Smart Card Payphones on Channel Tunnel Trains

Passengers on Eurostar trains which will operate from London's Waterloo International terminal to Paris and Brussels will be able to make phone calls using Smart Cards while speeding through the countryside on either side of the Channel Tunnel when it opens later this year. However, the phones will be dead for a period of about 26 minutes while trains are in the tunnel which does not have antennae.

Each of the 30 Eurostar trains will have four payphones - two in first class and two in standard class - provided jointly by Belgacom, BT and France Telecom.

Continued on page 143

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
Orga Kartensysteme

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 25 - Contactless cards

CONTENTS

Smart Card Payphones

Continued from page 141

The payphones have been specially designed to accept credit and charge cards such as American Express, Diners Club International, Eurocard, JCB, MasterCard and Visa, as well as a new pre-paid card which will only be available in bars on the Eurostar trains and can only be used on the trains.

The pre-paid 120-unit card, can be purchased in pounds sterling (£12) or in French francs. It is the GPM256 card from Gemplus, France.

France Telecom will operate 64 Eurostar payphones, BT 44 and Belgacom 16.

A visual display provides step-by-step instructions in a choice of six languages - English, French, Dutch, German, Italian and Spanish with additional notices in English, French, German and Dutch next to each phone. A free helpline number is also available and connects to operators who speak Dutch, English and French.

A new feature on the payphones offers an optional paper receipt detailing how much the call has cost if you use a commercial credit card or charge card.

Users must dial the full national access code for the country they are calling, irrespective of where the train happens to be at the time.

The payphones will operate on the pan-European cellular radio system known as GSM (Global System for Mobile Communications), and the pre-paid card will operate on the proposed T2G European Standard. The new technology payphones were developed and manufactured for the three partners by the Sagem Group, a French company based at Cergy St. Christophe, near Paris.

Reception will be better than most mobile phones as the payphone design incorporates a more powerful transmitter than a mobile phone and is connected to an external aerial which means it does not have to send and receive signals through the metal structure of the train or the reinforced windows.

In a separate development, BT and France Telecom have worked with Eurotunnel to provide payphone facilities on either side of the tunnel. BT are installing 76 Payphone 2000 phones at British Rail's Waterloo International terminal and 43 at Eurotunnel's shuttle and freight train terminus in Folkestone.

While France Telecom payphones use Smart payphone cards, BT phones (with the exception of those on the Eurostar trains) currently use optical cards. BT have said that they intend to change to Smart phonecards in the future. Eventually it should be possible to use the same Smart payphone card in major public locations, such as bus and rail stations and airports, anywhere in the EEC.

Contacts: BT Corporate Newsroom - Tel: +44 (0)71 356 5369; Michel Plazant, France Telecom - Tel: +33 1 40 01 69 19; or David Tusa, Belgacom - Tel: +32 2 205 4000.

Innovatron Franchise in Algeria

Algerian company NETSYS has signed an agreement with Innovatron Ingenierie, subsidiary of Groupe Innovatron, to become a member of its franchise network Innovatron Data Systems and distribute Smart Card technology in Algeria. Based in Algiers, NETSYS specialises in telecommunications and is diversifying its activities.

Contact: Genevieve Boeuf, Communication Manager, Innovatron, France - Tel: +33 1 40 13 39 42. Fax: +33 1 40 13 39 59.

Schlumberger Appointment

Jacques Cosnefroy has been appointed General Manager of Schlumberger's Smart Cards product group and joins the senior management team of the Smart Cards & Systems Division. He will be based at head office in Montrouge, France, and responsible for Smart Card R&D, marketing, sales and worldwide manufacturing facilities.

Aged 48, he was previously General Manager of the connector divisions of the German company Harting Elektronik.

New EEPROMs from Thomson

SGS-Thomson Microelectronics has announced two new devices aimed at Smart Card applications where security is not an issue but memory performance, in terms of resistance to data loss or accidental corruption, is a prime requirement.

The ST14C02 2K bytes EEPROM and the ST14C04

4K bytes EEPROM are organised in byte configuration and are fully compatible with the I^2C bus.

Thomson says these devices are particularly suitable for applications such as healthcare cards or other applications involving data that the issuing authority requires to be openly accessible, so the devices include no security logic but offer the low cost and high data integrity essential in these applications.

Both EEPROMs have a guaranteed minimum endurance of one million erase/write cycles - the highest in the world. This is made possible by a unique memory cell design in which the conventional arrangement of vertically stacked gates is replaced by a lateral structure that minimises the thermal stress on the critical tunnel oxide during subsequent processing. In addition, every cell has a built-in redundancy that prevents random weak cells from compromising the integrity of the device.

Other key features include a data retention of more than 10 years, page write mode and self-timed programming cycle, enhanced ESD and latch up performance (with ESD protection to 4000V) and single supply operation. The supply voltage range runs from 3V to 5.5V, allowing the devices to operate from batteries or unstabilised power sources. The devices are supplied in die or micromodule form.

Unlike conventional EEPROM processes, only one polysilicon level is used and this process simplification leads to lower cost and higher reliability.

Contact: Maria Grazia Prestini, SGS-Thomson Microelectronics, Agrate, Italy - Tel: +39 39 6355 021. Fax: +39 39 6035 700.

Nevers City Card Demonstration

Representatives of 2000 local authorities were given a demonstration of Smart Card technology in the French town of Nevers recently.

Major GSM Launch in the US

Ameritech has become the first major US telecoms operator to enter the GSM (Global System for Mobile Communications) sector in the United States with the launch of its Cellular International

The GLOBULL CP8 card is used by schoolchildren to order their school meals every morning so that the kitchens can operate at maximum efficiency, and charging can be managed without the students having to carry and handle cash or tokens.

The management system for the town's school and extra-curriculum facilities has been produced jointly by Maelis and Bull CP8.

