuernseyCard." And as the interest in Smart Card technology gathers momentum, the company is also busy offering its experience to others who want to use their system.

Since its inauguration in 1987, it has been building its customer base and card reader infrastructure. Currently around 20,000 cards have been issued in Jersey (population 85,000) and some 190 card readers have been installed in merchant sites. About one third of the readers accept the JerseyCard for a specific facility including charge accounts at a major department store, a wines and spirits retail chain, a group of garages, and also as a membership access system to the local leisure centre.

This month, JerseyCard Ltd launches the JerseyCard Cash Purse - a pre-payment system useable at selected merchant sites as a general means of payment. The multi-function card is capable of offering 23 different services so there is no need to issue a new card. Customers who want to use the cash purse facility will pay a £5 administration fee which is a one time payment. For all other purposes the card will continue to be issued free to customers.

The cash purse will be initialised at the JerseyCard offices or at one of two other approved points. Cardholders will be able to go to any service provider to have the card recharged by handing over cash or using any debit card. The cards will be used initially in a department store, a garage group, a newspaper and gift shop chain and at certain public houses.

They will be available to two groups of cardholders - residents holding a card for one of the above purposes and, by arrangement with a French company organising conferences on the island, visiting delegates who will be issued with the pre-loaded cards which they can purchase prior to arrival and use to buy duty free gifts.

In Guernsey, where the system is being offered as a "department" of JerseyCard, the GuernseyCard is being used initially with a garage chain but will soon include three other garages and a large store. This says JerseyCard Ltd, opens the door for any retail chain operating in both islands to use the system.

Chris Parlett, Executive Manager, JerseyCard, said: "We are also talking to the airline and the hydrofoil company who operate inter-island services."

The first card using the JerseyCard system has just been launched in Scotland in conjunction with JerseyCard, with another due soon in the South of England. Lanarkshire Card Ltd are planning to duplicate the JerseyCard operation in part of the Strathclyde area of Scotland south east of Glasgow and covering Motherwell, Hamilton, East Kilbride, Coatbridge, and Airdrie.

As in the JerseyCard system, the scheme is being financed by private investment. Dave Mather, of Lanarkshire Card, says: "We intend to duplicate the JerseyCard operation in Lanarkshire area and are now seeking customers. The response so far is quite good." The clearing of the transactions, he said, would be through the Bank of Scotland.

Another success for JerseyCard is that one of the largest UK Training and Enterprise

Councils based in the Midlands of England, has recently agreed to use the JerseyCard and data collection system in a pilot to track the progress of people going through a training programme in their area. As a result, JerseyCard are now in discussion with several other TECs with a view to providing a training credits system.

A major UK tyre and garage chain has recently expressed interest in the JerseyCard system and they continue to entertain a stream of visitors from all over the world.

Mr Parlett said: "JerseyCard will continue to offer our system in other parts of the country and in other countries."

In the Jersey scheme the IC Card reader terminals also read credit and debit cards. The IC Card can be used as an account card, a membership card or an electronic purse and the cardholder can have several different services on his card which is used in conjunction with a Personal Identification Number (PIN).

Service providers pay JerseyCard a rental for taking space on their chip. The service providers process their transactions through Barclays Merchant Services "on preferential terms" and as a result Barclays has substantially increased its market share of the acquiring business on the island.

Card details

Type:	Contact
Fabricator:	Gemplus
Dimensions:	ISO ID1 size
Contact location:	ISO 7816-2 Front
Chip manufacturer:	SGS-Thomson
Chip Ref No.:	GPM416
Chip type:	Memory
Memory type:	EEPROM
Standards:	ISO 7816
Comms protocol:	T1
Security:	PIN (four digit)
Cryptography:	DES (Terminal only)

Contact: Chris Parlett, Executive Manager, JerseyCard Ltd Tel: +44-(0)534 37713.

The NIST Advanced Smart Card Access Control System (ASACS)

The security technology group of NIST (US National Institute of Standards & Technology) has designed an advanced computer access control system in response to the needs for a secure yet easy to use authentication scheme. The smart card and related terminals (called smart drives) have been developed by Datakey Inc. in collaboration with NIST.

The scheme is recommended for use in US Government Internet systems (ASACS is being integrated by Trusted Information Systems Inc. - TIS) as well as in banking networks and other networks which must restrict access to sensitive but unclassified data. This project was sponsored by the US Defence Advanced Research Project Agency (DARPA).

