Gaudi Multiservice Smart Card Trials in Dublin

Dublin is carrying out a multiservice Smart Card trial within the Gaudi project, the largest project of the European Commission funded Drive programme.

Called DASH, the three-month trial will examine the idea of using one Smart Card to pay for a variety of services - in this case to pay for bus journeys, toll charges, parking and making telephone calls.

Continued on page 23

Smart Card News

Editor: Jack Smith

Technical Advisor: Dr David B Everett

Editorial Consultants:

Dr Donald W Davies, CBE FRS
Independent Security Consultant

Peter Hawkes,
Principal Executive
Electronics & Information Technology Division
British Technology Group Ltd

Chris Jarman
Managing Director
Orga Card Systems (UK) Ltd

Published monthly by:

Smart Card News Ltd
PO Box 1383, Rottingdean
Brighton, BN2 8WX, England
Tel: +44-(0)273-302503
Fax: +44-(0)273-300991

ISSN: 0967-196X

Next Month

Smart Card Tutorial Part 19 - Anonymous Payment Schemes.

CONTENTS

Multiservice Card Trials

Continued from page 21

The Gaudi (Generalised and Advanced Urban Debiting Innovations) project in Dublin examines the use of a contact Smart Card to access and pay for a variety of city public services.

A total of 2,000 cards will be issued. The 2K bytes EEPROM Smart Cards and readers have been supplied by Schlumberger Technologies, France.

Taking part in the trial are:

* Dublin Bus who are providing DASH services on one bus route;
* Telecom Eireann, who are providing 20 phones adjacent to the bus route;
* Irish Car Parks with 500 parking spaces available in the city centre car park; and
* National Toll Roads, who operate a toll bridge in the western suburbs.

These service providers are mutually independent and do not have any commercial relationship.

Brendan Flynn, Gaudi Project Manager, Dublin Bus, said that in addition to these independent applications there is an Electronic Purse implemented on the card. This (a single common electronic purse which is available to all services), represents a payment means which is accepted for payment by all the service providers.

The DASH card can be used to store weekly or monthly season tickets on the Dublin Bus route, and can also be used to pay for individual bus journeys, with the fare being deducted from the electronic purse.

The card can store phone call units which are deducted as the call progresses as with existing telephone chip cards. However, if there are no call units left on the card, then the electronic purse will be accessed and decremented by the monetary value of call units.

In paying for tolls, the cardholder will hand over the card to the cashier in the toll booth who, using a handheld card reader, will deduct the appropriate toll from the electronic purse.

A 12-week season ticket for parking can be stored on the card which is checked for validity on entering and leaving the car park. Alternatively DASH cardholders who are only occasional car park users can pay the parking fee from the electronic purse.

The cards are rechargeable at a number of point of sale outlets for reloading the electronic purse, telephone units and season tickets.

A further five European cities are taking part in the Gaudi project - Barcelona, Bologna, Marseille, Rome and Trondheim - with each of them concentrating on a different aspect of the problem of traffic demand management in urban areas.

Different technologies are being tested in the various cities. The project in Marseille, for example, is developing a "hands free" ticketing system in which the customer has a handheld transponder-type device into which is inserted a contact Smart Card which communicates with a validator at a distance of a few metres.

Unlike conventional proximity contactless cards, the customer initiates the transaction by pressing a button on the unit.

Contact: Brendan Flynn, Project Manger, Dublin Bus - Tel: +353 1 703 3049.

US^3/GIS Collaboration

US card manufacture, US^3, and General Information Systems (GIS) have announced a collaboration agreement on Smart Cards under which GIS will provide applications development and technical support for US^3 products throughout Europe; and US^3 will support the GIS OSCAR operating system in its product range.

GIS will offer volume production facilities in the Far East for rapid product delivery and the two companies will work together in the development of future silicon along with the operating system required, to meet emerging international standards.

Contact: Marcus Hodge, Product Marketing, US^3 - Tel: +1 408 748 7725. Fax: +1 408 748 7724.

TV Licence Savings Card

BBC TV are piloting a Smart Card system which it is hoped will make paying for a TV licence easier for people on low incomes and reduce losses through licence evasion.

The trial is a joint initiative between the BBC and British Gas whose Quantum metering system is to be installed nationwide. Customers will be able to put value on their Smart Cards at 11 participating newsagents in the White City area of London instead of purchasing licence stamps at a Post Office.

Currently the BBC have 20.2 million TV licence holders who pay a fee of £83 a year, rising to £84.50 a year from 1 April.

The pilot scheme is aimed at providing a flexible cash method of payment primarily for people on low incomes who may not have a bank account.

Customers can load value onto the card at the participating newsagents and check on the value held in the card by inserting it into a card reader.

Eventually cardholders will be able to pay their licenses at Post Offices by inserting the card in a reader and having the fee deducted. During the pilot scheme, however, the licence authority will inform cardholders when they have enough value on the card to pay for a licence and ask them to post the card to them so that the amount can be deducted.

New Santal Health Card

The new Santal Health Card, shown on page 21, is the SX 8K bytes EEPROM card from French manufacturer, Solaic (SCN October 1993).

The Santal project began in 1988 and 36,000 Smart Cards (Bull CP8 8K bytes EEPROM cards were used in the first phase) have been issued in the Saint-Nazaire health district of France. It is planned to issue 60,000-100,000 of the new cards during the second phase period 1994-96.

Contact: Philippe Cirre, Centre Hospitalier St Nazaire, France - Tel: +33 40 90 60 11.

ORGA Appointments

Dr Lutz Martiny has been appointed Managing Director of ORGA Kartensysteme GmbH, based in Paderborn, Germany. Previously he was Managing Director of GAO (Gesellschaft fur Automation und Organisation) in Munich.

Paul Hill has been appointed Managing Director of ORGA Card Systems (UK) where he was previously Marketing Director. He succeeds Chris Jarman who has been appointed Vice President, Corporate Strategy & International Business Development, in the parent company ORGA Kartensysteme GmbH.