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

Card Europe Working Groups

Card Europe has set up four Working Groups to study areas of interest to members - contact and contactless Smart Card convergence, the use of Smart Cards in education, the role of Smart Cards in the home services marketplace, and user perceptions and requirements as inputs to the standards making process.

A local chapter has been established in the UK and has met under the chairmanship of David Greer, the Information Services Manager of Birmingham Training and Enterprise Council.

It is also planned to start up local chapters in Spain and Ireland before the Autumn, and to follow this with at least three more country chapters before the end of the year.

All members will be linked through the Card Europe Information Centre which is an on-line service accessible through a local connection in all European countries.

Liaisons have been formed with other associations, including the US Smart Card Forum and RTI Focus, the UK representative body for the transport industry.

Contact: Alan Liebert. Card Europe - Tel: +44 (0)923 897477. Fax: +44 (0)923 897414.

Network.

The service enables Ameritech's customers to take advantage of the pan-European digital GSM phone network when travelling in Europe, with billing back to base, and opens up a potentially large telecom market segment.

The contract for the supply of Smart SIM (Subscriber Identity Module) cards has been awarded to Schlumberger Smart Cards & Systems and follows Ameritech's partnership with European GSM operator, NetCom, also supplied with SIM cards by Schlumberger.

Compliant with ETSI/GSM standards, the SIM cards provide PIN code verification for customer identification, and employ sophisticated encryption algorithms for "active" second-level identification before granting access to a network.

The cards also meet the emergent TE9 European standard, providing operators with an open system that enables GSM functions to be combined with other telecom or banking applications as they become available. The cards are available with up to 8K bytes of EEPROM for storing user data (Ameritech's have 3K bytes), and are easily and securely programmable by the operator using Schlumberger's SIMflex software.

Ground-braking application

Richard Peck, Telecom Products Marketing Manager, Schlumberger, said: "We are particularly pleased to win this order because Ameritech's ground-breaking application provides a showcase for the advantages of Smart Card-based subscriber identity modules to the American audience at a time when crucial decisions are being made about the shape of the country's future telecom networks.

"We view Ameritech's decision as a step towards establishing this vital new technology in the North American telecom market."

The service has been launched to corporate customers in the Great Lakes region the operator serves - Illinois, Michigan, St. Louis Missouri, Ohio and Wisconsin.

Contacts: Bertrand Dussauge, Communications Manager, Schlumberger Smart Cards & Systems, France - Tel: +33 1 47 46 62 47. Fax: +33 1 47 46 68 66. Richard Peck, Telecom Products Marketing Manager, Schlumberger Smart Cards & Systems, USA - Tel: +1 804 366 4177. Fax: +1 804 424 2236.

Innovatron Record Sales

French company Innovatron Ingenierie reports record sales of 200,000 microprocessor cards and 2,000 terminals to the former Soviet Union in the first half of 1994.

In June the company signed five new contracts for electronic purse systems in Moldavia (Dekart and Eolis), in Ukraine (Donuglekombank and Inko Bank) and in Latvia (TCS Riga). The new schemes represent 42,000 E3744 microprocessor cards from Solaic and 300 TPSCAM 1000 terminals designed and manufactured by Innovatron.

Innovatron Ingenierie has two other electronic purse schemes under development. One is for Moscow's Tveruniversal Bank which ordered 500 TPSCAM 1000 terminals (300 of which are being assembled in Russia for the first time).

The second project has been commissioned by the Siberian Commercial Bank which started with 15 terminals and 1,000 cards in September 1993 and has now ordered a further 600 terminals and 50,000 cards.

Innovatron Ingenierie is widening its Smart Card range with two new microprocessor cards. One has 1K bytes EEPROM and 3K bytes of ROM, and the other has 3K bytes EEPROM and 6K bytes of ROM. In addition, the company is now offering Automatic Teller Machines (ATMs) and is considering the local manufacturing of terminals by the end of this year.

Contact: Genevieve Boeuf, Communication Manager, Innovatron Ingenierie, France - Tel: +33 1 40 13 39 42. Fax: +33 1 40 13 39 59.

Petrol Card in Czech Republic

The first payment system in the Czech Republic using reloadable Smart Cards is being installed at 36 filling stations and is scheduled for completion at the end of 1994 when it is expected that about 2,000 cards will be in use.

Designed and developed by SEC-COM, a manufacturer and system integrator in the field of ID card applications, the system is being implemented for KAME petrol stations in the eastern part of the country.

The system

The system consists of EFTPOS terminals connected to computerised cash registers made by SEC-COM, Gemplus GPM896 protected memory reloadable cards, a central card management system from SEC-COM, and KAME's transaction accounting system.

Each terminal consists of a master terminal operated by the petrol station staff and connected to a computerised cash register and a customer slave terminal sitting on the customer side of the counter. The slave terminal has a contact Smart Card reader, display and keypad.

Customers who wish to use the card service fill in an application form at any of the petrol stations for processing in the administration office. Pre-initialized cards are sent in a sealed envelope from SEC-COM to the administration office with the card number printed on the envelope and forwarded to the petrol station where the application was made.

A PIN is defined by the customer when the card is first inserted in the terminal. Customer cards can be reloaded with value at each petrol station by depositing a corresponding sum in cash. The sum is entered on the master terminal keypad and confirmed by the customer. The amount is then credited to the card and a receipt is printed.

To make a payment with the card the customer inserts the card into the Smart Card reader in the slave terminal and enters his or her PIN. The card balance is displayed and the cashier enters the payment value. After the customer confirms the value, the amount is debited from the card and the transaction is stored in the terminal memory. Each cashier has a merchant card which is used at the beginning of each shift to activate the terminal. At the end of the shift the total receipts are printed out and sent to the cash register for later transfer to the administration office for processing. The transfer of transaction data (not only cashless) is made daily on diskettes.