ASACS is the third in a series of NIST research projects which involve the design and development of smart cards with cryptographic capabilities and the application of such cards to problems in computer security.

A key feature of the ASACS smart card is its cryptographic capability which offers the following algorithms,

- RSA
- DSA (Proposed NIST digital signature algorithm, see appendix)
- DES

This is probably the first implementation of the proposed new DSA algorithm on a smart card. The IC chip is the Hitachi H8/310 using a 10mhz clock. The cryptographic performance is shown in the table below,

Algorithm	DSA	RSA
Global Computation	off card	N/A
Key Generation	29 seconds	off card
Pre-computation	28 seconds	N/A
Signature creation	0.05 seconds	25 seconds
Signature verification	56 seconds	5 seconds

The card contains the following public key command set,

- Generate keys (DSA)
- Load private key (RSA)
- Load public key
- Encipher (RSA)
- Decipher (RSA)
- Pre signature computation (DSA)
- Signature creation (DSS)
- Signature verification (DSS)

The Hitachi H8/310 has 10K bytes of mask ROM, 8K bytes of EEPROM and 256 bytes of RAM. Although the current card does not conform to ISO 7816-3 the next generation NIST card will conform using the T=0 communications protocol. The card is of standard ISO ID-1 size with the connector on the front of the card.

The ASACS card implements the following set of cryptographic functions,

- Secure user authentication (3 way encrypted handshake)
- Generates message authentication codes (MAC)
- Low speed file and line encipherment
- Support for ANSI X9.17 automated key distribution
- Support for applications using portable reader/writer
- Secure data storage for cryptographic keys and user passwords
- Secure data storage for audit trail information
- Random number generation
- Public key digital signature capability (DSS and RSA)
- PIN verification

Datakey Inc. has developed a product line that consists of the signature card and two readers. The model 10 desktop smart card reader/writer connects to the users work station using an RS232 serial interface. The terminal supports card based user authentication for both local and wide area network log on.

The model 20 portable smart drive includes a keyboard and display as well as the standard RS232 serial interface. This unit is designed for users who travel between different work sites.

The ASACS card and desktop reader/writer system is available from Datakey Inc. in small quantities for $150:00

Contacts:

James Dray - ASACS Project leader NIST Security Group. Tel: USA. 301-975-3356

Gary Ostrem - Datakey. Tel: USA. 612-890-6850

Appendix - The NIST Proposed Digital Signature Standard (DSS)

The DSS algorithm is in many ways similar to Schnorrs signature scheme. The DSS algorithm was announced by NIST in August 1991 and was published for public comment. The security of the DSA algorithm is based on the discrete logarithm problem which is no less than the difficulty of factorisation. The algorithm contains the following global computations,

$p = 2^{511} < p < 2^{512}$ where p is prime

$q = 2^{159} < q < 2^{160}$ where q is a prime divisor of p-1

$g = h^{(p-1)/q}$ Mod p where $0 < h < p$ such that $g > 1$ (i.e $g^q = 1$ Mod p)

p, q and g are global constants for a particular security scheme.

Key calculation

A users public and private keys are calculated as follows,

Private key x = an integer such that $0 < x < q$
Public key $y = g^x$ Mod p

Signature computation

The user calculates a signature on a message digest m as follows,

Choose k to be a random number $0 < k < q$
Calculate $r = (g^k \text{ Mod } p) \text{ Mod } q$
Calculate $s = k^{-1} (m + xr) \text{ Mod } q$

The signature consists of r and s each of 20 bytes.

Signature verification

The checker verifies the signature as follows,

Compute $w = s^{-1}$ Mod q
$u1 = mw$ Mod q
$u2 = rw$ Mod q

Calculate $v = ((g^{u1} * y^{u2}) \text{ Mod } p) \text{ Mod } q$

If $v = r$ as received then the signature is verified.

