Russian Banks Introduce Smart Card Technology

Two banks in St Petersburg, Russia, have introduced Smart Cards, and a number of other projects are now in operation. In addition, Russia is modernising its telephone infrastructure which includes the introduction of a national GSM (Global System for Mobile Telecommunications) Network using Smart Cards as the Subscriber Identity Modules (SIMs). Ed Mattix, a spokesman for US West International which is participating in the work with Russian partners, said GSM Smart Cards in use in Russia are expected to reach "hundreds of thousands" by the year 2000.

Continued on page 203

Paying by Smart Card at an EFT Terminal manufactured by Monetel, the French subsidiary of Ascom, Switzerland.

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 16, Key Management Continued

CONTENTS

Smart Cards in Russia

Continued from page 201

In St Petersburg, the Promstroibank and the Bank of St Petersburg have issued Smart Cards to their employees for cash withdrawals and as an electronic purse. This allows staff to make cash withdrawals at the bank and to obtain services, such as paying for meals in the company restaurant using the electronic purse function.

Innovatron Ingenierie says the operating principle is simple. The terminals are connected off-line to the bank's data service responsible for managing the card (crediting the electronic purse) and the account (authorising cash withdrawals according to the individual's credit position).

Since May, the Promstroibank has distributed 1,600 cards and purchased some 15 terminals. Specialising in the manufacturing and construction industries, the bank is now studying the possibility of offering it to all its customers - companies employing 5,000 - 30,000 people.

The Bank of St Petersburg has started issuing 1,000 cards for use in about 15 terminals.

Moscow project

The Tcherkizovsky Kombinat delicatessen industrial combine in Moscow has issued Smart Cards to each of its 6,000 employees. A multi-service card, associated with an account, it will provide several different functions - cash withdrawal, monitoring of physical access and electronic purse (restaurant, catalogue sales etc).

Siberian bank

In Siberia, the Novosibirsk Bank offers business customers operating fleets of vehicles an electronic purse that can be used in affiliated service stations to make payments off-line. A single connection per day to the bank's data service makes it possible to complete the electronic funds transfer necessary for the inter-company clearing. One thousand cards were distributed and 15 terminals installed in October.

The cards used in all the projects above are 486 bytes EEPROM cards from Solaic, France.

GSM Network

Last month US West International, based in Englewood, Colorado, USA, announced the formation of a Russian joint stock company, United Telcom Far East with Russian partners DAL TELECOM International, United Telecom and VARTElecom, to implement wireless and cellular communications systems in the far east of Russia.

The company will provide GSM digital cellular telephone services in Khabarovskii Krai, Kamchatskaya Oblast and the Amurskaya Oblast, which include the major cities of Khabarovsk, Petropavlovsk-Kamchatskii and Blagoveschensk as well as a number of other important cities.

This month, US West announced in Moscow further GSM developments with the formation of another Russian joint stock company, United Telecom Ural, with partners Ural Telecom and United Telecom, to implement cellular communications systems in the Perm area of Russia. The service is expected to be available by second quarter 1994.

William J Bobb II, Vice President of US West International said: "The systems of this new enterprise will become an integral link in the Russian national GSM Network and an important next step in our participation in the modernisation of the telephone infrastructure across Russia."

Contacts: Genevieve Boeuf, Communication Manager, Innovatron Ingenierie, Paris, France - Tel: +33 1 40 13 39 50. Ed Mattix, US West International, London, England - Tel: +44 (0)71 333 8221.

Production Demo for Chinese

Sempac SA, based in Cham, Switzerland, has demonstrated its assembly line for the fully automatic manufacture of Smart Cards to the Chinese Government.

The occasion was a symposium organised by the Ministry of Electronics industry, in Beijing, last month. The company is represented in China by Barco Ltd, a Swiss/Chinese joint venture company.

Setback for London Bus Trials

London Transport's Smart Card ticketing trial in the Harrow area of the city has been postponed yet again. One of the reasons is that they have not received a sufficient number of the cards from GEC Card Technology to launch the trial.

The trial, involves 40,000 contactless Smart Cards from GEC and equipping 200 Buses operated by five companies with Smart Card readers from AES Scanpoint and Westinghouse Cubic.

When the project was first announced, the Harrow trial was scheduled for around mid-1993. This date slipped to the August Bank Holiday weekend and then to October/November. Now it has been postponed to January next year.

Roger Torode, Project Leader, London Transport, said: "We have not had an adequate supply of cards yet to get the trial going, and at the same time we are testing the card readers and have raised a number of issues with the manufacturers.

"The launch will require a publicity campaign and the run up to Christmas is not a good time for this so we are now looking at January."

John Meikle, GEC's Sales Manager said: "London Transport are currently evaluating the best way forward regarding the timing of the trial. As of today, no decision has been made regarding the launch date.

"Our manufacturing process is the first of its kind in the world, and we are still in the process of finding out the full capability and flexibility of the process."

Referring to reports that GEC Card Technology is producing a thicker contactless card for the London pilot, he commented: "The thickness of the card for London is based on the application and has been chosen by the customer for its robustness and style. GEC Card Technology will naturally supply the most suitable style of card for any particular application and have an on-going development policy to offer alternative versions for specific requirements. In fact, for the pilot scheme in London, a label is going to be used at the issuing point, which obviously has an impact on the thickness."

Contacts: Roger Torode, London Transport - Tel: +44 (0)71 918 4007. John Meikle, GEC Card Technology - Tel: +44 (0)922 616939.

Latvian Electronic Purse

The first Latvian electronic purse, known as the LATkarte and launched in the city of Ventspils in July 1993, allows users to pay for goods and services in stores equipped with payment terminals.