The moves come in a strategic reorganisation which has included acquisition of the remaining shares in ORGA UK.

ORGA's card sales in 1993 were 1.6 million microprocessor cards, mainly as Subscriber Identity Modules (SIMs) for GSM, the Global System for Mobile Communications; and 3.7 million memory cards mainly for the payphone and health care markets. Turnover in 1993 was DM47 million.

ORGA holding companies are UNIQA Chipkartensysteme GmbH (74.9%) and DETECON Deutsche Telepost Consulting GmbH (25.1%). UNIQA is owned jointly by PREUSSAG and BUNDESDRUCKEREI.

Contact: Paul Hill, Managing Director, ORGA UK - Tel: +44 (0)491 410997.

DataCard 9000 Enhancement

DataCard has announced the enhanced capability of its 9000 Series card personalization system to initialise Smart Cards at the same time that the card is encoded, embossed or graphically printed. The company says that initialization can take place at a rate of 700 cards per hour.

The DataCard 9000 is in use in major banks in Europe and was chosen by SIBS to personalise cards for the Portuguese Electronic Purse scheme.

Contact: Cheng B. Choo, DataCard, England - Tel: +44 (0)705 486444.

LORETA Changes to Mag Stripe

PHH Vehicle Management Services has announced that following a review of the technology used in its LORETA local garage account system in the UK it will be replacing its current Smart Card with a magnetic strip card.

LORETA (LOcal RETail Account) was developed using an 8K byte EPROM chip and there are now around 15,000 Smart Cards in use.

The scheme was launched in October 1990, and in 1992 was reported to be billing over £1 million a month with expansion plans. The Smart Card was seen as a key element in minimising the company's exposure to bad debt.

Godfrey Larque, Vice President, Network Services, commented: "Initially Smart Cards appeared to offer definite advantages in the field of garage local account card packages. On the other hand, magnetic strip cards are more readily accepted at the point of sale and PHH has continued investment in state-of-the art processing systems to increase their suitability in the local account arena.

"We have now reached a stage where the best opportunity for taking LORETA forward is in magnetic strip form. We are therefore directing current investment in this direction and will introduce a new magnetic strip version in 1994."

The Smart Card version of LORETA was developed jointly by PHH and Schlumberger Technologies, France.

Contact: Brecon Quaddy, PHH Vehicle Management Services, England - Tel: +44 (0)793 884544.

Phonecard Orders for Solaic

Solaic, the Smart Card manufacturing arm of Sligos, France, has won orders in two countries in South America for Smart Cards to be used in public phones.

They are to supply CAN-TV, the local telecommunications operator in Venezuela with five million cards.

Last month, Solaic supplied 250,000 cards to Tele-2000 in Peru.

The phonecards in both orders are memory cards with an SGS-Thomson 1305 chip.

Solaic is a major supplier of phonecards and has won orders in most countries in Europe. These are the first orders obtained outside of Europe.

Contact: Charles Juster, Communication Manager, Solaic, France - Tel: +33 1 49 00 96 33.

Wegener/News Datacom Deal

Wegener Communications, a subsidiary of Wegener Corporation based in Atlanta, Georgia, USA, has announced an agreement with News Datacom to jointly develop and market encrypted transmission systems based on Smart Cards.

News Datacom provides conditional access and subscriber management systems for pay-TV operations around the world, including BSkyB in the UK, while Wegener Communications designs and manufactures audio, data, and video transmission products and systems for satellite and terrestrial networks.

Contacts: Ken Leffingwell, Wegener Communications, USA - Tel: +1 404 623 0096. Valerie Gopthal, News Datacom, UK - Tel: +44 (0)628 74774.

New Publication

The Advanced Card Report: Product & Services Directory, published by The Schuler Consultancy, USA, price US $179 (international US $189), offers a quarterly update service for US $119 (international US $149) per annum.

A guide to companies in the advanced card industry, particularly Smart Cards, it has fact sheets on over 65 companies with cross-reference tables to locate companies by products, services, applications and industries served.

Contact: The Schuler Consultancy - Tel/Fax: +1 301 869 6920.

First Smart Card in Thailand

The Thai Farmers Bank (TFB) has issued the first Smart Card in Thailand with a first phase target of issuing 20,000 cards and installing 200 readers by mid-1994. The eventual plan is to extend the scheme and target some 300,000 users nationwide.

Called the TFB Smart Card, is was developed by the Bank and local information technology company, Loxley Business Information Technology Co. (LOXBIT), as a new version of the Bank's credit card.

The multi-use card has four initial functions - SmartCash to provide an alternative means of payment for small cash transactions and establish the prototype of the electronic purse concept; Smart ID to alternatively authenticate the cardholder in case of a large withdrawal from his or her TFB account; Bonus Points providing instant bonus for TFB credit used for cardholders and create frequent shopper and loyalty programmes for participating retail and service providers; and Medical records where data is stored in the card for use in case of emergency. It can also provide supporting data on visits to participating hospitals.

The system uses Gemplus PCOS (Payment Chip Operating System) microprocessor cards and VeriFone CM450 readers and terminals.

Contact: Natalie Leerapun, Loxley Business Information Technology Co., Thailand - Tel: +662 201 3104. Fax: +662 201 3108.

BSkyB Using 3.25m Smart Cards

British Sky Broadcasting (BSkyB), the UK-based satellite broadcasting company, has announced profits of £84.8 million for the half-year ending 31 December 1993.

The growth in operating profits was primarily the result of a substantial increase in subscribers. The success of the Sky Movies Channel and the launch last September of the Sky Multi-Channels Package increased the number of paying subscribers by 900,000 over the six-month period to reach 3.25 million.

As each subscriber uses a Smart Card for descrambling the picture, this means that BSkyB is maintaining its lead as the biggest user of Smart Cards in the UK.

BSkyB use the VidioCrypt encryption system developed by News Datacom and Thomson Consumer Electronics.

AT&T Restructures Card Division

AT&T has restructured its Smart Card operations, elevating its business from an internal "venture" to a division in its own right of AT&T Consumer Products.