Smart Card Tutorial - Part 2

How the IC card is made

The manufacture of a smart card involves a large number of processes of which the embedding of the chip into the plastic card is key in achieving an overall quality product. This latter process is usually referred to as card fabrication. The whole operation starts with the application requirements specification. From the requirements individual specifications can be prepared for the chip, card, mask ROM software and the application software. The ROM software is provided to the semiconductor supplier who manufactures the chips. The card fabricator embeds the chip in the plastic card. It is also quite normal for the fabricator to load the application software and personalisation data. Security is a fundamental aspect in the manufacture of a smart card and is intrinsic to the total process. However we will consider security separately in subsequent articles in this series. We will look at each of the stages in the manufacture of the smart card as shown in fig. 1.

Chip specification

There are a number of factors to be decided in the specification of the integrated circuit for the smart card. For the purpose of this discussion we will consider a CPU based card although the manufacture of a memory card is substantially a subset of that described here. The key parameters for the chip specification are as follows,

-Microcontroller type (e.g 6805,8051)
-Mask ROM size
-RAM size
-Non volatile memory type (e.g EPROM, EEPROM)
-Non volatile memory size
-Clock speed (external, and optionally internal)
-Electrical parameters (voltage and current)
-Communications parameters (asynchronous, synchronous, byte, block)
-Reset mechanism
-Sleep mode (low current standby operation)
-Co-processor (e.g for public key cryptography)

In practice the semiconductor manufacturers have a range of products for which the above parameters are pre-defined. The task of the designer is therefore concerned with choosing the appropriate product for the particular application. As mentioned previously security may be an important issue for the application and accordingly there may be extra requirements on the physical and logical security offered by the particular chip. Conformance to ISO standards is also likely to be a requirement and in this area ISO 7816 - 3 (Electronic signals and transmission protocols) is the principle standard to be considered. It should be noted however that ETSI (European Telecommunications Standard Institute) are currently developing new standards for the CEN TC224 committee. These standards are more stringent than that described by the ISO standards. For example the ISO 7816-3 allows a card current supply of up to 200 mA. ETSI have recommended 20mA for normal use and 10mA for applications such as portable phones.

Card specification

The specification of a card involves parameters that are common to many existing applications using the ISO ID-1 card. The following list defines the main parameters that should be defined,

- Card dimensions
- Chip location (contact card)
- Card material (e.g PVC,ABS)
- Printing requirements
- Magnetic stripe (optional)
- Signature strip (optional)
- Hologram or photo (optional)
- Embossing (optional)
- Environmental parameters

The characteristics of the smart card are part of the ISO 7816 part 1 (physical) and 2 (contact location) standards. The choice of chip location has been a difficult subject due largely to the use of magnetic stripes. The early French cards put the IC module further off the longitudinal axis of the card than the standard eventually agreed by