Each transaction is stored by the card and the terminal, and once a day, the data is collected manually from the terminal using a large-capacity memory card (512 bits). This card is then inserted into the machines at the bank to complete the clearing operations (customer's account/retailers account).

The electronic purse system in Latvia (formerly part of the USSR) was designed by Software House Riga using Innovatron Ingenierie development facilities. Innovatron supplied the cards - 25,000 from Solaic, and the 200 TPSCAM 1000 electronic payment terminals which were assembled locally.

Ventspils (population 50,000) was chosen for the launch as it is the largest port on the Baltic Sea and handles some 50% of the production of the Russian oil and chemical industry.

Importantly, it is also a cosmopolitan region with many foreign companies operating from the port and paying their employees in hard currencies. The electronic purse provides a useful vehicle to enable users to convert this foreign currency into lats or dollars.

To support the new venture, Software House Riga set up its own bank, the Union Baltic Bank, and is currently distributing a version of the Latvian electronic purse for tourists - a personalised card in the name of the bank and given without necessarily opening a bank account.

Contacts: Valdis Lokenbahs, Vice President, SWH Riga, Latvia - Tel: +371 2 751 590; Genevieve Boeuf, Communication Manager, Innovatron Ingenierie, France - Tel: +33 1 40 13 39 50.

European Standard for IEP

Parts 1 and 2 of the European standard for Intersector Electronic Purse (IEP) systems are now ready for approval and comment.

The work has been carried out by Working Group 10 (WG 10) of Technical Committee 224 (TC224) of CEN, the European Committee for Standardisation.

Part 1, Concepts and Structures, describes a general model for IEP systems, focusing on the participants, their requirements and relationships, configurations, the functionality of the system and its applicability.

Part 2, the Security Architecture, describes the detailed security architecture of IEP systems, including the use of cryptographic algorithms and the underlying assumptions concerning key management necessary to implement IEP functionality for interoperability. It also defines the assumptions and conditions necessary to implement the described security architecture.

A substantial amount of work has been done on a draft of Part 3 dealing with Data Elements and Interchanges, whereas work on the Part 4 concerning Devices has not yet started.

Ole Lachmann, Convener of WG 10, said the aim of the work on IEP standards is to ensure interoperability between prepaid Electronic Purses installed in IC cards issued by many issuers from many countries and covering the needs of service providers from all sectors.

The work on the development of the IEP standard began in WG 10 in January 1991 with 10 members from five European countries and has grown to 38 members from 12 European countries. Members are involved in most of the developments towards national and international purse systems in Europe, he said, and the exchange of views and experiences within the Group has already had a major impact on these developments.

A major factor in the progress of the work of WG 10 has been the decision of the EC Commission to fund a five-person project team to meet in three weeks session four to five times a year to produce detailed technical drafts based on instructions from WG 10.

Contact: Ole Lachmann, Convener of CEN/TC224/WG 10 - Tel: +45 31 65 13 30. Fax: +45 31 65 42 69.

Belgian Electronic Purse

Banksys, the Belgian national shared ATM and EFTPOS network, is planning to launch a Smart Card electronic purse scheme next year for the payment of low-value amounts. Following extensive research, Banksys will start a pilot project towards the end of 1994.

The intention is that the electronic purse will be used for the payment of small amounts, for example, car parking, at automatic ticket machines, for public transport, making telephone calls, and for purchases at newsagents and grocery shops where people still pay with loose change.

Banksys figures show that 203 million withdrawals and payments amounting to 536 billion francs were made at terminals in 1992.

Contact: Dominique Hautain, Banksys, Belgium - Tel: +32 2 727 6111. Fax: +32 2 727 6767.

US Navy Orders Smart Cards

Micro Card Technologies Inc (MCTI), the Dallas, Texas-based US affiliate of Bull CP8, France, is to supply Smart Cards and terminals to the United States Navy.

Automated Visual Communications Inc. chose MCTI to supply 7,000 SCOT 100 cards and 85 Bull payment terminals for the Navy recruitment centre in San Diego, California.

This payment system, tested and proven at the Navy training centre in Parris Island, South Carolina, since 1987, will be used by the 21,000 recruits that pass through the San Diego base every year.

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

Swiss Rail Travel Cards

Swiss Federal Railways has placed an order for 50,000 Bull CP8 cards for use as rail travel cards.

The rail card project has been in operation since 1 May 1993 with two types of card combining the Swiss Federal Railways Half-fare travel card facility with other services. This card, which is valid for one year and costs sFr. 150, entitles the holder to a 50% discount on all tickets of the public transport system.

Almost two million people in Switzerland (some 40% of the inhabitants over 16 years-of-age) use this card.

The Half-fare travel card is combined with the Eurocard credit card (magnetic stripe) to become the Eurocard Rail Card, and with the Swiss PTT's Postcard - a Smart Card electronic purse - to become the Postcard Rail Card.

To use the card for identification purposes on the trains, the cardholder's photograph is placed on the reverse side of the card, making them the first credit/debit cards in Switzerland with a photograph.

Rail Cards are issued and distributed by Eurocard and the Swiss PTT, licensed by the Swiss Federal Railways to issue the Half-fare travel card.

Massive boost

Since May, 1993, 25,000 cards have been purchased, 90% of them Postcard Rail Cards. A special promotion for both Rail Cards is planned for Spring, 1994, when most Half-price travel cards are supposed to be renewed.

If this trend in favour of the Postcard Rail Cards continues, it will give a massive boost to the electronic purse in Switzerland. The Swiss PTT currently has 29,500 Postcards issued in its trials in Biel/Bienne and plans to extend the scheme throughout the country in 1995. (SCN July 1993).

Contacts: Martin Enz, Marketing, Swiss Federal Railways - Tel: +41 31 680 4240; Beat Tschammen, Swiss PTT Postcard Project - Tel: +41 31 338 5445.