The Smart Card unit was created in 1991 and, under its President, Diane Wetherington, established itself as a leading supplier of contactless Smart Card systems.

It was successful, for example, in automatic road tolling systems using contactless Smart Cards, and recently announced an alliance with Chemical Bank to conduct trials of a Smart banking and stored-value card in New York City during 1994.

Carl Ledbetter, President of AT&T Consumer Products, said: "This move reflects the success of the venture and the readiness of the consumer marketplace to accept the convenience of our Smart Card technology in financial transactions and other applications, including campus environments, transportation and the health care industry.

"As part of a larger business unit, the Smart Cards organisation can take advantage of a larger pool of expertise in the areas of R&D, sales and marketing, and will be backed by the assets of one of AT&T's major divisions."

John Bermingham has been appointed President of AT&T Smart Cards, replacing Diane Wetherington who will now lead another business at AT&T yet to be announced. Bermingham also holds the position of Group Vice President of the Advanced Communications Technologies Group, part of AT&T Consumer Products.

Contact: Michael Jacobs, Communications Manager, AT&T - Tel: +1 908 582 4767.

Electronic Purse Systems

International interest in national Electronic Purse schemes was evident at Smart Card '94 in London this month as delegates from all over the world crowded into the conference room. If the success of the topic can be judged by the number of questions asked by delegates, then this was the highlight of the three-day conference.

As the questions came, mainly on the technical and security issues of the Electronic Purse schemes presented, Day Chairman, Robin Townend, of Barclays Bank, UK, wisely took account of the high level of interest and let the sessions flow on. They over-ran into coffee, lunch and tea breaks, and long after it was supposed to have ended, cleaners and maintenance workers were fretting outside closed doors waiting to get in.

Delegates heard presentations on projects in Denmark, Switzerland, Portugal, South Africa, Finland, France, Belgium and the UK (the Mondex system covered in detail in the December 1993 issue of SCN).

In an opening overview, Mr Townend said it was already difficult to document all EP systems as there were too many of them, but he featured those relating to National Electronic Purse schemes and other major operations of significance.

A noticeable feature, he said, had been that every Electronic Purse scheme had been delayed in its implementation, in consequence there were only four national schemes live at the 1st of January this year - in Denmark, Finland, Switzerland and Taiwan. The table below sets out the current position.

National Electronic Purse Schemes

Country	Scheme Operator	Sector	Status
Australia	NSW Government	Government	Tenders in
Belgium	Banksys	Banking	Planning Trial
Denmark	Danmont	Inter-sector	Roll-out
Finland	Avant	Central Bank	Trials
France	La Poste	PTT	Planning Trial
Germany	GZS	Banking	Spec. Agreed
Latvia	Union Baltic Bank	Banking	Planning Trial
Portugal	SIBS	Banking	Planning Trial
Singapore	NETS	Banking	Trials
South Africa	Inter-bank SCC	Banking	Agreeing Spec.
Spain	SEMP	Banking	Trials
Switzerland	Swiss PTT	PTT	Planning roll-out
Taiwan	FISC	Government	Roll-out
UK	Mondex UK	Banking	Planning Trial
USA	Inter-bank SCC	Banking	Planning Trial

Other countries considering EP implementation include Brazil, Bulgaria, Canada, Indonesia, Korea, Lebanon, Poland, and Thailand.

A conclusion was that there was no standard approach and therefore no unique blue print for either the business case or the implementation. Issues would vary from one approach to another, even in the same country as issuers all started from a different perspective.

Although the commercial banks appeared to have grasped the initiative, other industry sectors saw opportunities too, he said. This might cause pre-emptive responses from the central banks to regulate the operators thereby ensuring tighter control through licensing and closer monitoring of the impact of EPs on the money supply. Such action should also ensure proper consumer protection.

Multibanco Electronic Purse

Portugal's Multibanco Electronic Purse (MEP) service called Porta Moedas Multibanco will be launched in Lisbon in April this year.

The scheme is being developed and will be operated by SIBS (Sociedade Interbancaria de Servicos) on behalf of its 30 shareholder banks in Portugal.

SIBS investment for the launch of MEP are around 6 million ECU covering:

* A major ATM network upgrade
* 200,000 MEP cards
* 5,000 Deposit cards
* 500 standalone EFTPOS and 300 portable MEP-only terminals
* 200 electronic cash registers and diversified self-service vending machines
* Card personalisation equipment.

The service will be launched with an anonymous MEP card that emulates cash as closely as possible, but a dual card (Bank credit/debit card with an MEP) may be introduced in 1995.

The Smart Cards have been selected from existing IC cards. The MEP card is the PCOS 1K byte EEPROM rechargeable Smart Card from Gemplus. It is planned to launch with 5,000 cards and have 200,000 cards issued within six months.

The retailer Deposit card, which enables merchants to capture the "electronic safes" from the terminals and to deposit them in the bank using an ATM or a terminal with on-line capabilities, will be the SX card from Solaic which has 3K bytes of EEPROM. SIBS have ordered 5,000 Deposit cards.

Finnish Avant Card

Finland's national Electronic Purse system is called Avant and has been developed by Setec Oy, the Bank of Finland's security printing house. Another Finnish company, Toimiraha, has the responsibility of commercialising the system.

There are two types of Avant cards. One is the disposable value card which is loaded with a fixed amount of purchasing value and used in public phones. The number of these cards in use is expected to grow to 480,000 next year. The other type is a reloadable card which is the future Avant payment medium. It is estimated that 36,000 of these will be in circulation at the end of this year.

The Avant system has already been introduced in public phones and in the parking system of the city of Helsinki. The next large use area is public transport.

Mr Olli Harjama, of Toimiraha, said it is estimated that pre-paid cards will amount to FIM 5.6 billion in seven years, which is a third of small payments. The number of Avant electronic purses is estimated to be 1.5 million.

"The Avant system will succeed," he said, "because it is open to everyone. There is no need for overlapping investment. The cost of payment is minimised. One card valid for payment everywhere is more convenient than a card jungle.

