German Motorway Toll Trial is GSM-based

An automatic toll collection system based on the GSM (Global System for Mobile Communications) phone and Smart Card is to be trialled on a German motorway. Called Sagem, the system has been developed by DeTeMobil (Deutsche Telekom Mobilfunk GmbH), a subsidiary of Deutsche Telekom.

Sagem is based on using the existing communication infrastructure and offers the possibility of other services such as accessing traffic conditions and weather reports, and calling out emergency services in the event of a breakdown or an accident. The privacy issue is addressed by offering a pre-payment mode where tolls are direct debited from the card.

Continued on page 43

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 20 - Smart Cards and Key Management

CONTENTS

German Motorway Toll Trial

Continued from page 41

Dr Werner Kremer, DeTeMobil, says GSM is the only existing pan-European standard for mobile communication and is becoming nearly a worldwide standard. This, and the fact that the basic infrastructure investments in GSM have been made, makes the introduction of GSM-based AFC (automatic fare collection) extremely inexpensive.

A wide range of additional services including traffic management as well as telematic services can be offered with the GSM standard interface.

The GSM based AFC solution is the pan-European alternative to existing AFC systems, which are diverging in many aspects.

The system has the following features:

* AFC does not affect traffic. Multi-lane operation under all traffic conditions is possible.

* No infrastructure measures are required at the roadside.

* Standards of EFT (Electronic Funds Transfer) will be applied offering protection and unambiguous communication. High level security will meet the requirements of both banking institutions and end users.

* Smart Card technology, differentiated modes of payment and the confidence in a fraud-proof medium guarantees personal data protection.

* Multi-functionality of the mobile equipment can be offered without further communication infrastructure investments.

Motorway trials

The system will be amongst those trialled by the German Transport Ministry on the A555 motorway between Cologne and Bonn to test various technologies. These tests will look at the technologies with regard to the equipment required for vehicles, the infrastructure for charging tolls, accounting procedures, collection procedures, and enforcement. A system will be selected and introduced between 1996 and 1998.

Payment modes

Drivers can choose to pay using various debit card or credit card modes of payment, or with a reloadable pre-paid card which guarantees that the user will remain anonymous. Drivers who do not have the on-board toll collection equipment can purchase a flat rate certificate at sales outlets authorising them to use a specific route for a specific length of time and pay in cash or some other means of payment.

People who try to avoid paying will be detected by taking random samples. An enforcement unit consists of several cameras which may be permanently mounted on bridges or used as mobile units alongside the road.

Klaus Hummel, Managing Director, Technical Division, DeTeMobil, said: "In a number of system analyses, DeTeMobil has tested and shown the technical capabilities of a GSM solution, developed automatic toll collection functions and demonstrated this in the D1 network. The result is a communications concept for tomorrow's road traffic.

"Unlike systems set up in a specific location, cellular radio technology is able to provide blanket coverage. Communication is possible at any time and place, regardless of the speed of the vehicle, the number of lanes, weather conditions, whether traffic is moving or stopped, or whether the vehicle is in front of, or has passed, a toll charging area."

He said is was possible to offer drivers inexpensive basic equipment for recording tolls via a universal transmitter-receiver with the attraction of the equipment being upgraded for use as a mobile telephone.

Transport authorities would have the option of broadcasting local traffic information relating to a specific event, using the GSM-based broadcast functionalities. Parallel to this, third parties could also offer additional services developed for a specific purpose, such as parking space reservations, protection against theft, fleet management, monitoring of dangerous goods etc. Emergency breakdown and emergency call

services could also be reached from any location.

Identification of toll charging areas takes place in the vehicle, using the satellite-based Global Positioning System GPS and later on might be handled with in the GSM system. The toll charged when a toll charging area is passed is determined in the vehicle. The rates are set by the toll system operator according to the traffic authority's instructions and can be changed depending on the time of day or road conditions via the GSM system. With such a dynamic pricing procedure, it is possible to vary rates in accordance with exhaust emissions, the flow of traffic or other conditions.

Contact: Reinhold Mertens, Sagem Project Manager, DeTeMobil, Germany -Tel: +49 228 9866-700. Fax: +49 228 9866-705.

Siemens Licence MIFARE

Siemens AG and Mikron Gesellschaft fur Integrierte Mikroelektronik GmbH, based in Graz, Austria, have signed an agreement whereby Mikron will licence Siemens with its MIFARE contactless chip card system for use in automatic fare collection. Other applications are access control, ski ticketing and electronic purse.

MIFARE is a radio frequency identification system designed primarily for public transit applications. The system comprises contactless Smart Cards and read/write units to communicate with the card. Communication distance between reader and card is up to 10cms. Mikron has developed a high speed RF communication interface with more than 100Kbaud data rate.

The card measures 54 x 86mm with thickness 0.76 to 1.5mm and has 1K byte EEPROM. Typical transaction time is <100 ms.

Contacts: Martin Buhrlen, Sales & Marketing, Mikron, Austria - Tel: +43 316 2799-0. Fax: +43 316 2799-33; Laura Hotham, Corporate Communications, Siemens, England - Tel: +44 (0)344 396396. Fax: +44 (0)344 396326.

FRAM Cards for Manchester Pilot

The recently developed "In Charge" card with FRAM (Ferroelectric Random Access Memory) (SCN June 1993) will make its debut in the UK in the Greater Manchester public transport trials starting this month. The new card is called OneCard .

ERG Electronics, Australia, who are responsible for supplying the system, have ordered 5,000 of the contactless cards for the pilot. They were developed for applications such as electronic fare payment in mass transit systems by Racom Systems Inc. and Ramtron International Corporation in the US.