Crypta Plus Card

Centennial Technologies Inc. has announced the signing of a license agreement with Telequip Corporation to manufacture and market a PCMCIA (Personal Computer Memory Card International Association) Flash Memory Card with a built-in

Contact: Miroslav Ohnut, SEC-COM, Zlin, Czech Republic - Tel: +42 67 520219. Fax: +42 67 520239.

PREMID Toll System for France

AREA, Societe des Autoroutes Rhone Alpes, in France, is to install Combitech Traffic Systems' PREMID 3100 electronic toll collection system using Smart tags on its entire network.

The system will be installed by Grenobloise d'Electronique et d'Automatisme (GEA), of Grenoble, starting in Autumn 1994. When fully operational in mid-1995, the system will comprise some 115 automatic vehicle identification (AVI) lanes covering highways A41, A43, A48, A49 and A430 which range from Lyon-Chambery-Annecy and extend to Albertville and Grenoble in south-east France.

It is calculated that at least 45,000 tags will be issued as all current pre-paid magnetic cards will be exchanged for AVI tags.

The decision to use the PREMID system follows two years of practical experience with 20 lanes and more than 8,000 tags in an open system with PREMID 31000 integrated with coin machines delivered by CSEE Peage. The overall error rate is reported to be less that five per 100,000 transactions.

Contact: Claes Claeson, Combitech Traffic Systems, Sweden - Tel: +46 36 19 43 84. Fax: +46 36 19 43 01.

Quantum Team Move

The British Gas Quantum System team have moved to the following address: British Gas plc, The Quantum System, Blaydon Office, Derwenthaugh Road, Swalwell, Newcastle-upon-Tyne, NE16 3BQ. Tel: +44 (0)91 414 7011.

Smart Card integrated circuit which performs security, identification and authentication functions.

Called the Crypta Plus Card, it can be used as a secure token for mobile and desktop computer users to protect data and applications, and allows for communicating data securely over wired or wireless networks. In addition, the card ensures data integrity and performs the private key operations used in data encryption and digital signatures and should be of interest to the financial industry as a means to identify and authenticate parties to a financial transaction.

Support for new RSA standard

Card resident software will support the new RSA PKCS #11 standard (anticipated to be the first published standard for the use of public key cryptography with tokens and Smart Cards), as well as secure data interchange using existing encryption standards including DES, DSS, PKCS and RSA.

Jack McDonald, Vice President of Sales, says: "We are very excited about taking this product to market. We see a real need for a cost effective, reliable solution to protect data and communications as computer, communications, and home entertainment technologies and services begin to merge. The cards are available now and our immediate marketing focus will be on point of sale applications."

Crypta Plus Cards can be custom ordered with 2 to 16M bytes of non-volatile Flash memory, utilising both word-wide and byte-wide transfer modes. The Crypta Plus consists of five major elements - card interface logic, attribute memory, Flash memory array, memory lock logic and Cryptographic Support Processor (CSP).

The primary functions of the CSP are to provide secure control of secret passwords and encryption keys and to provide support functions operating on these data elements in a secure environment. The software resident on the CSP supports security functions using protocols which enable passwords and keys to never leave the chip once they are stored. The CSP module conforms to Level 3 of the US Federal Information Processing Standards Publication 140-1, "Security Requirements for Cryptographic Modules."

Security features provided by the CSP:

* Secure storage of keys and passwords.

* Memory Lock Logic prevents users from accessing data stored in the Flash until the Crypta Plus Card is "unlocked" with a random-number password.

* Passwords stored in CSP can be changed, but not read, by host resident software.

* Provides for other password options such as a "handshake" mode where host and stored passwords must match.

* Secure key and password storage in the Flash memory.

* Secure remote log-on using single key encryption.

* Public Key encryption, developed for public data exchange.

* Digital signature verify both the integrity of the data and identity of the sender.

* Can be partitioned into "read-only" and "read-write" sections.

* Automatic password expiration.

Telequip Corporation is an industry leader in electronic money handling and secure communications equipment while Centennial designs, manufactures and markets PCMCIA PC cards and solutions for use in portable computers and industrial applications.

Contact: Jack McDonald, VP of Sales, Centennial Technologies Inc. - USA - Tel: +1 508 670 0646
Fax: +1 508 670 9025.

High Volume ID Card Production

A new high-volume ID Card personalisation system has been announced by the FMN Holding Group whose headquarters for systems development are in the UK and France.

The announcement comes at an opportune time following the announcement by the UK Transport Secretary that plastic credit card style driving licences with photographs are to be issued to Britain's 32 million motorists from July 1996 (see page 158), plus the on-going debate on the need for a national identity card to combat crime.

Their new system, called the SL 3720 will be on display at the major European showcase, CarteS 94, in Paris in October and is planned to be in full production later this year.

FMN say their system offers three particular advantages over other personalisation systems:

- It is extremely fast with production speeds of around 720 per hour.
- It offers a secure solution as all information is sub-surface rendering images and information virtually impossible to change or erase.
- The system can be integrated in-line with most existing card producing equipment eliminating the need to feed pre-punched cards as an "off-line" operation for personalisation.

Utilising Thermal Dye Sublimation technology, and incorporating a new multiple-head printing system, personal data and photographs can be printed directly onto a substrate, for example PVC overlay, at production speeds of around 720 per hour.

Printing at 300 dpi resolution, the device personalises material off the webb, and the subsequent reel of printed material is then cut to the required length by it's own dynamic guillotine. These strips of material may then be attached to the pre-printed core sheets, or serve as a sub-surface overlay for the face or reverse of the cards prior to conventional lamination and punching.

Acquisition of data to feed the SL 3720 may be achieved in "real time" in order to maintain continuous print, and open database connectivity is used to communicate with client applications which may include the client's own system when running gateways to other applications such as Ingres, ORACLE, Sybase, Db2, CICS, Teradata and others which may include an FMN installation incorporating capture stations.