"The Avant card is also safe and it respects the individual's privacy. This feature is especially appreciated by the Finnish consumer."

Inter-bank EP in South Africa

The four major banking groups in South Africa - ABSA, FNB, Nedcor and Standard Bank - will pilot an inter-bank Electronic Purse project starting in July. The pilot will run for six months in one shopping complex close to Johannesburg.

Cedric Edwards, Senior Manager Smart Card Projects, at First National Bank of South Africa, said that the success of banks in the "New South Africa" will depend on their ability to change. Traditional markets are stagnating, and new, emerging markets require new products and marketing strategies.

"My own Bank has cash dispensers on the back of 4-wheel drive vehicles which are used to pay wages and pensions in remote areas of the country using fingerprints as identification," he said. "We are also experimenting with voice recognition as an alternative."

At present very few black people qualify for a credit card because of low income. They make the majority of their payments by cash, whether they be for clothing, groceries, household goods or rent. Muggings on trains, in townships and even at ATM's are common and there is a requirement for a means to replace all cash transactions.

Mr Edwards said that the banks participating in the pilot will issue a minimum number of cards to customers at their local branches and upgrade existing point of sale terminals to accept the cards.

Gemplus, with their South African agents, Net 1, developed the application on behalf of the banks, and the test will use Gemplus cards containing ST16623 microprocessors.

Mr Edwards said that the plan is to have the application masked onto chips from at least two manufacturers. The application has been written to fit on a card with 4K bytes of ROM and 1K bytes of EEPROM and after the trial each bank will be free to order from the supplier of their choice.

The intention is to roll-out the products to the rest of the country early in 1995 as terminals, ATM's and branch equipment was upgraded.

"Ultimately," he said, "all ATM cards could be replaced by Smart Cards. Card numbers could therefore reach 15 million. We expect the eventual number of point of sale terminals to be in the region of 100,000."

Two products will be piloted - A debit card, the transactions on which will be processed against a cheque account; and an Electronic Purse with PIN protection. Both cards will contain a non-protected purse for low value transactions.

The Electronic Purse is the product that the majority of the banks' customers will be offered. Cardholders will be able to load value onto a card from any existing bank account through an ATM or self-service device or with cash through a branch teller.

Provision has been made to share cards with other applications, the first to be accommodated will be the pre-payment of electricity

Belgian Inter-sector EP

In Belgium, Banksys with a national network delivering ATM and EFTPOS services, is to trial an Intersector Electronic Purse (IEP) in two medium-sized towns at the end of this year.

The IEP is intended to be accepted for a wide variety of activities as well as in small retail outlets (newsagents, grocery and bakers shops), in vending machines (drinks, snacks, tickets, parking meters and "pay and display"), payphones and various mobile activities such as taxis and home deliveries.

The card will be an ICC card and a PIN will not be required for purchase transactions. The card will be reloadable at ATMs.

Critical success factors are seen as: purse holder readiness to use the IEP, extensive and early contact with service providers and suppliers of vending machines, the right product concept and marketing as a petty cash replacement, and willingness by card issuers and purse providers to penetrate the market rapidly in a joint approach that is both card and terminal driven.

Japan Rail Contactless Trial

Japan Rail is to trial the Sony FeliCa Remote Card System in transportation ticketing in Tokyo with about 400 employees who will be issued with contactless Smart Cards.

Sony makes the point that the card was not adapted for use as a transportation ticket but was specifically designed for this application and embodies the characteristics demanded by rail, bus and other transportation service providers of user friendliness at an affordable price, achieved by combining very high-speed data transfer rates, variable target-to-card communication distances and ample memory capacity on an ISO-size card.

The cards, distributed by Mitsubishi Corporation, will be used in automatic gate machines which offer a card touch and go function or can read the cards at a distance of up to 50 cms.

The system consists of a reader/writer unit and the Sony Remote Card. Main characteristics of the card are as follows:

* ISO standard size (84.5 x 54 x 0.76mm)
* 2K byte memory
* Hard logic on ASIC
* Battery powered (minimum three-year life)
* Compatible with both 30 MHz or 2.4 GHz reader/writer
* Communication distance up to 100mm with 30 MHz reader/writer
* Communication distance up to 500mm with 2.4 GHz reader/writer
* Transaction time under 100 ms (including error correction)

Sony used several new technical solutions in developing the system including proprietary technologies for the processing of 2.45 GHz signal using CMOS, production of cards (including battery components) using a film lamination process, bonding of the bare IC directly onto the film, and a modulation method for achieving high speed data transfer rates.

The system will be marketed internationally in co-operation with Japan's leading trading company, Mitsubishi Corporation

Contact: Yoshitaka Kurauchi, Manager, Card Systems Development Dept., Sony, Japan - Tel: +81 3 5448 6832.

Hands Free Access Control

Another system using contactless Smart Card technology is the CassaNova system from ELIS, of Austria, shown below in use as a ski pass. The Smart ticket is carried in the skier's sleeve pocket and is read by the proximity reader.

Contact: Doris Bednar, ELIS Identifikations-systeme, Austria - Tel: +43 1 89 100 3954.

Mini MelCard from Mitsubishi

Mitsubishi has launched a new half-size contactless IC card designed specifically for convenience to the user and to provide fast, easy and reliable access control to mass user systems.

At half the size and double the thickness of Mitsubishi's credit card-sized version, the new contactless MelCard measures 43mm x 54mm x 5mm. Built to withstand daily wear and tear, it is easily converted, for example, into a key fob.

It is envisaged that the card will be used in ticketing systems, automatic warehousing and even production control.

The card operates at communication distances of up to 800mm and a typical operation takes less than 0.2s. It features a single chip microcontroller and communicates with the reader/writer via half duplex amplitude shift keying transmission. The 8bit microcontroller makes for wide-ranging application functions and high security whilst at the same time using little power.

Contactless Card Development Kit

Mitsubishi are also offering the Mitsubishi MelCard contactless card development kit for the evaluation and development of contactless IC card applications for access control systems.