GSM Orders for Gemplus

Gemplus Card International, France, has obtained two new orders to supply SIM (Subscriber Identity Module) Smart Cards for GSM, the Global System for Mobile Telecommunications.

The company is supplying 10,000 SIM cards to QTEL, Qatar's public network operator, which will be the first company to introduce Smart Cards and GSM in the Gulf States.

Gemplus is also supplying 50,000 SIM cards to Turkcell, the first national operator to implement the GSM network in Turkey.

The cards in both orders are to be supplied before the end of 1993.

Contact: Bernard Morvant, Gemplus Card International, France - Tel: +33 42 32 50 26.

First Free Flow Tolling System

Saab-Scania Combitech AB, of Sweden, and its Austrian partner GESIG, have been awarded a contract for a complete free flow, non speed limiting, multi-lane debiting and enforcement tolling system in Austria.

The contract, worth 35 million Shilling (approx £2m) was commissioned by OSAG (Osterreichische Autobahnen-und Schnellstrassen-AG). It will use Smart Card technology and is the first of its kind in the world.

GESIG/Saab-Scania Combitech will start to install the toll system on the Tauern highway in autumn 1994 and first evaluations are expected early 1995 when the system comes into commercial operation. When the pilot project has been successfully completed country-wide installation will start.

The system will be based on Smart Cards, with stationary antenna and associated equipment debiting the cards inserted in "in-vehicle" units attached to windscreens.

Contact: Birgitta Alshom, Saab-Scania Combitech AB, Sweden - Tel: +46 36 19 40 00.

SWIFT Orders Smart Cards

SWIFT, the Belgium-based Society for Worldwide Interbank Financial Telecommunications, has ordered 60,000 Smart Cards and more than 3,000 CAD reader/encoders from Bull CP8 to be used to enhance security for Electronic Funds Transfer messages by its member financial institutions.

The 8K bytes EPROM Bull CP8 Smart Card will use a dedicated SWIFT algorithm. The cards are programmed by SWIFT to generate unique log-in codes for each financial institution.

When an authorised operator receives his card from his supervisor, he inserts it in a tamper-resistant Secure Card Reader that sends commands to the card and reads data from it. The operator uses the card with a PIN to log on to the network automatically. For additional security, cards can be programmed to operate with two PINs to provide dual control.

The SWIFT system is called USE (Users Security Enhancement) and is now pilot testing. It was tested with 10 users in the first phase from August to October. The second phase, which will run until the end of January 1994, involves 60 users. The equipment will be deployed to all member financial institutions during 1994, after which USE will come into mandatory operation.

Contact: Luc de Clercq, Manager SWIFT Users Security Enhancement Project, Belgium -Tel: +32 2655 3111.

New Design for Jerseycard

Jerseycard has introduced a new design for its multi-application Smart Card widely used by over 20,000 residents - about a quarter of the population - in the largest of the Channel Islands. The new look card shows the location of the Channel Islands in relation to Britain and France.

A French company, Finances et Monetiques, which signed a contract with Jerseycard earlier this year to issue pre-paid rechargeable Smart Cards to visitors arriving in the island, have now decided to use the Jerseycard network instead of setting up their own terminal and card network. This means that the card can be used immediately at over 60 terminals in more than 30 sites on the island.

The users will have money stored in the card’s electronic cash purse, and can use it to purchase gifts, meals and even pay for day excursions.

The first cards, which are GPM416 EEPROM memory cards from Gemplus Card International, France, have just been issued, and Jerseycard expect a gradual build-up of business into the 1994 tourist season.

Contact: Chris Parlett, Executive Manager, Jerseycard - Tel: +44 (0)534 37713. Fax: +44 (0)534 89665.

Smart Card Patents

Groupe Innovatron says that its Smart Card patent licensing policy will continue until the year 2000.

Between 1974 and 1979, Roland Moreno, inventor of Smart Card systems and Chairman of the Innovatron Group, filed a series of pioneer patents for which 187 licenses have been granted to date worldwide.

"Conversely to some assertions, that licensing policy will not end in 1995," says the Group in a statement issued last month. "Indeed, the group of ’selfconnector’ patents, which have been filed last, will expire, depending on the countries, between 24 January 1998 and 13 September 2000.

"Innovatron’s licensing policy will thus go on, as expected, until the year 2000."

It said that recently the German patent office decided, after a particularly long and strict examination, to grant the corresponding "selfconnector" German patent, reinforcing the scope and the validity of the group of general application patents.

Contact: Francoise Marceau, Innovatron, France - Tel: +33 1 40 13 39 00.

Galaxy Expocard Success

Galaxy Registration, Inc., of Frederick, Maryland, USA, has been using Schlumberger Smart Cards in large trade shows and professional conventions for registration and data management for the last two years.

The system uses Smart Cards from Schlumberger Technologies, France, with 8K bytes of EEPROM memory.

Cards are issued to all visitors and are encoded with their personal details such as name, company name and type, address, and their product interests obtained from the registration form. In a conference situation, the card can be used to gain admittance to the various sessions. Attendants at the doors use handheld terminals to read the delegate's card to ensure that he or she is authorised to attend that particular session, and to record access. This provides the conference administration with accurate information on the number of attendees from which to judge the interest level of the subject and helps in planning future conferences.

Exhibitors rent Expocard readers, designed by Galaxy, for their stands. Inserting the card into the reader gives the visitor an opportunity to convey his product interests, and personal profile, quickly to the exhibitors while the exhibitor receives an immediate print-out of the contents of the Smart Card. The visitor's data is stored in the reader for future use.