The loss of the order is a blow for GEC Card Technology in the UK who were to supply their contactless cards for the pilot.

John Meikle, GEC Sales Manager, said that they had to develop a special mask for the Manchester project and the specification was not available until the end of August. The company had also had problems with a new card production line and had concentrated their efforts in supplying cards for London Transport's trial in Harrow.

Manchester's next order will be for 500,000 cards and ERG will decide in June what contactless technology they will use for the roll-out.

Gemplus Office in Beijing

French card manufacturer Gemplus has opened a sales office in Beijing, China. Mr Yang Yan Bing has been appointed Sales Manager.

The company is already active in China, operating through its subsidiary in Singapore. It is providing off-line payment cards for the Bank of China, has equipped the GSM mobile communications site in Shanghai with Gemplus SIM cards, and is currently working on the first application of Smart Cards for the Shenzen Stock Exchange. In north China more than 10,000 students use Gemplus cards for identification, as a portable file and for buying meals in canteens.

Contact: Yang Yan Bing, Sales Manager, Gemplus Beijing - Tel: +86 1 831 6688.

Japanese Market Trends

An overview of Japan's IC card market and trends

was given by Toshio Utsunomiya, of JICSAP (Japan IC Card System Application Council) speaking at Smart Card '94 in London last month.

Compared to Europe, the Japanese IC market was small, primarily because of the widespread use of magnetic cards - about one billion magnetic stripe cards used mainly as cash withdrawal, credit and ID cards; and PET (polyethylene terephthalate) telephone cards amounting to over 2 billion.

However, steady progress had been made in recent years on the development of systems that took advantage of the functions of IC cards, and rapid commercialisation had began. As of 1993, a total of 2.5 million IC cards had been issued.

Increasing in popularity were employee and membership card systems, while another recent trend was the steady spread of local government cards designed to help provide residents with various services.

Operational systems

Among examples of operational systems was the Sukoyaka Card in the Goshiki-cho Parent-Child Healthcare system which holds information about the medical care and health of the mother and child. The card is issued at birth and functions like a maternity record book storing information concerning examinations at hospitals at birth and other stages in the child's development together with treatment received. It also contains a dental history.

Mr Utsunomiya said that data from examinations and patients interviews and data on growth could be converted to graphs or tables and displayed on computer screens, thus making it easy to determine progress and facilitating guidance provided to patients or persons undergoing an examination. The service began in May 1992 and about 300 cards have been issued.

At Makuhari Techno Garden, an intelligent building park comprising six office complexes, 10,000 cards have been issued to tenants for use as pre-paid cards for cafeterias, vending machines, and goods sold. Pre-payment is made at six IC card handling machines inside the complex. The card also functions as a security device to operate gates on certain floors, underground parking lots, and controlled access to computer rooms.

The Taisei Construction IC Partner Card system is designed to facilitate employee supervision information and is being implemented nationwide. Features include the ability to instantly determine which employees are in the workplace, and the qualifications possessed by an employee. The system was launched in April 1993 and is now in use in 130 locations with a target of 400 sites.

An example of a campus system is in operation at Tokyo Kogakuin College of Technology. Called the MUSASY (MUltimedia Super Access SYstem), the Smart Card provides access to 26 Videotex terminals used for various types of inquiries and applications, for example, reading mail sent to students from instructors, checking grades for each term, attendance records, applying for commuter passes for trains and buses. Students can even check their biorhythm.

The cards can also be used as pre-paid cards for purchases in cafeteria, stores and at vending machines.

At the Karasuyama shopping district, customers are offered a pre-paid Smart Card for purchases. Cardholders can also purchase goods at participating retailers by using an ordinary credit card along with the IC card.

Customers collect loyalty points on purchases and these points can be used towards tickets to special events, tickets for municipal buses and product purchases etc. Nearly 7,000 cards have been issued.

Currently the biggest single Smart Card project in Japan is the Nissan Car Life customer loyalty and vehicle service scheme with 450,000 users (SCN December 1993), but recently NTT Data ordered 1.8 million Smart Cards to be used in a customer loyalty scheme by one of Japan's biggest petroleum companies.

Contact: Toshio Utsunomiya, JICSAP, Japan - Tel: + 813 5401 2932 Fax: +813 3433 8921

Healthcare Cards in the US

The United States did not have a substantial

domestic Smart Card production capacity and it was difficult for user organisations to find the equipment and expertise they needed, especially for very large-scale applications such as President Clinton's proposal to put Health Security Cards in the hands of over 225 million citizens, said Benjamin Miller, Editor and Publisher of Personal Identification News, speaking at the recent Smart Card '94 Conference in London.

"Even the magnetic stripe card industry which produces 450 million bank, oil and retail cards a year, will be hard pressed to fill such a sizable order in a quality fashion," he said.

Reform plan

While the health reform plan initially called for magnetic stripe cards protected by PINs, the regional "alliances" which would operate the system would be free to include additional technologies. A consortium of Western states was one region which planned to investigate Smart Cards to carry additional health and welfare functions.

Eventually, he said, all the national cards might carry a chip, but the most immediate effect of the President's announcement had been to stimulate a great deal of interest in Smart Cards for regional and local applications.

The largest application to date was the Department of Defense's Consolidated Healthcare System for military personnel and dependents in Hawaii. This was a multi-million dollar investment involving, initially, 300,000 microprocessor cards.

Contact: Ben Miller, PIN - Tel: +1 301 881 6668.

First National Loyalty Application

Clean Card from the Clean Way company is the first loyalty application to be launched on a national scale using Smart Card technology. It is a new service to enable uniformed employees to have their work uniforms cleaned in a network of 1,000 dry cleaners throughout France.