The PC-based kit costs £799 and comprises the MelStar 100 contactless transceiver unit, three MelCard contactless IC cards, software, instruction manual, AC adaptor and cables.

The software provides step-by-step project development and evaluation and the MelStar 100 transceiver provides fast card reading and system access/operation at distances up to 14cms. It operates from 220/240V supplies.

Contact: James Pemberton, Smart Card Product Manager, Mitsubishi Electric UK - Tel: +44 (0)707 276100. Fax: +44 (0)707 278625.

Third Generation Card for BT

British Telecommunications company, BT, whose move into disposable Smart Payphone cards was announced in SCN last month, have revealed further details of their requirements now that tenders have been submitted from a number of consortia.

The new cards, to be introduced in 1995, will be a "Third Generation" concept to take BT into the 21st century, said Michael Meyerstein, BT, Development & Procurement, speaking at Smart Card '94, in London this month.

Key requirements are that the cards can be used for more that one pre-payment application and capable of international acceptance in payphones with a migration path towards multi-application and electronic purse functions.

BT, for commercial reasons, was less forthcoming about value-added services which will become available via the phonecard. Mr Meyerstein said: "In the near future, BT's customers will benefit from our Smart Card strategy by being able to access a host of new services available over our network both in payphones, in the home and in the office.

"The ability of Mondex Smart Cards to provide 'cash' transfers over the telephone is a good example of this. Smart Cards also have the potential to become a universal access mechanism to telecomms services, thereby bringing in the era of Personal Numbering and Universal Personal Telecomms (i.e. the merging of mobile and fixed network services).

He also quoted Bruce Bond, Director of BT's Products and Services Management division as saying: "BT believes that Smart Cards will play a key role in providing new and innovative services."

Third Generation concept

France Telecom and Deutsche Bundespost Telekom have announced, at separate meetings, a new type of disposable IC telephone card, called the "Third Generation" concept which is capable of meeting all of BT's requirements, he said.

Third Generation is basically an EEPROM telephone card IC (i.e. it has a counting capacity of many thousands of units) with the addition of active cryptographic authentication and extra, user-definable, memory.

All Third Generation designs have the following features in common:

* Security logic to control read/write memory access, counter operation and addressing of memory.

* First 104 memory addresses compatible with today's EEPROM cards (i.e. 64 bits IC/card ID, 1 bit personalisation flag, 39 bits secure EEPROM counter).

* Cryptographic process to authenticate the card and to protect the decrementing operations. The process uses hard-wired one-way crypto function and stored secret key.

* Extra, protected memory for the storage of user-data for future applications.

The Third Generation concept was developed by European PTOs, card suppliers and IC manufacturers. The idea is to have a card which is sufficiently secure and has enough features for it to be used by all European PTOs. This concept would produce lower card prices and pave the way to inter-operability.

At least two different designs are currently vying for the title of Third Generation. These have been announced to European PTOs by France Telecom in Paris and Deutsche Bundespost Telekom in Munich, using ICs produced by SGS-Thomson and Siemens, respectively.

Authentication

All Third Generation designs use the principle of a crypto function which is embedded in the hardware of the IC, coupled with a unique secret key which is put into the card as part of the personalisation process.

The card is authenticated by a security module, which in BT's case will be in the payphone, which presents it with a random-number

"challenge." The card uses its crypto capability to transform the challenge into a "response." The security module checks to see if the response is correct.

Calculating the response requires use of the card's unique secret key, but this can be used only by the card's internal logic and cannot be read by the payphone. Therefore, the security module has to synthesise the card's secret key using the same process as was used during personalisation of the card.

Inter-operability

Deutsche Bundespost Telekom and the Netherlands PTT have recently announced a scheme to use the same card type, initially a 104-bit EEPROM device but migrating to the Third Generation solution soon.

France Telecom is trialling an advanced EEPROM card (called the T2G) and is expected to go over to a true Third Generation soon. DBT and FT have announced that they will achieve inter-operability of Third Generation cards by 1996.

The various Third Generation designs are not fully compatible in that they use different crypto functions and key lengths and different methods of presenting the response.

Inter-operability and multi-sourcing might therefore require the BT payphone to be able to recognise these different types and to invoke the appropriate suite of software. The security module might likewise have to be capable of running different crypto functions for key-generation and authentication. The sharing of secret data between different payphone operating companies in a deregulated international market is an issue which needs to be resolved.

User benefits

Potential benefits of disposable IC cards to BT's customers are: Pan-European use of BT phonecards, applications using the extra memory, greater collectability of cards due to better graphics, greater availability of payphones due to improved reliability, and access to a wide range of services from payphones.

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.

Corporate Identity for Fortronic

Fortronic, the Scottish-based supplier of Smart Card systems and terminals, has assumed the corporate identity of its parent company De La Rue and is now known as De La Rue Fortronic. De La Rue is also a joint venture partner with French Smart Card manufacturer, TRT-Philips, in Delphic Card Systems, based in England.

Smart Card Tutorial - Part 18

Security and the Electronic Purse

There are now a large number of national electronic purse initiatives and it's probably true to say that no two schemes are the same. The basic principles are however common and at this stage we will attempt to determine the core security requirements and see how they may be achieved. For our purpose we will take the simplest model shown in fig.1.

The model just shows the three principle participants, the purse provider, the purse holder and the service provider. These are the primary commercial entities involved in an electronic purse system and in each case a security module is used to effect the necessary transactions. By convention we will refer to the security modules of the purse provider and service provider as SAMs (Secure Application Modules). The purse holder's purse by definition forms the other security module.

There are three relationships by which electronic value may be manipulated in the system,

* Purse provider - purse holder
* Purse holder - service provider
* Service provider - purse provider

Accordingly the core function of the electronic purse scheme is to provide transactions that allow electronic value to be transferred amongst the participants. These transactions may be different for each relationship or could in principle be the same. It is the commercial relationship that defines what may or may not be allowed.

The primary security requirement is obvious but none the less leads to a fundamental determination of the security architecture,

Requirement (1) - value conservation

Value shall not be created or destroyed except in an authorised fashion.