Transactions are logged so show producers are able to track leads for each exhibitor, as well as the traffic patterns of all visitors. Therefore, in addition to providing superior sales lead generation and management, Galaxy gives the show producer an insight into the effectiveness and weaknesses of the event.

The card can also be used at a product locator which sorts and prints out a special directory of exhibitors and their stand locations.

Expocard will be used in more than 150 trade shows over the next 12 months. The average Expocard event has 10,000 visitors and 300 exhibiting companies, but some of the events are as large as 100,000 visitors and 1,500 exhibitors. Galaxy expects to establish its first non-USA office in The Netherlands in early 1994.

Contact: John R Laughlin, Chief Executive Officer, Galaxy Expocard Registration & Data Management, USA - Tel: +1 301 662 9400.

Mitsubishi Enhances Melcard

Mitsubishi has enhanced its Melcard range of contactless Smart Cards. The reader/writer to card communications distance, using a new design reader/writer, has been increased from 50 cms to 80 cms, and the data rate has been increased from 25.6K bits per second to 153K bits per second.

Melcards are standard size but in thicknesses of 1.4mm and 2.5mm. Typical applications are providing ID authorisation and proof of payment functions in physical access control; passenger entry and exit to public transport, car parks and motorways; and factory automation.

Contact: James Pemberton, Smart Card Product Manager, Mitsubishi Electric UK - Tel: +44 (0)707 276100. Fax: +44 (0)707 278692.

Pay-TV Card Order for Bull CP8

Interaccess, the Scandinavian television broadcaster has ordered 100,000 PC2 Smart Cards from Bull CP8 for use in their pay-per-view encryption system for programmes broadcast on the Astra satellite.

Bull says the order brings the total number of PC2 cards shipped to various broadcasters to the million mark.

VeriGem Capital $5 Million

VeriGem, the joint venture between VeriFone and Gemplus which will market complete electronic purse solutions under the SmartCash trade mark, has an initial start-up capital of $5 million, according to the October issue of Stratagem, the quarterly newsletter published by Gemplus.

New Operating System

Personal Computer Card Corporation, based in Florida, USA, has announced an improved series of Smart Cards with its new Secured Smart Card Operating System (S^{2}COS).

The new operating system provides security features for the development of applications in access control, security, and personal identification among other uses.

It is designed for use in electronic purses, debit/credit cards, financial services, electronic benefit programmes, healthcare plans and other applications requiring confidential data exchange with customers by encrypting sensitive data with the DES algorithm.

Security features

The company says that S^{2}COS enables Smart Cards to provide:

- Secure password management and distribution
- Protection from counterfeiting of cards
- Password (key) verification without revealing the password
- Verification of the card, cardholder, terminal, and transaction host
- Security to prevent the discovery, substitution, blocking, or misdirecting of data
- Creation of machine authentication codes (MACs)
- Support for multi-application uses of Smart Cards
- Data protection in a multi-tasking environment
- Ability to control data access using biometrics

There are three types of S^{2}COS cards - user cards providing authentication functions and secure data storage; application modules with protected password storage which serve host systems working with user cards; and issuing modules which format cards into secured directories and files.

Technical manuals and limited quantities of S^{2}COS cards are now available.

The company currently markets several access control systems for personal computers and networks that use Smart Cards. Their Personal Computer Security System (PCSS) offers features such as access control, directory control, program authentication, file encryption and an audit trail, and their Network Identification (NetID) features automatic log-on to Novell and Banyon Vines networks, plus secure password management and storage.

Contact: Steve Dollar, Director of Marketing, Personal Computer Card Corporation, USA -Tel: +1 800 992 1079.

Smart Card Starter’s Kit

New from Bull CP8 is a Smart Card Starter’s Kit designed for schools, colleges and universities, but useful in public and private organisations such as town halls, local authorities, companies, government agencies and retail stores which will be using Smart Cards.

The product comes in a case containing a card reader, SCOT 50 personalised cards, technical reference manuals and a Smart Card user’s guide. To operate you connect the reader to a PC and follow the instructions.

Part 1, "Discovering the Smart Card," is accessible to anyone who can use a PC, while

Part 2, "Developing a Smart Card Application," requires a knowledge of programming in C.

Bull CP8 says it is a good way of obtaining "hands on" experience and determining requirements while training staff.

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

AFC System in Tampere

Inter Marketing, based in Espoo, Finland, is to supply and instal its MTS 2010 automated fare collection (AFC) system for Tampere City Transportation and three private bus operators in the Tampere area of Finland. GEC Card Technology is supplying 50,000 contactless Smart Cards for the project.

Installation starts this month and the system is planned to come into operation in February, 1994, with the first tickets for school children and retired people. Other ticket types will all be in use by May, 1994.

The MTS 2010 System

The MTS 2010 AFC system uses a new method of data transfer by radio modem, and all data transfers are protected against unauthorised access using the DES encryption algorithm.

In a typical system, bus units include the electronic ticketing machines (ETM), card readers (available for contact or contactless Smart Cards and other types of cards) and radio modems.

When passengers enter the bus, they validate their cards in the card reader and the transaction is automatically stored on the card and in the driver's unit. (The driver can also sell single tickets using the ETM).

At the end of the shift, the driver enters the exit code into the ETM and all fare data accumulated during the day is automatically transferred to the depot computer using radio modems.

The depot system includes a microcomputer, data processing software and radio modems for data transfer. When all the fare data has been transferred from the ETMs, the system processes the data and produces various reports.

Changes or upgrades to the software can be maintained by remote support and sent directly to the depot system using the telephone network. In addition all changes are automatically transferred from the depot PC to the ETMs and the card readers using radio modems.

The system enables a flexible connection to external clearing systems. The customer can also choose to use the MTS 2010 clearing system.

Inspectors have portable reading/validation devices which are compact and light for carrying around.