Recognition of cards printed by the SL 3720 will be by way of a unique tag code which will be readable under a black UV light source.

FMN offer a range of data acquisition and card printing systems as well as a "bespoke" design service for clients with requirements for unique hardware or software applications, and full on-site customer support in most countries.

Contacts: Nicholas Kingsley, International Operations Manager, FMN, UK - Tel: +44 (0)462 420922. Fax: +44 (0)462 420944. Thierry Lormiere, FMN, France - Tel: +33 93 32 05 47. Fax: +33 93 32 09 17.

CFC-free Cards from Mitsubishi

Mitsubishi Electric report that ozone depleting substances such as CFCs have been eliminated from IC memory card production at their Tajima Factory in Japan by introducing new and alternative manufacturing methods.

In 1990, the company says it eliminated CFCs from it's IC card assembly processes, and 1.1.1. trichloroethane (TCA: methyl chloroform) from the same lines in May last year. New cleaning liquids have been developed to remove rosin residues from printed circuit boards during assembly and manufacturing as an alternative to CFCs and TCAs.

These moves are in advance of the Montreal Protocol call for the phasing out of ozone depleting substances by the end of 1995, and obviates the need under the US 1990 Clean Air Act to label products manufactured using ozone depleting substances from May this year.

Contact: Christine Warren, Mitsubishi Electric UK - Tel: +44 (0)707 276100.

Satellite TV Service

DirecTv, the new direct broadcast satellite service in North America said to have a potential subscriber base of 50 million viewers, could become one of the largest single applications for Smart Cards, likely to be surpassed only by Smart national identity card schemes.

Launched in June this year, the service has been described as the most spectacular leap in television entertainment since the advent of colour TV. Two high-power Direct Broadcast Satellites (DBS) will deliver approximately 175 television channels with picture quality comparable to a video laser disc, and sound that rivals an audio compact disc.

Programming will be delivered by DirecTv, a unit of GM Hughes Electronics, and USSB (United States Satellite Broadcasting Co.), a division of Hubbard Broadcasting.

The new DSS (Digital Satellite System) consists of a compact 18-inch satellite dish, dedicated digital receiver and interactive remote control, with a suggested retail price of $699.

Programming includes every major basic and multi-channel premium television network as well as first-run pay-per-view films direct from major Hollywood studies, sporting events, specialty programmes, free channels and public service and educational broadcasts.

Programming flexible

DSS programming is structured to be flexible so customers pay for the programming they want and have more control over the amount they spend for television. Film fans will be able to watch the most popular films any time by choosing from the 40-50 pay-per-view channels offering hit movies starting as often as every 30 minutes, or from multi-channel premium services. There will be more than 50 of the most popular subscription channels plus specialty programming for viewers with special interests.

DSS also features an innovative parental control system that allows owners to lock out specific channels, establish rating limits and control pay-per-view spending.

Thomson Consumer Electronics, headquartered in Indianapolis, Indiana, is the developer of the system's digital compression technology which allows multiple video signals to be transmitted through a single satellite channel, and is supplyng satellite receiving antennae and set-top decoder boxes for the DirecTv entertainment and information delivery system.

The company is also the initial DSS supplier under its RCA brand name. Under the terms of the contract, Thomson has an exclusive agreement to manufacture the satellite dishes and set-top terminals for 18 months, or until one million units are sold. After that, other companies can begin producing the equipment under specific licensing agreements from Thomson.

News Datacom, based in the UK and a subsidiary of The News Corporation, provides the conditional access and encryption system. The company specialises in advanced data security and is one of the world's leading providers of conditional access systems.

Access to programming will be controlled by their Smart Card-based security technology. With Thomson News Datacom jointly developed the VideoCrypt system for pay-TV scrambling and security which is used by British Sky Broadcasting in the UK and about a dozen more major pay-TV services around the world.

First application

This is the first application of News Datacom's established conditional access control Smart Card technology to compressed digital television.

The Smart Cards are being supplied by US3, the biggest Smart Card manufacturer in the United States, who also supply BSkyB which has a subscriber base of over 3.5 million.

The security and replaceability of Smart Cards allow frequent opportunities to introduce new business features and protect against obsolescence through the incorporation of advancements in Smart Card technology.

Contacts: Linda Brill, DirecTv, USA - Tel: +1 310 535 5062. Steve Blum, USSB, USA - Tel: +1 612 642 4666.

Canal Control by Card in Ireland

A Smart Card-based control system for operating canal locks, paying for public mooring facilities and other services has been installed on the Shannon-Erne Waterway in Ireland in a £30 million scheme funded by the European Commission.

The installation has been carried out by Irish company PCAS - Process Control and Automation Systems (E.D.) Ltd.

A 55 kilometres canal links the Shannon River in Southern Ireland to Lough Erne in Northern Ireland and has been used by over 1,300 boats in the first seven months of this year.

Lock control system

The system controls 16 locks on the canal and each lock has the following equipment:

- A programmable logic controller (PLC)
- Three water level sensors (upstream, downstream and in the lock)
- Four sets of boat sensors (upstream and downstream sides of both lock gates)
- An alarm to warn boats if they are obstructing moving lock gates
- Two sets of red and green traffic lights (upstream and downstream sides of the lock)
- A radio system to call patrol vehicles if assistance is required.
- A Smart Card reader unit and reader head
- A hydraulic power unit and valve block
- Eight hydraulic cylinders: 2 lock gates and 2 sluice gates at the upstream and downstream side of the lock.
- A push-button console with buzzer acknowledgement.

The equipment for the system is housed in two stainless steel enclosures located at the side of each Counters are installed in the control system enclosure to register the number of usages of the sewage pump-out and chemical toilet disposal facilities for the local authorities.