The Clean Card is the Gemplus GPM896 protected memory card. It is personalised with the company's and employee's name and credited with a number of cleaning tokens authorised by the company for its staff and may be used for a pre-determined period.

Each user manages his or her own dry cleaning credit directly and chooses when to visit any one of the network outlets.

Clean Way has customers in the following sectors: passenger or goods transportation (air, sea and land), telephone industry, cosmetics, funeral services, supervision services and security, museums, company sales teams, receptionists, etc.

At the dry cleaners, the card is inserted in a reader and the charge is deducted for the service. When credit is used up, a new cycle begins and the card is automatically reloaded by the terminal which communicates with the computer server to identify the cardholder, his company and the credit allocated to that individual.

At the end of each cycle, Clean Way sends the client company a statement showing cleaning frequencies for each individual. A phone call to Clean Way can vary the credit allocated to personnel according to the season and type of work undertaken.

Contacts: Raphael Blascot, Clean Way, France - Tel: +33 1 41 21 00 00. Caecilia de Saint Victor, Gemplus, France - Tel: +33 42 32 51 54.

DS Card from Philips

A new Smart Card, the DS 1K byte EEPROM card, has been announced by TRT Philips, Smart Cards & Systems, France. A general purpose multi-service microcontroller card, it offers a simple and flexible logical memory organisation to access services.

Applications are seen as portable file card, identity card, company card, membership card, fidelity card, access control card to buildings or to a service provider computer.

Contact: A J Selezneff, International Marketing Manager, TRT Philips, - Tel: +33 1 41 28 75 84.

Swedish Allterminal Project

Swedish Police will be the first government agency to test the new Allterminal PC network security system based on Smart Cards to control access to personal information.

The system, developed by two Swedish Companies, AU-System and Dynasoft, is being evaluated at a local police district outside Stockholm. During the year, 2,100 personal computers will be equipped with Allterminal software and hardware, and 10,000 employees will be issued with Smart Cards.

As new PC-based computer systems with modern client/server technology are now replacing old terminal systems in the regional offices of many government agencies such as the Social Insurance, Tax and Police Agencies, to improve efficiency and services, there has been concern about the need for high security to prevent unauthorised access to personal and confidential information.

As a result a number of Swedish government agencies went out to tender with a Common Requirement Specification called Allterminal to emphasis the usage of the PC as a general purpose terminal for all government applications.

Key concepts of Allterminal are:

* Each user carries a Smart Card containing a signed certificate of identify.
* All authentication is based on the asymmetrical key system RSA.
* The certificates and the keys in the Smart Card can also be used for Host computer authentication, generation of session keys for data encryption and for producing Digital Signatures.
* Smart Cards personalised and issued by a central authority.
* All software modules in the PC have open interfaces which enable other hardware and software suppliers to produce compatible products.

The Smart Card

The Smart Card used in the system is the Philips DX 2K byte EEPROM card. This was chosen for its RSA calculation capabilities. Since the RSA calculation is handled completely within the card, the secret RSA key is never exposed. An optimised calculation unit on the card permits RSA signature computation using 512 bit keys in less than 500 ms. This is significantly faster than that possible in software on most PCs.

User data, symmetric keys for the PC file encryption and X.509-compatible certificates with the user's verified identity are stored in the card memory.

Several Smart Card readers can be used in the system - currently readers from Philips, Gemplus and Schlumberger are supported.

The user's name and personal identification number is printed on the front of the card. Most organisations will also have the user's photograph and signature printed on the card to make users more aware of the importance of the card for security. The Smart Card with photo may also be used as a company ID card in the future.

The user must identify himself to the local access control system by inserting his Smart Card in the reader and entering his secret PIN code. The card stays in the reader during the operation of the PC. If the card is withdrawn the PC is automatically put in standby mode. If the user does not re-enter his card within a predefined time, the PC is re-booted.

All directories in the PC are marked with a special "key file." The user's access to a directory is only permitted if the corresponding key is available in the user's Smart Card.

Protection against disclosure is strengthened by encryption functions which automatically provide for the encryption of all information which is stored on the hard disk of the PC. The file encryption is based on encryption keys stored in the Smart Card, and is done transparently, without any intervention from the user. Several users may share the same information if they have the same group key stored in their Smart Card.

No new programs may be installed in a "secured PC" without intervention by the system administrator. All programs are also checked for possible viruses before execution by computing and verifying a check-sum pre-computed at installation time for every executable module. A

special module for boot protection also denies access to the hard disk if the system is booted from floppy disk.

Communication with different host computers and servers requires the use of a challenge and response access control system. A module for digital signatures is available as an option.

Discussions are taking place with several other government agencies for the installation of another 4,000 personal computers and the issuing of 20,000 Smart Cards.

In the private sector, various companies have expressed interest in the Allterminal system as a general solution for data security. Discussions are also being held with the banking industry for using the Allterminal Digital Signature module to secure bank transfer transactions from customers using their own personal computers.

Contact: Hans Nilsson, AU Systems Communication, Sweden - Tel: +46 8 726 7500.

Dutch Rail Project

Netherlands Railways will decide this year if they are going to proceed with a proposal to introduce contactless Smart Card ticketing, following a feasibility study and the drawing up of a specification. A project team are currently estimating costs and benefits as well as several scenarios for introducing the card.

Netherlands Railways will then decide if the specified image of the new travel pass system fits within their business goals, specifically as a tool for refining and redefining the transport services for its customers; and if they will be able to recoup their investment.

If the decision is positive the project will move on to a trial phase and phased implementation within the company and nationwide, says Project Manager Wetse de Boer.