Point of sale units enable customers to purchase new cards or credit existing cards. They include the ticket vending machine, a loading unit and a modem which is used to transfer the sales transactions to the depot system for processing. Any changes, for example, to the tariff tables, are automatically updated during the night using a modem.

The MTS 2010 Contactless Smart Card Reader

The MTS 2010 Electronic Ticketing Machaine

Key concepts behind the MTS 2010 system are seen as flexibility, security and compliance with international standards. This, says the company, provides a solid basis for multi-application city card systems in which a single card can be used not only for transportation, but also for loaning books at public libraries, paying parking or for health care fees etc.

Tampere project

In the Tampere project, Inter Marketing will supply 350 ETMs with integrated contact Smart Card readers, 350 Universal readers for the GEC contactless Smart Cards, automated data transfer by radio modems, depot systems, inspector units and 50 kiosk point of sale units.

Inter Marketing has designed and manufactured products for banks, retail businesses and the service sector since 1968, and its product range includes money handling equipment, self-service automates, security systems, alarm systems, access control and time-keeping systems, EFTPOS and POS systems, fare collection and ticketing systems and Smart Cards together with all related equipment and software.

MLT, a subsidiary owned by Inter Marketing provides fare collection systems for public transport companies.

Contacts: Timo Hyvarinen, Sales Manager, Inter Marketing, Finland - Tel: +358 0435 9213. John Meikle, Sales Manager, GEC Card Technology, England - Tel: +44 (0)922 616939.

Smart Vending Machines

Two new automatic in-cup vending machines have been launched by Maxpax for use in large offices and sites.

Model 12/80, with a capacity of 850 cups, offers up to 12 flavours of hot, chilled and carbonated drinks, and the 9/80, with a capacity of 625 cups, offers nine flavours.

Both models offer a choice of payment between coins or the recently launched Maxcard cashless vending system using Gemplus 2K bits EEPROM rechargeable memory cards (SCN September 1993). The cards give the flexibility to offer employees free or subsidised drinks.

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

Fuel Card System

The US Department of Defense is to use Smart Cards to implement a new system of fuel distribution developed by the Applied System Institute as part of the Fuels Automated Mangement Systems (FAMS) programme. Micro Card Technologies Inc has been awarded a contract to supply TB 100 Smart Cards.

Action Against TV Pirates

British Sky Broadcasting (BSkyB), the UK Pay-TV broadcasting company, and News Datacom who, jointly with Thomson Consumer Electronics, developed the VideoCrypt system used by BSkyB for the encryption of television signals, are getting tough with pirate hackers.

In a joint statement last month the companies said that VideoCrypt had always been a specific target for pirates and recent attacks were nothing new.

What was new, they said, was a deliberate change in policy by companies "to pursue all hacks in both the civil and criminal courts."

Criminal offence

A spokesman said: "Both News Datacom and BSkyB are determined to ensure that the pirates do not succeed either technically or economically. The use of a pirate card is a criminal offence and each time a pirate card is found, technical measures are taken to stop the user receiving a clear signal. This renders the card useless within a very short period of time."

At a hearing in the High Court in London last month, BSkyB obtained an order against David Lyons of Satellite Decoder Systems, Ballyegan, Eire. The injunction, pending trial, prevents Mr Lyons from importing, selling and advertising pirate cards in the UK. He also undertook to supply the court with a full list of all his suppliers and customers in a sworn affidavit.

BSkyB also announced that legal action had been taken against Hi-Tech Innovation of Innovation House, Albany Park, Camberley, in Surrey, and Christopher Cary, also of Camberley, Surrey. Injunctions against both had been granted, pending trial.

Permanent injunctions had been obtained against Joe Ibrahim, trading as Satellite Communications, of Chorley, Lancashire; and card production company RSD of Stirling, Scotland, run by John Ross and Patrick McGrorty.

Contact: Sally Osman, Publicity Director, British Sky Broadcasting, London, England - Tel: +44 (0)71 705 3200.

Mini-Coupler from Gemplus

The GC1400 Mini-Coupler from Gemplus is designed to provide system integrators with easy access to a Smart Card interface. The device makes it simple to adapt existing equipment with the ability to read and write Smart Cards, and it can be integrated in payment terminals, ATMs, access control systems, or park meters etc.

The GC1400 is based on a modular hardware and software architecture and is equipped with a card connector and is only slightly larger than the connector itself.

Expansion cards can be easily added to connect a keyboard, a display, additional memory, an RS-232 interface, a real-time clock, or input/output lines.

Contact: Marketing Department, Gemplus Card International, France - Tel: +33 42 32 50 00.

Bank Security System

French bank BNP has ordered a further 6,000 CAD 2000 Bull CP8 Smart Card reader/encoders for its logical access control system.

The order is part of its plan to increase the number of workstations in its branches. BNP employees are issued with Smart Cards authorising access to the information they require for their jobs.

The order brings the number of CAD readers used by BNP to over 30,000, making the bank Bull CP8’s biggest customer in Smart Card logical security access control.

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

New South Wales Tender

The Stored Value Smart Card project tender in New South Wales, Australia, closed last month and the evaluation process - expected to take six-nine months - has now started. The number and identity of the bidders has not been disclosed.

New Production Technologies

New card production technologies were announced by two speakers at the International Card Manufacturers Association Convention Conference in Portugal last month.

New Laminating Technology

A new laminating technology for the production of plastic cards was described by Jonathan Lowe, of Ciba Polymers, Cambridge, England, which has been developed as the result of collaboration between the Structural Adhesives group of Ciba (the Swiss Chemical Corporation), Burkle, and Louda (both manufacturers and suppliers of card manufacturing equipment and based in Germany).