Cardholders can check the number of units remaining on the card at reader units with liquid crystal displays located in the laundry rooms.

There are a further six sewage pump-out units for boats on Lough Erne. These used to be manually operated but are now driven by a diesel engine and are operated with the same Smart Cards as used on lock and the user performs lock operations by pressing the appropriate buttons on a stainless steel console which is mounted on a pedestal at the side of each lock.

User operation

Access to lock operations is controlled by a Smart Card. When a user inserts a card into the Omron Smart Card reader it checks to ensure that there are sufficient units remaining on the card and deducts the amount required (currently one unit) and sends a signal to the PLC which starts the hydraulic power unit and allows the user to pass his boat through the lock by pressing the appropriate buttons on the console to adjust the water level and move the lock gates.

The Smart Cards from Gemplus in France are of the same design as Telecom Eireann Call Cards and are available in 10 and 20 units They are available from the patrollers on the waterway, boat hire companies and local shops.

Public mooring facilities

Six mooring locations are available to the public and the system controls access to showers, chemical toilet disposal and laundry rooms. It also controls the operation of a washing machine and tumble dryer in the laundry room and a sewage pump-out for boats on the mooring.

A PLC is used to control the facilities. The same Smart Card readers and cards as those used for the locks are used to gain access to the facilities and operate the equipment. Different charges are levied for each facility, for example, two units are required for a shower and no units are needed to enter the laundry room.

the Shannon-Erne waterway.

PCAS, based in Carlow, 80 kilometres from Dublin, began trading in 1976 initially in the area of electromechanical systems but has migrated into programmable control systems, supervisory systems and plant automation. Its expertise includes the monitoring and remote control of hydroelectric stations. The Shannon-Erne waterway project is their first application using Smart Card technology.

Contact: Michael Tracey, PCAS, Ireland - Tel: +353 503 42377. Fax: +353 503 42620.

Smart Card Privacy Issues

Concerns about the privacy issues in Smart Card applications, particularly access to personal data, have been voiced in the UK and Canada.

Eric Howe, the Data Protection Registrar in his tenth report to the British Parliament, says Smart Cards have data protection privacy implications in respect of who shall have access to the personal data on them and who shall have the ability to read, add to or alter those data.

Smart Cards have many possible uses in both the public and private sectors. These include their use for payment purposes, perhaps with facilities which create an "electronic purse," for the prevention of credit card fraud, and for holding details of medical conditions and treatment.

In Canada, Tom Wright, Ontario's Information and Privacy Commissioner has reported on the implications of the use of card technology by government and says such systems should be open and transparent to data subjects who should know their inherent rights when using the card, what information the card contains, how it will be used, and what risks that use implies.

Cardholders should have the right to:

* participate in the determination of what personal information the card contains and who has access to it.

* access and correct information held about them on the card, as well as in any related database.

All uses and disclosures of information on the card should be subject to the prior and informed consent of the data subject.

Where possible, individuals should be free to refuse the card without jeopardising their access to the service involved. Similarly, holding a Smart Card should not confer benefits (other than perhaps enhanced service) unavailable to those who choose not to utilise a Smart Card, he says, adding that Smart Card technology should only be used by government to enhance access to government information and services and not as an instrument of social control, for example, as a method of conducting surveillance or a means of creating computer profiles.

On security he says: "The full measure of security available through the technology should be used to prevent misuse or inadvertent access. This should include the use of PINs, authentication protocols, encryption, and the segregation of multi-use applications to prevent possible merging or matching of various databases. The use of Smart Cards to conduct computer matches or linkages should be restricted."

He calls for "privacy impact" statements to be prepared and issued prior to the approval of new or revised Smart Card applications.

In his report to Parliament, Mr Howe also warns that the issue of a national identification system is too fundamental for the UK to allow itself simply to slip into having a de facto national identification system.

If pressures continue for a system, he says, there should be a careful evaluation of any benefits which might flow from it and a weighing of these against the undoubted risks to privacy and personal freedom.

"The argument, which is sometimes produced, that the innocent have nothing to fear, may have emotional appeal, but adds little of substance to the debate," he says.

He felt that none of the four publicly created identification systems - the planned driving licence with a photograph, the proposed social security "swipe card", the National Insurance Number, and the new National Health Service Number - is adequately protected against forming the basis of a de facto national identification system.

"A de facto system could therefore develop with no proper analysis of the advantages and disadvantages of such a system, without effective debate in Parliament and without proper statutory controls."

Contact: Eric Howe, Data Protection Registrar, UK - Tel: +44 (0)625 535711. Fax: +44 (0)625 524510

Plan to Track Vehicles

A call for all vehicles to carry electronic ID cards to enable police to monitor the movement of Britain's 30 million motorists has been made by an all-party Commons Transport Committee which also warned that motorway tolls based on similar technology would be neither desirable nor workable without far more Government research.

The findings are a blow to the Government's plans to introduce a nationwide network of tolls using Smart Card technology within five years.

The Committee, chaired by former Tory transport chairman Paul Channon, said research showed tolls would divert huge amounts of motorway traffic on to nearby local roads, resulting in an environmental nightmare for local residents and causing as many as 2,800 additional injury-accidents per year.

Tolls would be a highly visible new charge which even at relatively low levels could have a high annoyance factor, said the Committee.

However, the government has announced its intention to introduce electronic tolling on motorways when the necessary legislation is in place and the technology is ready. Detailed testing and evaluation of two or three complete systems are scheduled to start early in 1995.

Transport Secretary Brian Mawhinney, said the government would examine with care the arguments and proposals made by the Committee and added: "Without improvements, the diversion of traffic which worries the Committee will happen spontaneously."

Lukewarm about Smart Cards

The Committee was lukewarm about Smart Card technology for tolling describing it as the "least disadvantageous approach." (Smart Card News interprets this government gobbledegook as meaning the "most advantageous approach.")