In 1992, the Netherlands Railways conducted a feasibility study to establish if train tickets could be replaced by a chip card which would combine different tickets with various functions such as tickets for bicycle sheds, parking and bus travel; offer more suitable tariffs, allow for quick and accurate monitoring of the number of passengers per ticket type and allocate revenues to the different transport operators.

Much attention was given to contactless chip cards because of the speed of reading the card, for example, during peak hours, when trains carrying approx. 1,000 passengers per train stop at a platform every three minutes. Passengers also have to leave the platforms within that time.

In 1993, Netherlands Railways carried 900,000 passengers a day. Other public transport companies carried about 2.6 million passengers a day (at 1990).

The study reached the following conclusions:

* combining different tickets in a single chip card is possible and is in demand among train users and other public transportation companies.

* Chip cards offer many possibilities for structuring and differentiating tariffs.

* When using chip cards as train tickets, it is possible to measure quickly and accurately the number of passengers per ticket type and per trajectory (i.e. registration of the transport performance).

* allocation of revenues to the various trains and/or buses should be based on the registration of transport performance.

A chip card system could be paid back through additional earnings or through savings due to reduced fraud.

The project team recommended introducing a new type of ticket in the business plans, developing a combined ticket together with other partners in public transport, introducing a combined pass, starting with a combination of facilities within the holding (train ticket, train-taxi ticket, tickets for parking facilities and bicycle sheds).

Contact: Wetse de Boer, Netherlands Railways - Tel: +31 30 353422.

Reading Bus Trials

A Travel Card is to be launched on 200 buses operating in Reading, Berkshire, England, this month and holders will be able to use it for paying bus fares and for parking in Reading Borough Council car parks. Later it is hoped to extend this facility to National Car Parks (NCP).

The card will be a magnetic stripe card initially but it is intended to upgrade to a Smart Card when more services are available such as travel on British Rail and entry to civic amenities. It will be available in values of £1, £5 and £10, and later £20. Ticket machines being supplied by Wayfarer are equipped with Smart Card readers.

Contact: Pat Baxter, Project Leader, Reading County Council - Tel: +44 (0)734 875444.

Boosters for Road Tolling

Contactless card manufacturer, Nedap, has developed a battery operated booster for use in conjunction with standard access control cards. Working at a frequency of 2.45 GHz it facilitates the reading of cards at distances of up to 20 metres.

For secure contactless Smart Cards, a non-intelligent booster working at a frequency of 5.8 GHz is under development.

Aimed at public transport applications such as road tolling the boosters, for example, can be placed behind the windshield of a car. With a Contactless Smart Card put in front of the booster it can communicate over longer distances at high bit rates of 60kbits.

The booster unit does not contain any data to be secured and the transaction with the card takes place in a realtime mode without storing data in intermediate buffers.

The booster unit operating at 5.8 GHz will have an anti-collision protocol, for which the card already contains provisions.

Contact: Johan Hogen Esch, Director R&D, Nedap, Netherlands - Tel: +31 5440 71111.

Helsinki Travel Card Trial

Four separate electronic ticket machine trials using Smart Cards have been carried out in Helsinki, Finland, under the collective name of the Helsinki Travel Card Trial, and involved three trials on buses and one with taxis.

The important feature of the trials was that they were each evaluating different technologies, leading to comparative conclusions. Among the findings were:

* Proximity and contactless travel cards were faster to use than contact cards.

* All the overall systems in the trial proved technically suitable and reliable, but the quality of the Smart Cards used in the trials was not adequate.

Heikki Sahlsten, Helsinki Metropolitan Area Council, speaking at Smart Card '94 in London last month, explained that 2,430 passengers asked for trial cards and 1,480 were actually used.

The bus routes chosen were two internal routes (nos 91 and 92) of the Helsinki City Transport (HKL) which are metro feeder routes; and Vantaan Liikenne Oy's (VLOY) nos 360, 361 and 362 which are regional trip routes. Taxi cards were tested in invataxis operated for the disabled by Handicab of Espoo.

Trial 1 on HKL bus no.91 used the AES Datafare contact card system supplied by AES Scandinavia and using DNP contact Smart Cards.

Trial 2 on KHL bus no.92 used the Buscom 700 proximity card system supplied by Buscom Oy and their contactless proximity cards.

Trial 3 on VLOY bus nos 360, 361 and 362 used the MTS 2010 contactless card system supplied by Inter Marketing Oy using cards supplied by GEC Card Technology.

Trial 4 in Handicab Oy taxis in Espoo used a contact processor card supplied by Setec Oy.

During the one year trial period there were 129,104 card validations on the bus routes, and

4,228 on the taxis.

Bus stop delay measurements suggested that the average speed of use of the various card options compared to the conventional 30-day bus pass (1.7 sec/person boarding bus) was: much slower in the case of the contact card (1.6 sec/person); slightly slower in the case of the contactless card (0.6 sec/person); and slightly faster in the case of the proximity card (0.2 sec/person).

Card faults

Mr Sahlsten said that in the bus trials the electronic ticket machines worked reliably after some initial problems, but the Smart Cards failed to satisfy the requirements set for them in regard to accessibility.

The quality of the memory and processor cards proved even less adequate; the cards broke often -

* contact cards (AES) over 100 units (over 20%)

* contactless cards (Inter Marketing) over 50 units (over 10%)

* proximity cards (Buscom) <10 cards (about 1%)

All the contact cards were exchanged for new ones and the new cards did not break.

In the taxi card trial, the readers installed in the vehicles suffered from faults caused by the power supply, which led to a card reading failure rate of around 8%. On the other hand, all the cards supplied worked faultlessly.

It was concluded that the most suitable form of new fare payment system would be one based on proximity or contactless Smart Cards capable of being reloaded.