At the heart of the plastic card manufacturing process used throughout the world was the need to fuse plastic layers together using heat and pressure to form the basic structure, he said, and these could cause processing problems not easy to resolve.

In the new process, bonding the card layers is carried out at room temperature using minimal pressure and using a rapid curing adhesive. In this way, card manufacturing can be made into a continuous process and offers quality and cost advantages over conventional manufacture.

Ciba has primarily developed the adhesive and processing technology used to bond the plastic layers together. It is a single component material, so no mixing is required and it cures by the action of ultra-violet light in fractions of a second. In this way, a strong consistent bond can be formed immediately without the need for heating.

The equipment designed for use with the adhesive has been developed jointly by Burkle and Louda and consists of a sheet feed unit (where printed core stock is fed into the laminator), the laminator (where the overlay stock is fed from bobbins and bonded onto the core), a cutter (to separate the output into sheets again), and a stacker (to stack the bonded sheets). Additional units such as a tape-layer and a punching unit can also be added as required.

The printed core is fed into the laminator where it is coated on both sides by a thin layer of the adhesive. The two overlay foils are then laminated onto the core using a rubber roller with slight pressure to expel all the air from between the sheets. The adhesive is then cured by passing under an Ultra-Violet lamp and immediate cutting and stacking of the sheets can take place.

The sheets are then available for further processing such as addition of magnetic strips, signature panel, holograms etc., or for punching into individual cards. Drilling and milling may also be carried out to enable chip cards to be made.

Reactive Thermo Sticking

Peter Liebenau, of Louda System, Germany, described a new method to bond chips in milled out cavities.

He described the hot melting, or "hot stamp" process using heat-sealing film to fix the chip in the milled cavity, and the more complicated method of working with a liquid bonding agent, before presenting the new method to bond chips called Reactive Thermo Sticking.

This was a humidity-reactive bonding method with thermosetting adhesive, and due to special dosing head it was possible to apply adhesive at several points within less than one second.

Advantages were that the adhesive was easy to handle and easy to dose in a fully automatic procedure. The bond was temperature-resistant and had a price advantage as it was about one-twentieth of the price with the same quantity of bonding agent required - 500 gr. Cyancrylat costs about DM 228.00 compared with polyurethane bonding agent costing about DM 12.00.

Considerable time could be saved in dosing and pressing which had a positive effect on overall production costs.

Contacts: Jonathan Lowe, Ciba Polymers, Cambridge, England - Tel: +44 (0)223 838310, Fax: +44 (0)223 838606; Frank Tinnefeld, Burkle, Freudenstadt, Germany - Tel: +49 7441 580, Fax: +49 7441 7813; and Peter Liebenau, Louda System, Munich, Germany - Tel:+49 89 6138 510, Fax: 49 89 6138 5193.

Contact v Contactless Prices

C2-Intern, a publication which promotes the C2 contactless cards, has published a price comparison between contact and contactless Smart Cards which prompted some of their readers to ask if the figures were really true and others to say it was impossible.

Now the publication has come up with more controversial figures, arguing that contactless cards last longer and therefore every year of longer life makes the contactless card cheaper than a contact card.

Over a three year period with 10,000 cards, the contactless card would be more expensive at DM 12.30 compared with the contact card at DM 9.61, but over a six-year period the contactless card would be much cheaper.

Assumptions made are that contact cards and couplers have to be replaced at the latest every three years, while contactless cards have a longer lifetime because they do not wear and tear (six years is assumed in the table below).

They also assume that out of 10,000 cards, one contactless and three contact cards are damaged during each year, a reader density of one reader for 200 cards, and estimate cost for transferring data from an old (or damaged) card to a new one.

The comparison, however, takes no account of lost or stolen cards. In the UK, for example, it is estimated that one in 40 cards is lost or stolen every year which amounts to 250 per 10,000 cards per year. In addition, service providers and users may not want the same card for a long period. Users too are fickle in that they want to be seen to be using the latest card with the additional functions and the new design.

Period of six years with 10,000 cards

	Contact Cards	**Contactless Cards**
10,000 cards in the first year	280000	360000
200 couplers in the first year	8400	8400
Damaged cards	84	36
Transfer data (damaged)	42	42
Replacing cards in the third year	280000	-
Transfer data (replaced)	140000	-
Replacing couplers in the third year	8400	-
Total costs in six years	716926	368478
Total cost per card in six years	71,69	36,85
Total costs per card/year (DM)	**11,94**	**6,15**

Smart Card Microcontrollers Part 3

Manufacturer	Texas Instruments	Toshiba	Toshiba
Type number	TMS373C012	JT9825	JT9964
Microcontroller core	TMS370	JTXXX	JTXXX
Architecture	8 bits	8 bits (Z80 software architecture)	8 bits (Z80 software architecture)
ROM	4K bytes	12K bytes	12K bytes
EEPROM	1K bytes	(External)	8K bytes
ECC			
Page write			
EPROM	-	-	-
Write cycles endurance			
RAM	128 bytes	512 bytes	512 bytes
OTP memory			
Voltage	5V	5V	5V
Max clock speed	10MHz	5.5MHz	5.5MHz
Max current		10mA	10mA
Sleep mode			
Special functions		None	None
Die size		N/A	N/A
I/O ports		1	1
Availability		Available in Japan	Available in Japan

Smart Card Tutorial - Part 15

Cryptography and key management (continued)

We have discussed a range of cryptographic algorithms for confidentiality, authentication and data integrity security services. We have also implicitly assumed that these algorithms are adequately secure in that their public knowledge will not invalidate the effective security. In other words the security of the particular security service depends on the management of the cryptographic keys. Whilst this is an achievable principle it is readily apparent that knowledge of the particular algorithm used does in fact give the potential attacker valuable information. In the military world the algorithms are kept secret to ensure the security and it is only the practicabilities of the situation that result in the more open use of the algorithm for commercial use. The use of Smart Cards is an advantage here since it is operationally possible to distribute IC cards to all participants without revealing the contents. The tamper resistant properties of the IC card make this an ideal carrier for both cryptographic keys and algorithms.