The report was more excited about the idea when coupled with a vehicle-mounted ID device. An "electronic tag", fixed by law to all vehicles, would give police an effective new tool in the fight against crime and terrorism.
In addition it could be used to store details of payments for road tax, parking tickets, speeding fines and motorway tolls.

The proposal for "Smart Number Plates," has provoked criticism from civil liberty groups who are concerned about the lack of controls for this kind of information, how it could be used and who would have access to it.

Avi-BoKS Security for PCs

AU-System Communication AB, of Sweden, are offering a Smart Card-based security system for Personal Computers based on the Swedish government's "Allterminal" security specifications.

Called Avi-BoKS, it is designed for standalone PCs and PCs in Local Area Networks (LANs), terminal emulation to host computers and client/server environments, and is also suitable for portable computers (laptops, notebooks, etc.).

The system, currently being piloted in several large organisations, provides protection against:

* unauthorised use of the computer

* unauthorised access to information locally
A card reader is connected to each PC, either built-in or external. All the user has to remember is the card's password as the system is transparent to the user with all other procedures, including log-ons, handled by the card in interaction with the local access control system.

If the card is withdrawn from the card reader while work is in progress, work is stopped. The same happens if there is a pre-determined period of inactivity on the part of the user, to provide protection if the computer is left with the card in place.

PC protection

Local PC protection embraces access control for protection against unauthorised access to programs and data files, automatic encryption of information written to the hard disk or floppy making information on the hard disk inaccessible even if the PC is stolen, detection of changes in programs, and boot protection. (If booted from a floppy the information the hard disk will be inaccessible.)

User identification

User identification is carried out in connection with log-on to a target computer (host or file server) through co-operation between the Smart card, an authentication module in the PC, and a corresponding module in the target computer. The target computer emits a random number which the

and centrally

* access to information if the PC is stolen

* monitoring of LANs and remote connections

* virus infiltration and other unauthorised changes in program codes or data files.

Smart Card

The Smart Card used in the system is the DX 2K bytes EEPROM card with 6K bytes of ROM from TRT Philips, Smart Cards & Systems, France.

Each card is unique and its contents cannot be changed. The card's microprocessor performs encryption calculations and the user's secret keys are stored in the memory.

Smart Card encrypts with its unique secret RSA key and the result is sent back to the target computer for checking.

Digital signature

An optional module for digital signatures makes it possible to check:

* that a document has not been changed
* the identity of the person who signed the document.

Digital signatures can be used for electronic mail, Electronic Data Interchange (EDI) etc. The module utilises data and functions in the Smart Card for key handling.

Encryption of data communication

To provide protection against unauthorised monitoring of a LAN or a remote connection, an optional module is available to encrypt all communication with the target computer.

Technical specification

Smart Card

Philips DX, 6K bytes ROM, 2K bytes EEPROM
Complies with ISO 7816-1/2/3
Calculator unit for RSA
Storage of user identity in conformity with X.509

(ISO 9594-8)

Card Reader

Philips PE112, Gemplus GCR200, or Schlumberger SCR60

Protection

Local access control system for administrators, users and guests

Encryption of files with KA-26 algorithm

Boot protection prevents accessing hard disk on system boot-up from floppy

Configurable logging function

Authentication

Strong unilateral authentication in conformity with ISO 9798-3

Line encryption

Exchange of session key with RSA

Encryption with DES or KA-26

Digital signatures

Based on ISO 9796 and PEM (RFC 1421-1424)

System requirements

Computer with Intel 80386 processor or higher
Hard disk with at least 1 Mb free
DOS 6.0 or later. Windows 3.1 or later.

Contact: Hans Nilsson, AU-System, Sweden - Tel: +46 8 726 7500. Fax: +46 8 19 33 22.

Smart Card Diary

ESCAT 1994 (European Smart Card Applications & Technology), Hotel Inter-Continental, Helsinki, Finland, 7-9 September.

Three days of Smart Card applications and user experiences from international speakers from ten countries. Contact: Congrex, Finland - Tel: +358-0-752 3611. Fax: +358-0-752 0899.

Paycard '94, The Gloucester Hotel, London, England, 19/20 September.

Topics include Europay International on the business case for the introduction of chip-based POS payment systems and BT on exploiting chip card technology in telephony, as well as loyalty schemes, fraud reduction and co-branding opportunities for retailers. Contact: IIR - Tel:+44 (0)71 412 0141. Fax:+44 (0)71 412 0145.

Profit from the Payment Card Business, Forte Crest Bloomsbury Hotel, London, 26/27 September.

Focuses on current market status and making the business more profitable, development of the electronic purse and some of the major applications for Smart Card technology. Contact: IBC Financial Focus - Tel: +44 (0)71 637 4383. Fax: +44 (0)71 323 4298.

CarteS 94, Palais des Congres, Paris, France, 18-20 October.

The 9th international forum for plastic cards technologies with plenary conferences on Smart Cards in the fields of payment, security, information management, commerce and technology, electronic payment systems; one-day forums on Cards and Local Authorities and Health Care Cards; and half-day seminars on Card and Law, Cards and Telecommunications,

Technocard, Stored Value Ticketing, Components 2000 and Cards and Security. There is also a major exhibition with over 100 exhibitors. Contacts: Joelle Catalano (Congress) - Tel:+33 1 49 68 52 60. Gilles Benay (Exhibitors) - Tel:+33 1 49 68 52 84.

European Payments 94 (EFTP0S & Home Services), Sheraton Grand Hotel, Edinburgh, Scotland, 14-17 November.

Celebrating its 10th anniversary, the conference aims to provide an in-depth review of financial payment systems throughout the world. Contact: Scottish Electronics Technology Group - Tel: +44 (0)41 553 1930. Fax: +44 (0)41 552 0511.

Global Smart Cards 1994: Exploiting The Commercial Opportunities, The Mount Royal Hotel, London, 23/24 November.