The taxi card trial results clearly indicated that a fare system based on contact Smart Cards as a replacement system for the present taxi voucher system for the disabled should be introduced as soon as possible. A conservative estimate of overall savings exceeded 20% compared to the voucher system.

Contact: Heikki Sahlsten, Helsinki Metropolitan Area Council - Tel: +358 015 61410.

Dutch Healthcare Card

A Smart Card is being used in the city of Delft, in The Netherlands, as a health insurance certificate and also as a patient card containing medical and emergency information.

Called the VIP-card, VIP stands for Verzekerings (Insurance) Identificatie (Identification) and Patientenkaart (Patientcard).

Since the pilot project was started by public healthcare insurer Zorgverzekeraar DSW in August 1993, 1,200 cards have been issued with a target of 30,000 by the end of this year. The card, which is still in the experimental stage has a microprocessor chip and was designed and printed by Sdu, the former State Printing & Publishing Co.

Nationwide implementation planned

The project will run until the end of 1995 and it is expected that the card will be introduced nationwide in 1996.

During the pilot, card readers are located at GPs, pharmacies and at the emergency ward of the Reinier de Graaf Gasthuis (a hospital). These card readers are connected to the computer of the healthcare provider.

By using the VIP-card, the healthcare provider identifies the patient and establishes the validation of insurance and allowances.

The GP, pharmacist or nurse inserts the VIP-card of the insured person into the card reader, and the patient data is displayed on the screen. The GP can add data to the card via his GP Information System. When the patient takes a prescription to

the pharmacy, the pharmacist can enter information about the type, quantity and usage of the drug prescribed from his Pharmacy Information System onto the card.

All cardholders are registered in the Card Management System held on computer. By a link-up with the DSW insurance system IKAZ, all personal and insurance transactions of insured persons carrying a Smart Card are passed on daily by modem. Whenever a card is inserted in a card reader, the card is updated if necessary.

Security

Data on the card is protected by a PIN number so that if the card is lost or stolen the data cannot be used or accessed by an unauthorised person. The cardholder can retrieve the data by entering his or her PIN code at a public terminal.

Healthcare providers authorised to read data on the card of their patient use a personal key code. This allows a GP, pharmacist or specialist to read or write only the appropriate data, for example, a GP is not allowed to change anything in the medication history that the pharmacist has written to the card. The GP is only allowed to change data in the medical section on the memory chip. The insurer cannot look at either medical or prescription data on the card.

Customer rights

Whenever an insured person objects to medical data or usage of drugs being recorded on the card, they may "lock" this part of the card. In this case the VIP-card remains as a certificate of insurance.

An interesting feature is that the insured person, using a public terminal, can enter the names and addresses and telephone numbers of two people who should be notified in case of emergency.

The following data is recorded on the card:

- Personal data - name, address, city, date of birth, sex etc to be updated by the insurance company.
- Insurance data: insurance company, insurance number, type of insurance to be updated by the insurance company.
- Medical data: chronic diseases, allergies to be updated by GP and/or specialist.
- Data on drugs: usage of drugs to be updated by the pharmacist.
- Emergency data - as described above, to be updated by the insured.

Contact: Frans C W ten Brink, c/o Zorgverzekeraar DSW, The Netherlands - Tel: +31 10 2 466 423. Fax: +31 10 4 265 506.

Hong Kong Mass Transit Project

In one of the world's largest contactless Smart Card projects, the major transport operators in Hong Kong have agreed to introduce a common card which can be used for payment of fares on all forms of public transport including, rail, bus and ferries.

Tenders have been issued to nine international companies for the supply of three million Smart Cards and 5,000 units of processing equipment.

The contract is scheduled to be awarded in June this year with service trials programmed for 1995. Subject to satisfactory performance of the system, full public introduction is scheduled for 1996.

It is envisaged that the Smart Card will ultimately replace the existing magnetic common stored value ticket (CSVT). It will act as an Electronic Purse. Unlike the CSVT, the new card will not be captured once the value had been used up. The passenger will retain the card and add value to it by using cash or machines at convenient locations throughout the territory.

In use, the passenger will simply place the contactless card in close proximity to the reader and the transaction is completed using radio communications without the card ever leaving the passenger's hand.

Initially, the Smart Card will only be used for transportation purposes, but it may later be extended as a payment method for other service applications such as parking meters, telephones, entry to swimming pools, etc.

Contact: Brian Chambers, Project Leader, Mass Transit Railway Corporation, Hong Kong - Tel: +852 751 2278. Fax: +852 795 9993.

Bank Islam Smart Card

Bank Islam in Malaysia, with over 50 branches, has introduced Smart Card Automatic Teller Machines (ATMs) for its 350,000 savings account holders.

The system is helping to reduce queues at bank counters during peak periods thus improving customer service, and making it convenient for customers to operate their accounts outside normal banking hours.

The Smart Card used is the SCOT 50 1K byte EEPROM card from Bull CP8, France. It acts as a replacement for the savings passbook while functioning as an ATM Card.

Smart Card ATMs are currently available at 11 branches representing the majority of savings account holders. By the end of the year all the branches will be equipped. Options available at the ATMs are - cash withdrawal, change PIN, cheque deposits, balance enquiry, printing of balance with last five transactions, and account transfers. About 10,000 Smart Cards have been issued since the system went live in June 1993.

Future developments will involve a Smart Card with a bigger memory capacity for use in applications such as charge cards, debit card, EFTPOS cards, and credit cards. It is likely that these facilities will be incorporated in one card.

Contact: Mohd. Yassin Mohd. Shariff, Senior Manger, Computer Department, Bank Islam Malaysia - Tel +60 3 293 5566.