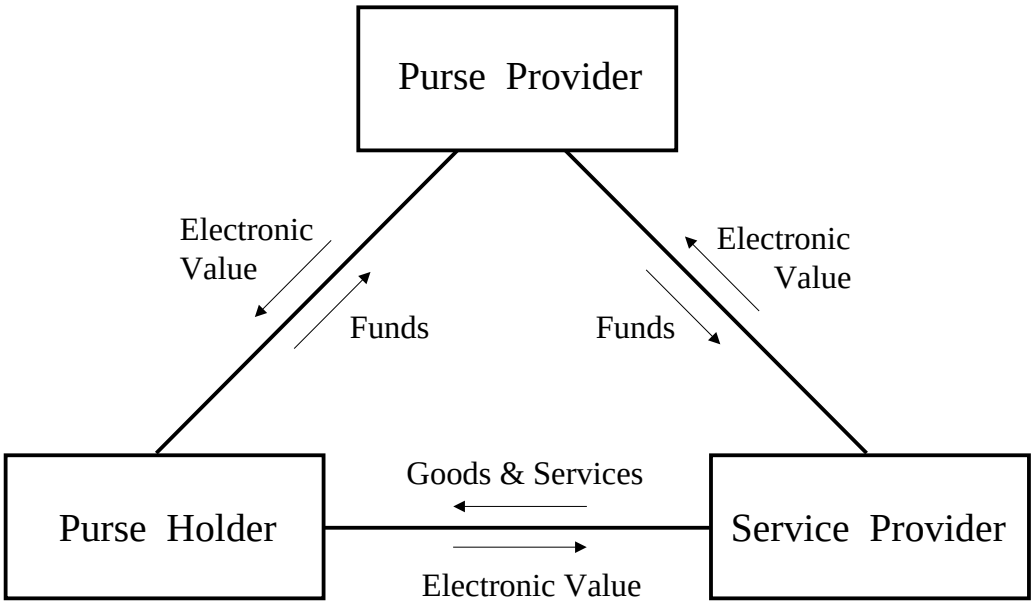

Fig. 1. The Basic Purse Model

Clearly in this basic model only the purse provider is authorised to create and destroy value. If either of the other participants can create value then we are faced with a fraud scenario. If value is destroyed then one or more of the participants will suffer an economic loss. We can rewrite the basic commercial model by using its technical components as shown in fig. 2. This enables us to write the requirements necessary for value conservation.

a) The data integrity of the value stores must be preserved

b) The value transfer protocol must maintain value equilibrium (i.e total value before a transaction must equal total value after the transaction).

In a real environment neither of these conditions can be guaranteed. Components in the system may fail leading to a breach in either requirement. Clearly such failure must be minimised and in so far as is possible recovery mechanisms must be capable of resolving such problems.

Integrity of the value stores

However the purses and SAMs are designed it is clear that the value store will be implemented by some form of non volatile memory. In practice this will almost certainly be EEPROM memory. There are two principle technologies used for EEPROM, Flotox and MNOS. Both of these technologies can fail albeit by different mechanisms. All EEPROM technologies have an