The IC card as a tamper resistant module.

The concept of tamper resistance is well established in the world of cryptographic security equipment. We have deliberately avoided the use of the word tamper proof as this is technically unachievable. As a starting principle it is a reasonable concept to compare the properties of tamper resistance with that of the security of a cryptographic algorithm. In both cases we are dealing with the work function required for a successful attack. In the case of the cryptographic algorithm we can consider the resources required to achieve a brute force attack by key exhaustion or in the case of the RSA algorithm for the factorisation of the modulus. We must also allow for some logical flaw in the algorithm that may result in some short cut for a successful attack. It is the latter point that is non deterministic.Since it is never possible to prove the absolute security of a cryptographic algorithm. In this situation our confidence in the strength of the algorithm depends on its exposure to expert analysis. Both the DES and RSA algorithms have withstood this public exposure to date resulting in some interesting methods of attack but that none the less still leave the algorithms with secure pedigrees from a practical point of view.

Tamper resistance is equally interesting and has occupied the minds of designers for a number of years. If we accept that we are just playing with the work function required to achieve a successful attack then it is easier to accept that adequate security can be provided. In a commercial world we normally define this adequacy in terms of a work function that ensures an attack is not economically viable. It is clear that this work function then depends on three parameters,

- time
- skill level
- resource availability

Time is fundamental to any security scheme and it is the primary task of the designer to ensure that the time required to make an attack, either exceeds the lifetime of the asset being protected or is such that the cost of pursuing the attack offers insufficient benefits. There should be no doubt in the readers mind that professional criminals are well equipped to develop the business case for their activities.

Skill levels should not be underestimated as an important factor in determining the security work function. In particular this parameter is closely linked to the rapid development of the relevant technology in this area. A quick look into the back of a modern television set compared with 20 years ago gives some dimension to these advances. The modern microcontroller used for Smart Cards is a brilliant feat of engineering that seems to know no bounds.

The last parameter refers to the need to acquire the necessary resources to effect an attack. When considering cryptographic algorithms we immediately turn our attention to the availability of the necessary computer resources and their effective MIPS (Millions of Instructions Per Second). Of course in this case we also need to take account of the increasing power of these machines and the now wide scale use of networks that enable groups of machines to be harnessed to attack a single problem. In the case of the IC chip we are concerned with more specialist equipment and their somewhat higher price tags. Modern silicon wafer fabrication lines are priced in billions of dollars. Furthermore the increasing complexities of the technology is such that these prices are unlikely to reduce.

We can define a tamper resistant device as one that offers both physical and logical protection against unauthorized access to its secret data. In our case that will be at least the cryptographic keys and perhaps the algorithm and other more general security data.

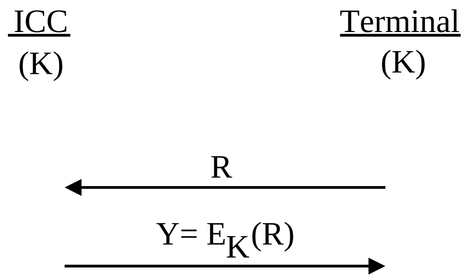
In terms of physical attacks the tamper resistant device should form a barrier to an invasive attack. There may be a number of barriers either physically hard or deliberately brittle such that an attack will evoke a response to eliminate the secret data. The classical bank safe forms a hard barrier to an attack but may also include invasion sensors that sound appropriate alarms when invoked in an unauthorized fashion. An integrated circuit chip may be encapsulated in such a way that removal of the barrier either damages the device or triggers sensors that may be used to eradicate the secret data. Some chips for example incorporate sensors in the passivation layer that set flags in a security register that may be interrogated by the application software.

It should be noted here that there is a difference between reverse engineering an IC chip and obtaining the data contents. As we have mentioned previously the data is stored in the ROM or EEPROM memory. In the case of ion implanted ROM and the EEPROM there is no obvious way of obtaining a visual image of the data contents. Thus the technique of reverse engineering, which are themselves extremely specialist, may result in the production of an electronic circuit diagram but do not reveal the data contents of the memory.

The subject of chip security is an important issue and one that we will refer to again but suffice it to say at this stage that the modern IC chip can form an extremely effective barrier to an invasive attack. Whilst some chips are clearly better protected than others the modern advances in technology are significantly on the side of the security designer. In terms of logical security this is very much in the hands of the designer and clearly steps should be taken to ensure that adequate security is achieved. For the moment it is reasonable to suggest that the IC chip can offer a tamper resistant module with a security work function adequate to meet the emerging commercial needs.

Key Management

This is really the crux of cryptographic security and it is in this area that the differences between symmetric and asymmetric cryptography become most obvious. Let us first look at symmetric cryptography as might be experienced using the DES algorithm. The whole purpose of security is to effect a security service between two or more entities. It is therefore readily apparent that a common key must be established between these entities before the security service can be effected. Let us consider the practical situation of an IC card effecting an application with a terminal. In fig.1 we show a simple situation where a common key (k) has previously been established in both the IC card and the terminal.



(Note $E_K(R)$ means encipher R with key K)

Fig. 1. A Simple Common Key

As an example we shall consider an authentication process where the terminal checks the authenticity of the ICC. Here the terminal sends the ICC a random number R. The ICC enciphers this number with the common key K and returns the response Y to the terminal. By using the same algorithm and key the terminal can check that the ICC knows the algorithm and common key K. It is readily apparent that in this scenario we would need to establish a global secret key in all the ICC's and terminals. Not only is this operationally difficult but any breach in security in any card or terminal would expose the global key. Clearly the tamper resistant properties of the terminal should be no less than that of the ICC.