CASCADE Project

A group of European companies are planning to achieve a "quantum leap" in Smart Card capability by developing state of the art 32 bit RISC processors architectures to boost processing performance and security protection. The new chip will also support advanced biometric functions such as voice profile recognition.

The project, called CASCADE (Chip Architecture for Smart CArds and portable intelligent DEvices), is funded under the European Commission's ESPRIT Open Microprocessor systems initiative.

CASCADE has been initiated by French Smart Card manufacturer, Gemplus, who will co-operate with ARM, the UK-based architect of RISC (Reduced Instruction Set Computer) processors with features such as high performance, low power and small die size. The new processor will be based on ARM's 32 bit RISC technology.

The group said: "The processing power of an ARM RISC is approximately 100 times higher than used in current Smart Card chip implementations. The capability of handling 32 bit data words will significantly improve the speed for the processing of complex calculations used in cryptographic algorithms. In addition, state of the art high level programming language compilers are available for ARM processors. An important increase in performance can thus be expected due to higher efficiency of code."

Biometrics technologies being developed by UK-based Domain Dynamics and Neural Computer Sciences, says the group, will open the use of Smart Cards to new applications with higher security constraints.

Innovations in Smart Card operating system and security technology will be introduced by the universities of Lille, in France, and Louvain, in Belgium. The operating system will use compression algorithms to increase on-chip storage capacity and provide public key algorithms for data encryption.

Dassault Automatismes et Telecommunications will build a card terminal capable of exploiting the new chip and conforming to ISO standards.

Project summary

Gemplus (France) as prime contractor and Project Co-ordinator and will provide all Smart Card specific developments such as the security modules (software and hardware), the card operating system and on chip peripherals. Contact: Patric Peyret - Tel: +33 42 32 50 00. Fax: +33 42 32 50 44.

ARM (UK) will design the chip architecture and provide the applications development tools. Contact: Matt Lee - Tel: +44 (0)223 400400. Fax: +44 (0)223 400410.

Domain Dynamics Ltd (UK) will develop the biometrics features to be integrated on the chip and the front-end circuitry in the card terminal. Contact: Stuart Timms - Tel: +44 (0)793 785491. Fax: +44 (0)793 782008.

Dassault Automatismes et Telecommunications (France) will ensure compliance with international standards for the project results and develop a card reader prototype. Contact: Thierry Collin - Tel: +33 1 30 81 25 61. Fax: +33 1 30 81 23 22.

Neural Computer Sciences (UK) will participate in the biometrics developments with DDL for the implementation of Artificial Neural Networks that will handle the biometrics data in the chip. Contact: Brian Kett - Tel: +44 (0)703 667775. Fax: +44 (0)703 663730.

University of Louvain (Belgium) will develop the cryptographic software (and possibly hardware modules) and co-operate at its integration with the CASCADE Operating System. Contact: Professor Jean Jacques Quisquater -Tel:+19 32 10 47 25 41. Fax: +19 32 10 47 86 67.

University of Lille (France) will provide architecture evaluation tools and study the lossless data compression algorithms to allow a data compression on the chip without slowing down of the data exchanges. Contact: Vincent Cordonnier - Tel: +33 20 44 60 47. Fax: +33 20 44 60 45.

ARTTIC (France) will provide the Project Office and management services. Contact: Bruno Cucinelli - Tel: +33 1 45 15 24 51. Fax: +33 1 45 15 24 60.

Motorway Tolling Invitations

Motorway tolling plans for Britain moved forward last month with the announcement of a schedule by John MacGregor, Secretary of State for Transport.

Since his statement last December that motorway charging would be introduced on Britain's roads, invitations have gone out to over 350 electronics manufacturers, software houses and consultants around the world to work with the government to develop the best technology.

He announced the following timetable:

* The appointment shortly of consultants to help the government's technology research.

* A seminar to be held by the Department of Transport in central London on 25 April to exchange information with industry and help companies to identify others with complementary technology.

* A response from interested parties who wish to participate by 31 May.

* The Department will begin assessment of complete systems or system designs in September.

* Early 1995 the Department will select two or three complete systems for detailed testing and evaluation during the year.

Mr MacGregor said: "No country has implemented fully electronic tolling on the scale needed to cover the British motorway system. I am confident that industry will rise to the challenge of identifying suitable technology and justify my belief that it would be feasible technologically to install charging here within about five years. The opportunities for business are enormous, not just in this country, but worldwide."

Industry guidelines

The tolling system will eliminate the use of conventional toll booths because of the land they would require and the congestion they would

cause. It is an essential part of the system that tolls can be paid electronically while vehicles are on the move.

The Department's invitation to industry and associated guidelines are available from Michael Goodwin, Department of Transport, UK -Tel: +44 (0)71 276 6694. Fax: +44 (0)71 276 6364.

Smart Card Diary

Prepaid Systems '94, Palais de Congres, Paris, France, 23-25 March.

Thirty-five international speakers will present their experiences and technologies related to prepaid card payment systems and the electronic purse. Contact: Analyses & Syntheses, France - Tel: +33 1 46 28 82 10. Fax: +33 1 46 28 95 63.
Cards & Commuters '94, Penta Hotel, Berlin, Germany, 30 March.

a la Card Conference on road pricing and urban commuter traffic management. Contact: Hoppenstedt & Wolff Verlag GmbH, Germany - Tel +49 40 668 6090. Fax: +49 40 270 8066.

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

Three days of seminars on technology and applications, preceded on April 10 by workshops on identification and advanced cards. Also a major exhibition of card and security technology. Contact: CTST - Tel: +1 301 881 3383.