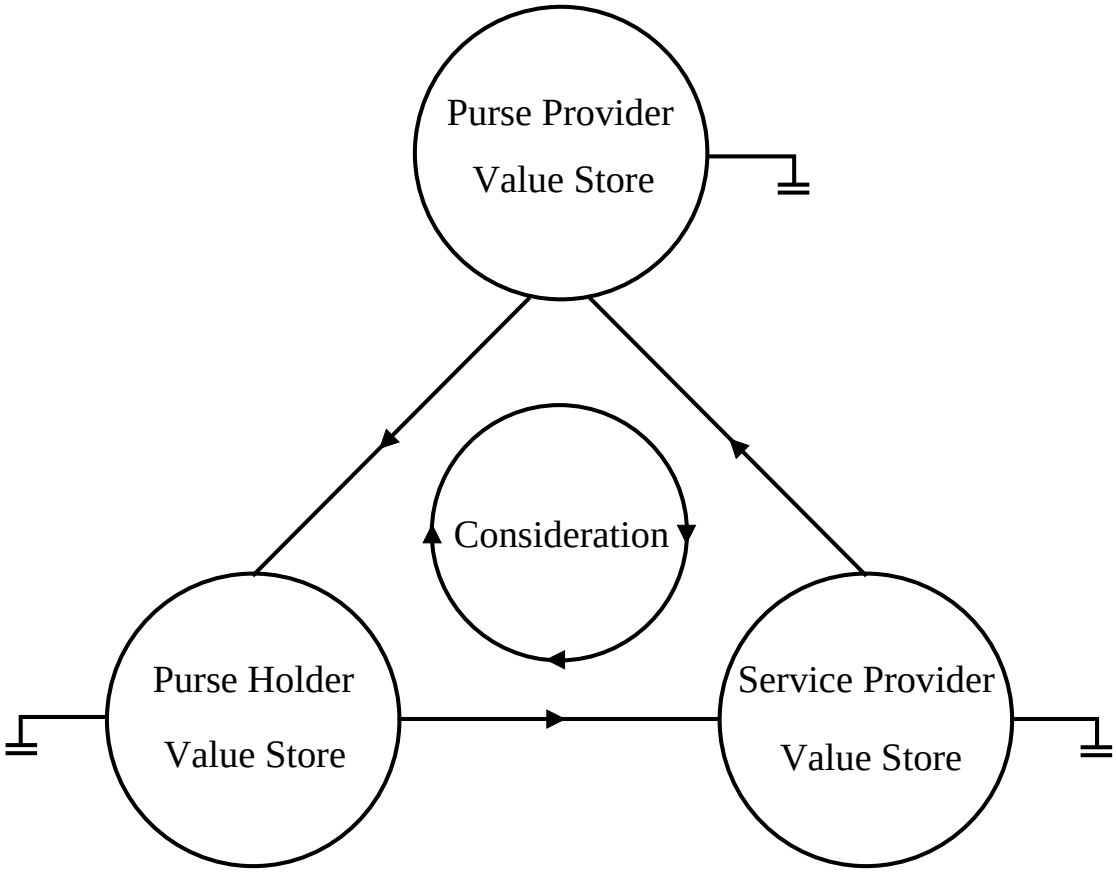

Fig. 2. Electronic Value Component Model

endurance capacity which is quoted by the manufacturers and is typically in the region 10^4 - 10^5 write cycles. Although this may seem adequate a busy service provider could invoke a thousand transactions per day. Assuming that the relevant data memory is only written once per value transfer we are still faced with a SAM life of 10 days if we take the lower of the range quoted above. Regardless of the design invoked for memory usage we must still allow for failure and it is clear that some form of data integrity function is necessary. Some implementors routinely use a four bit ECC (Error Correcting Code) for each byte of EEPROM memory. There are other possibilities such as the maintenance of mirror data images. So far we have considered failure conditions but quite clearly it is necessary to be assured that it is not possible to alter the content of the value store by unauthorized means. It would be quite horrendous if users could alter the content of this store by subjecting them to some form of external radiation. Similarly one must be assured that the integrity of data is preserved within the actual mechanism of the EEPROM write cycle. In an earlier part of the tutorial we explained in more detail the operation of such memories.

Value Transfer Protocol

The process of transferring value between the secure stores has been the subject of extensive academic research. There are a large number of options but most are based on the same security principles. The differences are in the cryptographic mechanisms used to achieve the necessary security services. The first requirement operates at a high level but is necessary to prevent potential fraud scenarios,

* The payer store must be decremented in value before the payee store is incremented in value.

Whilst the successful achievement of this requirement is necessary for value equilibrium (the converse is equivalent to unauthorized value creation) it leads to a number of value loss conditions in the event of some failure in the execution of the value transfer protocol. Accordingly the protocol needs sufficient auditability to enable recovery mechanisms to take place in the event of some failure.

The next three requirements are found in any electronic payment system,

* Entity authentication must be adequately assured
* Data integrity must be adequately assured
* Message replays must be prevented

We have defined that the value transfer protocol operates between two secure stores of value. Then in our simple model the fundamental payment mechanisms is made between the user's purse and the service provider's SAM. Thus the first requirement leads to mechanisms whereby the purse can authenticate the SAM and for the SAM to authenticate the purse. It is clearly mandatory for the SAM to authenticate the purse. The authentication of the SAM by the purse is necessary as part of the proof of payment security service and can prevent mischievous loss of value. A sequence of messages may be established which implements these security services as shown in fig. 3. Three separate phases are shown,

* Entity authentication
* Value payment
* Proof of payment

It is assumed here that the terminal plays no part in the cryptographic security services. Thus the entity authentication mechanism takes place between the purse and the SAM. The value payment transaction also takes place between the purse and the SAM whilst the transaction record proof may optionally be sent from the SAM to the purse. The requirement for this is dependant on the commercial structure of the electronic value scheme. If the individual transactions are not recorded by the terminal then the proof of payment can be completed by passing this message back to the purse. In all cases it is necessary to achieve two additional requirements,

* The purse holder should authorise the transaction.

* The purse holder should be adequately assured of the correctness of the transaction event.

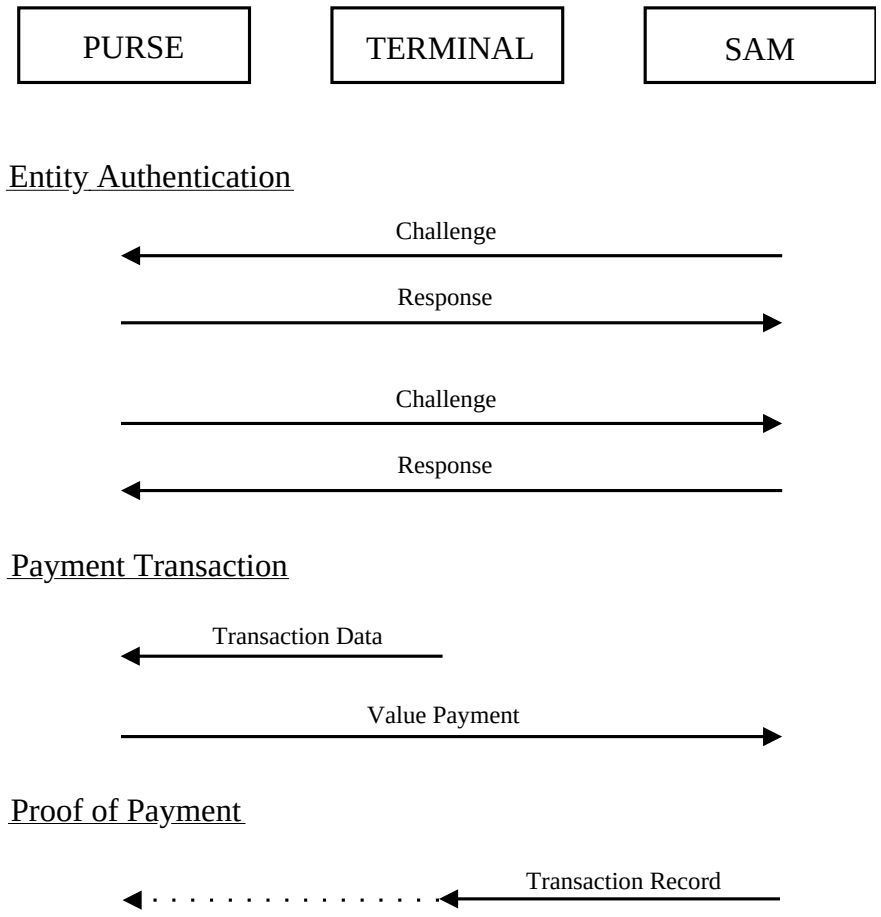

Fig. 3. Standard Payment Transaction

In practice these additional requirements place a security burden on the terminal to adequately allow the purse holder to control the payment transactions. At the very least he should be assured that what he authorises is actually what takes place.