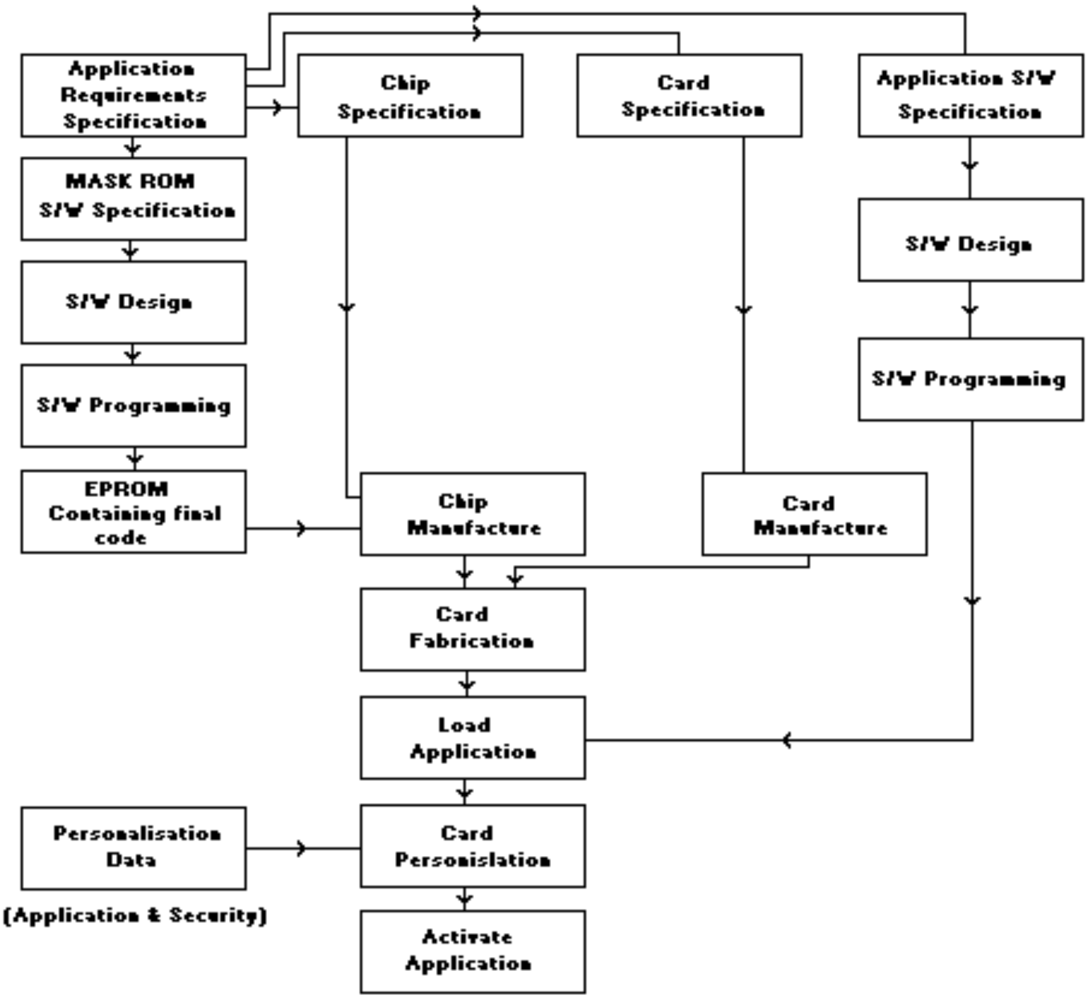


Fig 1 Stages in the manufacture of a smart card

ISO. This was preferable because of the residual risk of chip damage due to bending. The French Transac tracks were lower on the card which also made this position preferable. The now agreed ISO standards for magnetic stripes resulted in the French chip position and the magnetic stripe being coincident. Hence the now agreed lower location which does of course result in higher bending stress on the chip. The ISO 7816-2 standard does however allow the position of the contacts to be either side of the card. More recently there have been moves to remove this option with the front (opposite to the side containing the magnetic stripe) being the preferred position for the IC connector.

The choice of card material effects the environmental properties of the finished product. PVC was traditionally used in the manufacture of cards and enabled a higher printing resolution. Such cards are laminated as three layers with transparent overlays on the front and back. More recently ABS has been used which allows the card to be produced by an injection moulding process. It is even proposed that the chip micromodule could be inserted in one step as part of the moulding process. Temperature stability is clearly important for some applications and ETSI are particulary concerned here, such that their higher temperature requirement will need the use of polycarbonate materials.

Mask ROM Specification

The mask ROM contains the operating system of the smart card. It is largely concerned with the management of data files but it may optionally involve additional features such as cryptographic algorithms (e.g DES). In some ways this is still a relatively immature part of the smart card standards since the early applications used the smart card largely as a data store with some simple security features such as PIN checking. The relevant part of the ISO standard is 7816-4 (commands). There is a school of thought that envisages substantial changes in this area to account for the needs of multi-application cards where it is essential to provide the necessary security segregation. The developed code is given to the supplier who incorporates this data as part of the chip manufacturing process.

Application Software Specification

This part of the card development process is clearly specific to the particular application. The application code could be designed as part of the mask ROM code but the more modern approach is to design the application software to operate from the PROM non volatile memory. This allows a far more flexible approach since the application can be loaded into the chip after manufacture. More over by the use of EEPROM it is possible to change this code in an development environment. The manufacturer of a chip with the users ROM code takes on average three months. Application code can be loaded into the PROM memory in minutes with no further reference to the chip manufacturer.

Chip Fabrication

The fabrication of the card involves a number of processes as shown in fig. 2. The first part of the process is to manufacture a substrate which contains the chip. This is often called a COB (Chip On Board) and consists of a glass epoxy connector board on which the chip is bonded to the connectors. There are three technologies available for this process, wire bonding, flip chip processing and tape automated bonding (TAB). In each case the semiconductor wafer manufactured by the semiconductor supplier is diced into individual chips . This may be done by scribing with a diamond tipped point and then pressure rolling the wafers so that it fractures along the scribe lines. More commonly the die are separated from the wafer by the use of a diamond saw. A mylar sheet is stuck to the back of the wafer so that following separation the dice remain attached to the mylar film.