The 8th Financial Self-service '94 Conference and Exhibition, Sheraton Grand Hotel, Edinburgh, Scotland, 10/11 May.

Contact: Ms Paula Biagioni, Scottish Electronics Technology Group - Tel: +44 (0)41 553 1930.

Prepayment Cards and Electronic Purse, The Kensington Hilton, London, 26/27 May.

Leaders in prepaid cards will talk about their systems, including the banking partners in the MONDEX project. Contact: Kate Briscoe, AIC Conferences - Tel: +44 (0)71 329 4445.

Smart Card Tutorial - Part 19

Anonymous payment schemes

Those people involved in the marketing of electronic cash systems will need little persuasion on the product benefits of conventional cash. The simplicity and flexibility of payments in shops or even between individuals is hard to better. One of the obvious features of cash is its anonymity. In general you can make payments for goods or services with no audit trail that would lead a third party to your identity. Whilst consumer needs for such anonymity must vary we can all imagine situations where such characteristics are desirable if not essential. The classical electronic purse scheme as we have discussed previously leads to a rather effective audit trail on consumer spending. Lets look at this model again as shown in fig. 1.

The conventional electronic purse involves three processes,

- value load
- payment transaction
- transaction settlement

Each of these steps involves a number of audit trails. The issuer normally provides electronic value to the consumer against an account debit. Clearly the issuer must identify the account holder and obtain his authorisation for the transaction. We may also assume that any electronic purse instrument will contain a unique identification number. We can easily arrange for the relationship between the purse and the account holder to be independent but in practice they are highly likely to be linked. Accordingly the issuer can and almost certainly would build a transaction log that shows the loading of a particular purse against an individual account.

GraphicContainsDatafor

PostscriptPrintersOnly.

When the consumer uses his electronic purse to make payments for goods and services the service provider will make a record of the transaction as the basis of subsequent payment by the issuer. This transaction will need to include a record of the purse identity in addition to the value of the transaction. This transaction log however is totally anonymous in that it should not contain any correspondence with the card holder's identity.

When the service provider submits the transaction record for payment by the issuer the data record will contain the unique identity of the purse which the issuer can relate not only to the account holder but also to the particular service provider and for the value of the payment.

It is quite clear that the information collected by the issuer is sufficient to build an information data base on the account holder's spending behaviour. This has caused concern amongst many system designers but the problem has been addressed in some detail by the mathematician David Chaum who has produced a novel solution to this problem.

The essence of David Chaum's technique can be best understood by a simple allbeit some what incomplete analogy. Let us consider a method for making a $1 payment for goods in a retail shop. The stages in the process are shown in fig.2.

GraphicContainsDatafor PostscriptPrintersOnly.

The consumer takes a plain piece of paper that will become his certified $1 note. He prepares an envelope that contains this plain piece of paper along with a carbon copy paper. He then takes the sealed envelope to the bank who stamp the envelope with their certified $1 seal. The imprint of course ends up on the plain piece of paper contained inside the envelope. The bank will take payment for the use of the $1 seal but cannot see the plain piece of paper inside the envelope and therefore cannot subsequently identify the paper but can recognise the imprint of their seal.

Once outside the bank the consumer unwraps the envelope to remove the piece of paper that now has the bank's imprint for $1. The consumer takes the stamped paper to the shop which is able to recognise the bank's seal and offer goods in exchange. When this piece of paper is presented to the bank by the retailer then the bank can recognise it's seal and make payment in exchange to the retailer.

Chaum's mathematical equivalence can be explained by using an RSA digital signature. The main principle to remember is that the checking of a signature is made by comparing data with some mathematical transformation of that data. We can recall from previous discussions in the tutorial for an expression of the RSA algorithm using a public exponent of 3 as follows,

$S = M^d \text{ Mod } N$ (i.e $^3 M \text{ Mod } N$) √

$M = S^3 \text{ Mod } N$

GraphicContainsDatafor PostscriptPrintersOnly.

The signature (S) here is effectively the cube root of the message (M) created using the secret key d. N is the common public modulus.

The mathematical process proceeds as shown in fig. 3. All operations are assumed to take place modulo N although this is not shown in the figure for clarity. Instead of a piece of paper the operations now take place using numbers and mathematical transformations. The consumer chooses two random numbers r and x and forms $r^3 . f(x)$ where f(x) is a one way function of x. He takes this number to the bank which applies it's signature process thereby calculating the cube root. The number returned to the consumer is therefor equivalent to $r . {}^3 f(x)$. The point to notice here is that the bank knows neither x or r since only the product $r^3 . f(x)$ was supplied.

The consumer can now divide the number supplied by the bank by the originally chosen value of r to recover ${}^3 f(x)$. When he goes to the shop he gives the retailer both x and ${}^3 f(x)$ which are now equivalent to the $1 . The retailer can check the authenticity of this number by cubing ${}^3 f(x)$ to see if it corresponds to f(x) (i.e a conventional RSA signature check).

The retailer subsequently sends x and ${}^3 f(x)$ to the bank which can also check for its authenticity. However there is no way that the bank can make any correspondence between this signature and any of it's account holders. Therefor the transaction is truly anonymous. You can see that it was the use of the random number r that disguised the number provided by the consumer. This number was subsequently removed after the banks signature process. In the analogy this compares to the use of the envelope.

There are of course a number of short comings in the simple process described here and it is the ingenuity of Chaum's work in solving these problems that is particularly interesting.

We have mentioned previously that the principle weakness of a digital signature is the ease with which a fraudster may take a copy and therefor issue a duplicate. It is readily apparent that the retailer could phone the bank and ask if the particular signature in his hand has already been presented. However in practice this is not tenable with the concepts of electronic payments by an electronic purse.