By combining the security mechanisms we can reduce the message set into a generalised protocol as shown in fig.4. Here we have shown three core messages for the value transfer protocol,

* An authentication/transaction challenge
* A value payment / authentication response
* A transaction record

The first two messages are always between the purse and the SAM. The transaction record may be logged by the terminal for reconciliation with the purse provider or may be truncated by the SAM. Optionally the transaction record may be sent to the purse as an acknowledgement message.

Clearly these three messages must be cryptographically protected by some form of digital signature. This may be a true signature using an asymmetric cryptographic algorithm or some form of cryptographic check value using a symmetric algorithm. The important difference here is that in the case of the symmetric algorithm the terminal is unable to verify the

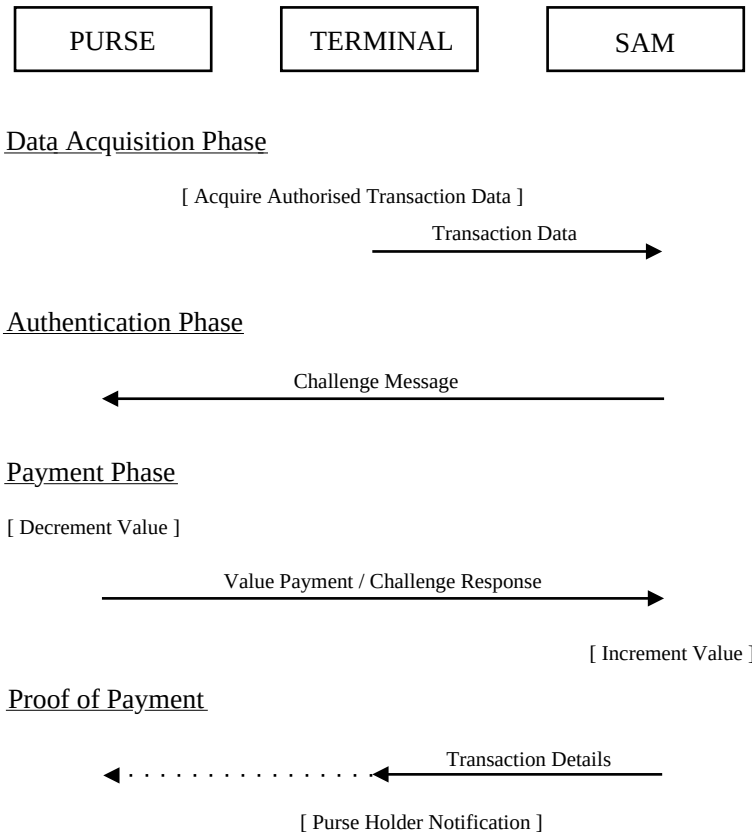

Fig. 4. Combined Authentication / Payment Messages

cryptographic mechanism.

For the value transfer protocol to offer adequate security the following requirements are necessary,

* The challenge message and the value response must be unique to the purse and SAM.

Apart from the transaction data the challenge message should incorporate the unique identities of the SAM and purse and should incorporate a transaction unique sequence number. The value response should incorporate the same data. By such means duplicate payments can be avoided. The transaction data may include information relating to time and date but it would be generally unwise to use such data as part of the security mechanism because of the difficulty of controlling the terminal data. The terminal operator needs to adjust such data for the normal operation of the terminal and therefore cannot be prevented from abusing such data.

David Everett

Next month: Anonymous Payment Schemes.

Card Growth Forecast

The European Smart Card market is expected to generate revenues of $1,343.6 million in the year 2000 - an increase of 20.8% over the 1993 value, according to a new report from international market research publisher Frost & Sullivan. Substantial growth of over 40% is expected for 1994 before the market returns to its long term development pattern after 1995.

Microprocessor cards are identified as the most interesting and active product segment, with estimated revenues of nearly $130 million in 1993. Demand for microprocessor cards is expected to experience significant growth and account for around 28% of total manufacturer revenues by the year 2000.

Assessing application trends, the report estimates that pre-payment cards accounted for more than 80% of total Smart Card shipments in 1993 and predicts that they will remain dominant, although gradually losing their share of the market to cards for banking and personal data storage.

Twelve countries are covered and the report gives France the lead, accounting for nearly half of total market revenues in 1993. Germany, the second largest market, is expected to become the largest market this year, driven by the nationwide health insurance project. The remaining European countries are expected to begin a strong phase of development from 1995 onwards, with the UK and Italy exhibiting above average growth.

Contact: Simon Robinson, Frost & Sullivan, England - Tel: +44 (0)71 730 3438.

Chelmsford Co-op Starcard

A thousand Starcards have now been issued to staff in the Chelmsford Co-operative Retail Society's Smart Card-based loyalty scheme in England.

It is planned to issue 20,000 cards to the existing and active membership of the Society in June this year and to ultimately extend the scheme to about 50,000 members.

The system was designed by the management of the Co-op, Saunders Jeffries who specialise in retail systems development and supply, and the Co-op's resident systems supplier, Piquet Computer Services.

The system supports staff log-on to EPOS systems, staff time and attendance, staff discount management, co-op member dividend management, a savings scheme, and incentive points known as "stars" can be stored in the card memory. Further functions are planned and will be introduced over the next few years.

The system uses VeriFone CM450 Smart Card reader/writer terminals and 2K bytes EEPROM Smart Cards with the Siemens SLE4418 chip.

Contacts: Hugh Garratt, Chief Executive, Chelmsford Star - Tel: +44 (0)245 490 101

Quantum System Progress

British Gas has now installed 115,000 Quantum pre-payment gas meters and envisage the potential installation by 1998 of 1.5 million meters and 6,000 Smart Card charging units as the system expands nationwide.

Smart Phone Pilot in Hanoi

Schlumberger is to pilot its Smart Card-based public payphone system in Hanoi, Vietnam, in competition with a Malaysian company offering a phone system using magnetic stripe cards. Success in the trial, which will run until mid-1994, could lead to a nationwide installation contract.