Wire bonding is the most commonly used technique in the manufacture of smart cards.

Here a 25uM gold or aluminium wire is bonded to the pads on the chip using ultrasonic or thermo compression bonding. Thermo compression bonding requires the substrate to be maintained at between 150C and 200C. The temperature at the bonding interface can reach 350C. To alleviate these problems thermo sonic bonding is often used which is a combination of the two processes but which operate at lower temperatures.

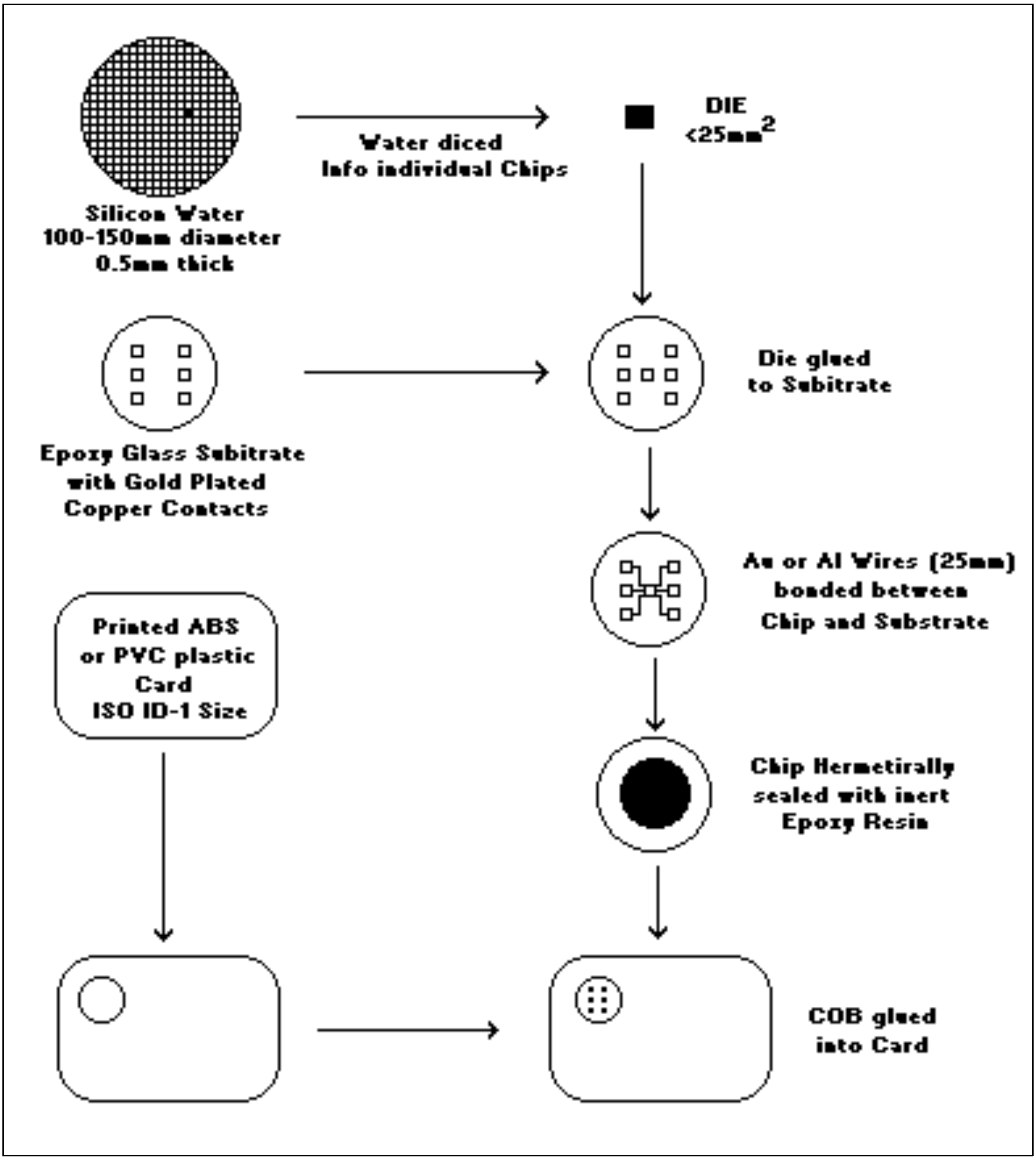
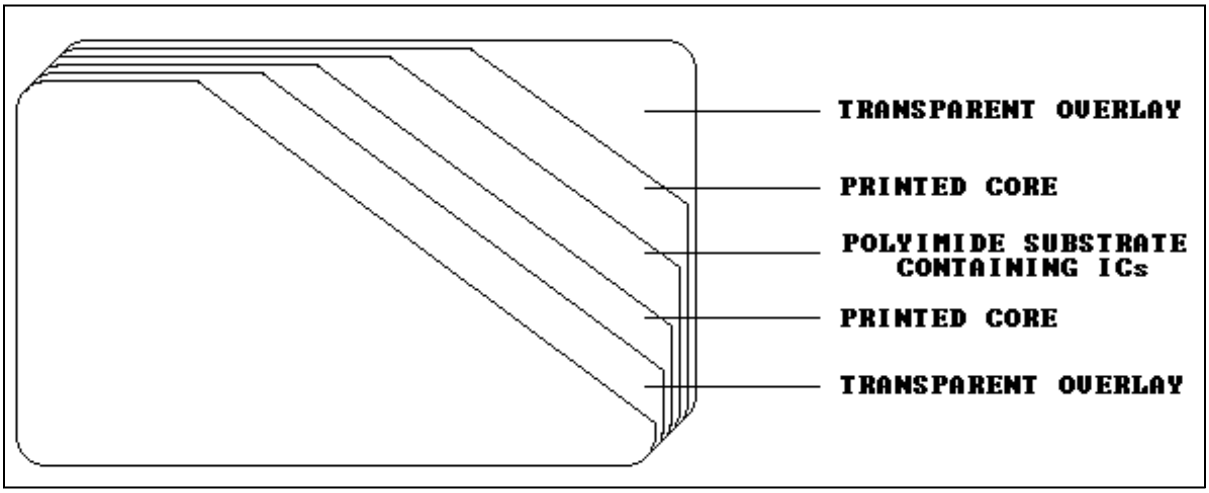