The conference will highlight the major benefits that have accrued to organisations from around the world that have pursued innovative Smart Card systems and look at the lessons that can be learnt from their experiences. Organised in association with Smart Card News and The Smart Card Club. Contact: AIC Conferences - Tel: +44 (0)71 827 5964. Fax: +44 (0)71 329 4442.

CardTech/SecurTech '94 West, Westin Hotel, Santa Clara Convention Center, California, USA, 30 November/1 December.

Conference designed to augment the larger East show held each Spring, will provide a general session on major industry trends followed by two tracks - the developers track focusing on technical issues associated with integration of advanced card and security technology into hardware and software systems, and the applications track looking at the business justifications and strategies. There will be over 40 booths in the associated exhibition. Contact: CTST - Tel: +1 301 881 3383. Fax: +1 301 881 2430.

Smart Card Europe, Royal Lancaster Hotel, London, 13/14 December.

The 2nd annual European conference focuses on the security issues, particularly regarding electronic purse schemes, and examines the major applications in the rapidly developing fields of transport and telecommunications. New to the conference is a tutorial on 12 December by Dr David Everett for those who want to get up to speed on Smart Card technology. Contact: IBC Technical Services - Tel: +44 (0)71 637 4383. Fax: +44 (0)71 631 3214.

Smart Card Tutorial-Part 24

Multi-application cards continued:

Now the time has come to try and put everything together. We are going to invent a hypothetical multi-application card by which means we can examine the various technical and security issues that arise in practice. No attempt will be made here to justify the business case that may result in such a card being produced. In fact as we mentioned previously the commercial issues that surround the development of multi-application cards are complex. This includes not only branding issues but also the fundamental concerns surrounding liability and ownership and therefore the responsibilities of the various parties.

The structure of our card is shown fig. 1. The card contains an operating system in the ROM memory of the chip and three applications to be installed in the EEPROM memory. The applications have been deliberately chosen to be commercially independent with totally different business requirements. Lets examine the functionality of each of these applications.

The electronic purse application is provided by a bank and consists of a value store and a cryptographic protocol by which means payment can be made from the purse. We will assume that this protocol is based on the use of the RSA digital signature. The application will involve a number of commands issued to the card by the terminal that will invoke the necessary responses.

The building access application is designed to invoke a card holder authentication process by using a PIN and a signed response from the card to confirm the users identity. This involves the terminal challenging the card by a cryptographic process in this case using the DES algorithm.

The retailer loyalty scheme involves two processes, one that identifies the card holder and another function that stores loyalty points on the card that may be used at the relevant time to receive the appropriate award.

The mechanism for each of these applications is shown in fig. 2. They are shown in a very simplified format just to illustrate the principles underling the security architecture. In all cases we have assumed the availability of a security module in the terminal that can offer adequate protection for the keys and is capable of invoking necessary commands to the application in the card. In each of the applications described here a challenge/response mechanism is used with the appropriate random number or sequence number to prevent message replays. The necessary security services of authentication and data integrity are achieved by means of the cryptographic signature mechanisms.

The electronic purse application uses an RSA digital signature scheme where each card has a unique public key/secret key pair. The initial interaction with the terminal requires the exchange of public key certificates which have been generated by some higher authority or global key centre. In order to check these key certificates it is necessary to store an authentic version of the public key of this global key centre along with the relevant public key/ secret key pair and the necessary public key certificate.

The building access application is assumed to operate using the DES algorithm and has a derived key per card. This key is derived from a master key using the ID of the card.

The retailer loyalty scheme is also assumed to use the DES algorithm for protecting the points scheme but additionally has a file access key to prevent the users ID being read by a unauthorised agency. A derived unique key per card has been used based on the users ID and a points master key.

Now let us look at how we can initialise the card to operate with these three applications. We have stated previously that the applications should maintain their own security which means that not only must each application support its own key management structure but that the operating system must ensure the necessary security segregation. Let us derive the necessary security requirements for the IC card,

1) The application must be able to trust the operating system
2) The operating system must be able to trust the applications.
3) Application security segregation must be assured
4) The cryptographic keys must be loaded securely

We can look at each of these motherhood statements to see what they mean in practice. The electronic purse scheme poses the greatest security requirement and clearly the provider of this application in particular needs to be assured that the operating system will protect the total working environment. It is likely that the operating system will be developed to the specification of the purse provider and will be subject to his certification process. Part of the purse application installation process will involve adequate steps to ensure the authenticity of the operating system. This may be achieved by procedural processes but is more likely to involve code authentication processes as well. We may also assume that in practice the cryptographic algorithms will be implemented in the ROM memory occupied by the operating systems. This is the most efficient use of memory space and allows the algorithms to be shared by the various applications.

However we have now run into our first problem, what is the process by which all the application providers can be adequately assured of the integrity of the operating system? If one of the providers is predominately responsible for the integrity of the operating system what is his liability to the other application providers in the event of a security flaw? The second requirement is necessary for the operating system to be able to ensure the necessary security segregation. We have previously mentioned various methods by which this can be enforced either by the hardware addressing structure of the chip or by the use of software interpreters. Conceptually the security segregation can also be achieved by certifying trusted applications and then checking the authenticity of the application when it is loaded by the operating system. For example the application could be signed using some digital signature function which is checked by the operating system The application security segregation is totally dependent on the approach adopted to achieve the multi-application architecture. If the approach adopted is based on the operating system only loading certified application modules then additional procedures are necessary to ensure that such applications do not stray outside of their authorised boundaries. In practice this involves validation and verification of the software code modules and is very difficult to achieve even for relatively small applications. Enforced segregation by hardware logic in the chip or the interpreter approach is lightly to be far more effective and means that there is no need for the parties to certify individual applications. Clearly this is the easiest approach to pursue commercially.