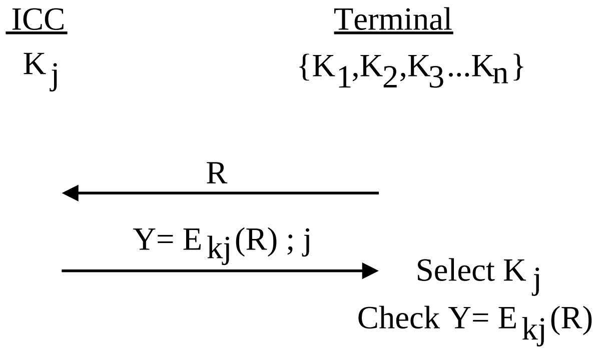


Fig. 2. Terminal Key Sets

We can improve our security vulnerability by using sets of keys in the terminal to achieve a level of security segregation as shown in fig 2.

In this situation a breach of security in the ICC only reveals the key Kj. However an attack on the terminal would reveal the complete set of keys. The assumption here is that the security of the terminal is higher than for the ICC.

Another variant of the key management process is to use derived keys as shown in fig.3

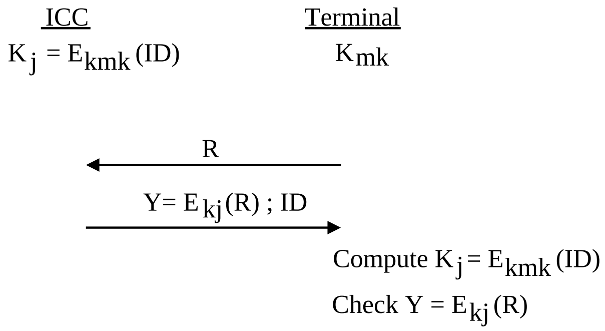


Fig. 3. A Derived Key

Here the terminal contains a master key K_{mk} whilst the ICC has been preloaded with a key derived from this master key. For example this might be an enciphered form of its identity ID.

In this scenario the global security depends again on the terminal but each ICC can have a unique derived key. This means that the effect of an attack on an individual ICC can be restricted to that individual card. In the previous case the segregation is proportionable to the size of the key set. In other scenarios it is possible also to have sets of master keys to generate a particular unique derived key.

Clearly the use of a unique key per card is a powerful security advantage but it must be appreciated that the terminal master key exposes the security of the system as for the first scenario.

David Everett

Next month, Key management continued.

Smart Card Diary

European Payments '93 (EFTPoS & Home Services), Sheraton Hotel, Edinburgh, Scotland, 16-18 November.

Contact: Paula Biagioni, Conference Secretariat - Tel: +44 (0)41 553 1930.

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

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

Smart Card '94 Conference and Exhibition, Wembley Conference Centre, London, 15-17 February, 1994, with a Smart Card tutorial on 14 February.

Conference Secretariat - +44 (0)733 394304.

CardTech/SecurTech '94, Hyatt Regency, Crystal City, Virginia, USA, 11-13 April.

Three days of seminars on technology and applications with a major exhibition of Card and Security technology. This event is presented by the Smart Card Industry Association and Personal Identification News.

Contact: CTST Tel: +1 301 881 3383.

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.

Schlumberger Public Fax

Schlumberger has developed a purpose-designed fax for public use which will accept payment by magnetic stripe or Smart bank or phone cards and offering both transmission and reception facilities, together with a conventional phone handset for voice communication.

Called Publifax, the new Group-3 terminal is the first to offer Smart Card payment, and to provide reliable, secure operation without the problems suffered by earlier systems such as paper jams and misfeeds.

Instead of feeding paper through the machine, users lay the document to be faxed in a compartment which easily accommodates standard A4 size objects. A scanner, which works something like a video camera, is sited several inches above, behind protection.

This non-contact approach guarantees that users cannot lose or damage documents, eliminates the need for prior photocopying, accepts thick documents such as an opened book, and minimises potential vandalism.

The printing system is similarly protected. Received faxes, and/or acknowledgement slips, are printed inside the machine, cut, and then dropped into the compartment.

Apart from the security offered by the use of Smart Cards, Publifax also features a patented anti-fraud system which can detect illicit external electrical connections.

Publifax can be operated as a free-standing terminal, or in conjunction with a remote PC-based supervision system called CSV 2000, as part of a network of managed public phone/fax terminals and providing daily traffic reports, the ability to download new tariffs, and with automatic alarms for maintenance and fraud/vandalism.

Instructions for use are printed in pictures and displayed in four languages with prompts, on a back-lit LCD.

Schlumberger says the primary market is the travelling business person, opening up possibilities for installation in airports, train and coach stations, petrol filling stations, hotels, etc. They anticipate initial market sizes of 1,000 terminals for most European countries. It is also seen as a future investment for local businesses, such as post offices and shopping centres.

Contact: Bertrand Dussauge, Director of Communications, Schlumberger Technologies Transactions Systems, France - Tel: +33 1 47 46 62 47. Fax: +33 1 47 46 68 66.

Card Production Machinery Order

Esec Sempac SA, of Cham, Switzerland, has received an order from B Rexroth Electronic GmbH, Lohr am Main, Germany, to supply a complete assembly line for the fully automatic production of Smart Cards.

Rexroth Electronic will use the Sempac equipment to manufacture moulded and recyclable identity cards.

Contact: Willi Truckenbrod, Corporate Vice-President, Esec Sempac, Switzerland - Tel: +41 42 44 53 53.