Fig 2 Smart card fabrication process

The die mounting and wire bonding processes involve a large number of operations and are therefore quite expensive. Because in general only 5 or 6 wires are bonded for smart card applications this approach is acceptable. However in the semiconductor industry generally two other techniques are used, the flip chip process and tape automated bonding. In both cases gold bumps are formed on the die. In flip chip processing the dice are placed face down on the substrate and bonding is effected by solder reflow. With tape automated bonding the dice are attached by thermocompression to copper leads supported on a flexible tape similar to a 35mm film.

The finished substrate is hermetically sealed with an inert material such as epoxy resin. The complete micromodule is then glued into the card which contains the appropriately sized hole.

The fabrication of a contactless card is somewhat different since it always involves a laminated card as shown in fig. 3. The ICs and their interconnections as well as the aerial circuits are prepared on a flexible polyimide substrate.



Application load

Assuming the application is to be placed in the PROM memory of the IC then the next stage in the process is to load the code into the memory. This is accomplished by using the basic commands contained in the operating system in the mask ROM. These commands allow the reading and writing of the PROM memory.

Card Personalisation

The card is personalised to the particular user by loading data into files in the PROM memory in the same way that the application code is loaded into memory. At this stage the security keys will probably be loaded into the PROM memory but as mentioned previously we will explore this in more detail later.

Application Activation

The final operation in the manufacturing process is to enable the application for operation. This will involve the setting of flags in the PROM memory that will inhibit any further changes to be made to the PROM memory except under direct control of the application. Again this is an integral part of the overall security process.

Fig 3 Contactless card laminations

Smart Card Diary

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'Expliotation 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.

CardTech/SecurTech/ISSA '93 Conference and Exhibition, Hyatt Regency Hotel, Crystal City, Virginia, USA, 18-21 April.

Ten concurrent seminars will be held throughout the three main days of the conference - CardTech tracks stressing applications of advanced card technologies, SecurTech tracks addressing specific applications, and ISSA (Information Systems Security Association) tracks focusing on security. A major exhibition is being run in conjunction with the conference. Contact: Ben Miller (CTST) Tel: +1 301 881 3383.