The forth requirement relates to the difficulty of loading the cryptographic keys in a secure fashion. In any security system the installation of cryptographic keys is always a difficult practical problem. There is an additional problem with Smart Card applications that relates to the volume of cards that need to be initialised with the security keys. In many cases this is likely to be measured in millions. Whilst it is possible in principle to develop procedures by which such keys can be managed in practice most designers would base their architecture on the use of a key transport key. This key will need to be installed in the IC card in an early stage in the card life cycle. The various application cryptographic keys may be protected by this key to enable the key initialization process to be optimised with simpler procedure operations.

We have now created a new problem in that we have invented two new keys that need to be generated, operated and destroyed in a secure fashion. The

before the application is loaded. It should be noted that this requires an additional key to be installed in the IC to check such signatures.

application authentication key and the key transport key both relate to all the applications. The question that arises relates to who is in charge of these keys? Any compromise of these keys would effect all the applications equally. There are many different solutions to this problem but at the end of the day all the application providers will need to accept the common security process by which such keys are managed.

The purpose of this discussion was not to dismiss the concept of multi-application cards but just to point out the difficulties that need to be over come to make such cards commercially viable. There are solutions to all the problems described here but such solutions are very dependent on the business requirements established by the operators of the various card applications. The question of branding is entirely a commercial issue and one for which the solution may be the most elusive of all.

David B Everett
Next month - Contactless cards

UK Photo-Card Driving Licence

Plans to introduce a plastic credit card style driving licence with photo identification for Britain's 32 million motorists have been announced by Transport Secretary Dr Brian Macwhinney.

In the longer term, the card could be adapted to become a Smart Card licence by the addition of a microchip with the possibility of including details of endorsements and help police enforce the law and discourage banned drivers, details on whether the driver wished to be an organ donor, contain emergency medical information such blood type and allergies, and possibly the driver's national insurance details.

Opposition

The Department of Transport, already facing opposition from civil liberty campaigners who oppose photographs on the licence and fear the introduction of a national identity card, are playing down the logical progression to a Smart Card.

Instead they are emphasising that it would be more convenient to carry, prevent driving test fraud by making it more difficult for the estimated 1,000 people a year who pass their driving test by getting someone else to take it for them. A photograph on the card would also hit black market sales of forged and stolen licenses.

The Department denies that photo-cards are the first step to a national ID card and say it will not be compulsory for drivers to carry them at all times.

Britain is one of the few countries that does not include a photograph on the driving license. Recent market research from the Driving and Vehicle Licensing Agency has shown that 72% of drivers interviewed preferred the proposed plastic card with a photograph to the present paper one.

July 1996 start

It is planned to introduce the scheme from July 1996 well ahead of the European Union law requirement for photographs on driving licenses by the year 2001.

First to receive the new licenses will be provisional licence applicants. Licence will be renewed within 10 years to keep photographs up-to-date.

Card Hack Attack Fails

Compared with the high security of microprocessor Smart Cards, the magnetic stripe card has long been recognised as insecure and an attractive target for forgers and counterfeiters, but would-be fraudsters came unstuck when they launched a massive hack attack on the New York Metropolitan Transit Authority's fare card.

According to the "New Scientist," a gathering of more than a thousand of the world's brightest hackers and phone phreakers in the city decided to demonstrate their technical prowess by cracking the subway fare card.

Although the group included hackers who have illegally accessed secret government computers around the world, the onslaught failed.

Mingling with the hackers were undercover government agents quietly gathering intelligence on the activities of the hackers.

The plastic fare card is slightly thinner than a credit card and is used to buy several rides in advance. Information on how much credit is left on the card is encoded on a magnetic stripe.

The hacker geniuses could not work out precisely how the information is encoded or find a way to alter the credit recorded on the stripe, at least not without using technology that would cost more than they could save by cheating the subway authority of its $1.25 fare.

One disappointed hacker advised: "If you really want to ride the subway for free, jump over the turnstile."

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.

BT Moves to Smart Payphones

British telecommunications company, BT, has placed multi-million contracts for new Smart phonecards and payphones in a major development that heralds the arrival of the Smart Card as an item of general use by the British public when the service is introduced in 1995.

Three companies, GPT, Landis & Gyr and Schlumberger will provide payphones able to accept Smart phonecards to replace the 39,000 cardphones currently in use.

The payphones will be conventional in appearance and offer a cash and card or card only payment option. Among the payphones being supplied will be two from GPT's Sapphire range - the Smart/credit card model (shown above) and the all payment model (bottom right).

Gemplus and GPT will supply the new Smart phonecards which will be pre-paid cards similar to the existing optically encoded cards and will be available in units of 20, 50, 100 and 200, costing £2, £5, £10 and £20 respectively.

The number of cards to be ordered has not been released, but quantities will be substantial as BT sells 20-25 million payphone cards a year.

The cards will be sold, as now, through the existing network of BT phonecard agents with around 50,000 outlets across the UK, comprising a wide variety of retailers, ranging from post offices and large chains such as WH Smith to small independent corner shops.

The cards will be the same size and shape as the existing BT Phonecard but BT says the design will allow more flexible and usable space for creative, customised designs and joint promotional opportunities with other companies. This means that we are likely to see company and special event promotional advertising on the cards and a dramatic growth in card collecting.

David Bell, BT Payphones' New Business Development Manager, says: "BT's existing Phonecard technology has served the company well but its future development is limited. Phonecards are, however, extremely popular with customers, Phonecard retailers and collectors.

"New technology will not only improve BT's service to customers but offer tremendous potential to make exciting new services available from BT payphones in the future."

The first new service will enable cardholders in the Mondex global electronic cash system, developed by the National Westminster Bank, to top up the value on their cards and make payments by telephone. The service is being introduced in Swindon, Wiltshire, in 1995 in a joint venture with Midland Bank and in conjunction with BT.