The solution proposed by Chaum solves the problem in a different way and results in a scheme whereby the identity of the consumer will be revealed if he attempts to spend the signature twice. This rather elegant technique is based on a definition of the number given by the consumer to the bank for signature. In a simplified form we will show the principle of the detection method as follows,

the consumer computes a vector (say 20

elements) for signing by the bank as,

$$[\ r_i^3 \ . \ f(x_i\ ,\ y_i)\ ]$$

Where $x_i = g(a_i)$ and $y_i = g(a_i \oplus ID)$ [$\oplus$ = exclusive OR]

Note: if $z = a \oplus ID$ then $z \oplus a = ID$

the a_i are randomly chosen and g() is another one way function. ID is the consumer account reference number. The signature created by the bank is now based on the product of these vectors.

$$\prod \sqrt[3]{\ } r_i^3 \ . \sqrt[3]{\ } f(x_i\ ,\ y_i)$$

as before the consumer can remove r which Chaum refers to as a blinding factor (i.e. the anonymity factor).

When the consumer comes to spend the signature in the shop the retailer issues a random challenge vector [c_i] for each value of i. The response from the consumer is as follows,

If $c_i = 0$ send a_i and y_i
If $c_i = 1$ send x_i and $a_i \oplus ID$

This enables the retailer to check the signature and the correspondence of the responses. All the information including the responses are sent to the bank by the retailer in order to claim his payment.

Now lets look at what happens if the consumer tries to spend the signature twice. The next retailer will issue another random challenge vector and statistically we may expect that at least one of the challenge vector elements c_i will be complimentary. This means that when the bank receives the duplicate signature it will also have the responses from both transactions and for at least one case will have both a_i and $a_i \oplus ID$. This will enable the bank to recover ID the consumers account number. In the full method additional random numbers and checks are made to stop the consumer cheating the bank on it's ID when the signature is first created.

There is another little problem with the method proposed so far. We have always assumed that the payment signature is for a $1 bill. In practice of course we need total flexibility on payment value. Well, the solution here is analogous to that above for revealing the account identity. In this case the challenge vector includes a representation for the value of the transaction. There is however a practical complication in that the initial signature generated by the bank needs to be based on a maximum value for that signature. If the consumer account is debited for that full amount then a reconciliation process will need to take place when the signature (with its lower value) is presented by the retailer to the bank. The whole process of anonymity will be spoilt if this took place on an individual signature basis.

The solution proposed by Chaum is for the consumer to obtain sets of checks from the bank so that the refund mechanism operates against the whole set. By this means the bank will be unaware of the amounts for the individual transactions. In order for this to work the bank's signature process operates with two signature moduli which enables the necessary blinding to take place.

We have gone all the way through this part of the tutorial without mentioning Smart Cards. Although we have never said so we have of course assumed that the consumer undertakes all the operations described here using a Smart Card which is his payment token. An interesting point to note about Chaum's method relates to the security requirements for the Smart Card. The only secret key operation is that undertaken by the bank and as such the bank cannot be defrauded because it will only pay on each signature once. The main security risk therefore relates to the use of duplicate signatures which in it self is not totally dependant on the security of the Smart Card. Under these conditions the vulnerable party is the retailer who needs to be assured that he is receiving the authentic signature. In his papers Chaum has proposed that for high value payments the retailer could phone the bank for signature authorisation.

David Everett

Next month - Smart Cards and cryptographic key management.

Smart Ticket for London Buses

Public interest in the contactless Smart Card ticketing system trial on London buses has surprised even London Transport's project team. As soon as the Smart Photocards were available, passengers queued for between 30 and 45 minutes to be among the first to have the new cards, and by the end of the week 3,000 had been issued.

The project, called BEST (Bus Electronic Smartcard Ticketing), is the largest public trial so far of a Smart card system for automatic fare collection.

If all goes well, the scheme will be expanded to all the capital's bus fleets. It could also be adopted by London Underground, and eventually by British Rail.

The trial, in the Harrow area of London, was launched last month by Steven Norris, the Minister for Transport, and will involve 200 buses on 19 bus routes operated by five bus companies.

Initially the Smart Cards are being issued as Smart Photocards which will be used along with their magnetic travel passes. It is necessary to retain the magnetic ticket for visual checking throughout LT's bus and tube network and for use at the entrance gates at London Underground stations.

Later a Farecard will be introduced for use only on the bus routes involved in the trial. The Farecard will act as a stored value ticket, holding a sum of money which can be used as and when the passenger requires.

---

subscription at any time then we will refund all unmailed issues.

The cards will be transferable between passengers but may only be used by one passenger at a time. Farecards will be sold for an initial value of £10, and the card can be "topped up" at newsagents in the Harrow area or on the bus. When it is "topped up" each £5 paid will provide £6 of travel value giving a 20% discount.

AES Scanpoint are supplying primary card readers with secondary readers for some buses to allow two stream boarding. They are also developing an exit card reader for recording cards

as passengers leave the bus. GEC Card Technology are supplying the contactless Smart Cards and components for incorporation into AES Scanpoint and Westinghouse Cubic Card readers.

Westinghouse are supplying card readers which will read both the GEC Smart Card and their own "Go Card" together with additional equipment for London Underground booking offices which will update an existing Smart Photocard when a new Travelcard or Bus Pass is purchased.

Wayfarer Transit Systems have developed modifications to the existing Wayfarer II ticket system used throughout London's bus network. Further contracts have been let to HMSO and to Nibbles Systems for an imaging system, the equipment with which to encode Smart Cards on issue, and printed overlays for the front and back of the cards.

Contact: Roger Torode, Project Leader, BEST - Tel: +44 (0)71 918 4123.