A Smart Way to Travel?

As the European Community moves towards more relaxed frontier controls there is a growing demand to use new technology, such as Smart Cards, to avoid queues and delays at passport desks.

Member states are being encouraged by Brussels to allow unhindered travel, but the British Government, while saying it will relax controls on EC citizens, has reserved the right to scrutinise documents at British points of entry. When the Channel Tunnel, linking Britain and France, opens there will be increased calls to ease restrictions on travellers.

A Smart Card, perhaps with some biometric identifier, is the likely long-term solution. Experiments are already underway in some countries. At Amsterdam's Schiphol airport, Dutch travellers who are frequent users of the airport - at least five times a year - can obtain a card containing passport details and a digitized fingerprint. They can avoid queues by using their Smart Card which positively identifies them as the rightful owner of the card through their fingerprint.

Advocates of this scheme say that the card readers and computer software could be installed at any airport.

Meanwhile, BAA, who operate the UK's airports say they are discussing such systems with the British Home Office but say it could be some time before Smart Card technology is available to British travellers.

Pilot test

In the United States, immigration officials are interested in a pilot test to be carried out at New York's JFK and Newark airports, which relies again on biometric techniques for the personal identification of the individual. Instead of fingerprints, the scheme uses hand geography technology. Passengers who are computer registered will have their passports scanned while a second system will read the palm of their hands to verify that they are who they claim to be and therefore the genuine holder of the passport.

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

□ UK £375

□ International £395

□ Please invoice my Company

□ Cheque enclosed

□ Please charge my credit card
Visa/Mastercard/Eurocard/Access

Name____

Position______________________________________

Company_____________________________________

Address______________________________________

____

Tel.____

Fax.____

Name_________________________________

Address_______________________________

____

Card No.______________________________

Expiry date____________________________

Signature______________________________
__

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

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

Gemplus Offering Public Key

Gemplus is offering an evaluation kit for public key cryptography called MIMOSA. The product is a public key algorithm Smart Card and Gemplus plan to introduce the Smart Card through the evaluation kit so that customers and potential customers can test this type of system and evaluate public key cryptography.

The G-Q (Guillou and Quisquater) algorithm has been embedded in the Philips 83C852 chip recently available from Philips in Germany. This will be the first public key chip from Gemplus which up until now has used DES for cryptographic security.

The G-Q algorithm was first proposed by Guillou and Quisquater at Eurocrypt '88 as a zero knowledge based identity scheme similar to that of Fiat and Shamir. This paper was updated at Crypto '88 to include a signature scheme.

The Fiat and Shamir signature scheme is

optimised for a lower processing overhead than RSA but at the expense of memory requirement and size of signature. The G-Q algorithm increases the processing but with less memory.

MIMOSA offers a method that keeps the number of keys and hierarchies required for multi-applications to a minimum. Gemplus says that this method, based on the use of a public key algorithm, considerably limits the role of the card issuer and enables more flexible management of cards.

The MIMOSA evaluation kit will be available shortly and consists of a software environment, sample cards, a card reader and accompanying documentation. MIMOSA is sold under a CCETT license.

Electronic Toll Collection

The electronic toll collection system under test at AT&T Bell Laboratories at Holmdel, New Jersey.

AT&T has developed an electronic toll collection system whereby drivers merely insert their personal Smart Card into a small radio transponder as they approach a toll-collection area. Receivers either mounted above the road or on the pavement (as illustrated in the drawing below) communicate with the transponder, noting the locations where the car entered and exited the highway, or where the toll was paid. The toll charge is transmitted back to the dash-top communicator and a record of the transaction is written onto the Smart Card.

The system allows drivers to pay tolls without stopping or fumbling for change, by identifying the moving vehicle. The transaction takes only milliseconds.

The card could operate as a prepaid debit card, or as a credit card with a running account and monthly billing.

Last April AT&T and Lockheed Corporation signed an agreement to jointly develop Intelligent Vehicle Highway Systems (IVHS) for a market said to be worth more than $200 billion over the next 20 years in the United States alone. Electronic collection of vehicle tolls is a key component of IVHS, and Lockheed has already installed the first such system in the US.

Contact: Michael Jacobs, AT&T
Tel: USA 201- 564- 3836.