

BT Tender for Smart Payphones and Cards

BT, the British telecommunications company, has gone out to tender for Smart Card public payphones and disposable Smart Cards.

The specification calls for the use of a chip which enables cryptographic authentication of the card as proof against counterfeiting and fraud.

It is not expected that the new cards will come into general use until some time in 1995.

Continued on page 3

France Telecom presents quality award to Solaic (See page 4)

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 18 - Security and the
Electronic Purse

CONTENTS

Supertag Implications for SCs	3
Smart Power Customer Card	4
Payment Metering Initiative	5
Schlumberger Art Competition	6
Health Cards in Germany	7
SA Interbank Card Standards	8
Telephone Cards in South Africa	9
SIM Portable Examiner	10
Buscom Fare Collection System	11
Gemplus Turnover 740 MF	13
Smart Card Diary	14
Smart Card Tutorial - Part 17 The Electronic Purse	15
Aladdin Cards for EuroDisney	20

BT Tender

Continued from page 1

The two main phonecard chips which can provide cryptographic authentication of the card are the SLE4436 developed by Siemens for Deutsche Telekom, and the ST1335 developed by SGS-Thomson in conjunction with France Telecom

Both of these chips are still commercially secret and technical specifications have not yet been published.

The potential market for Smart payphones and phonecards in the UK is substantial. At present there are some 120,000 public payphones in the UK of which 24,000 are cardphones. In addition there are around 300,000 coin payphones in protected indoor sites.

Currently BT cardphones are throwaway optical memory cards with annual sales reaching 20 million cards.

In France, where the Smart Card phone services are highly developed and marketed, France Telecom purchased 100 million cards in 1993. It's Carte France Telecom, for example, allows users to make calls from public telephones and have the charges billed to their home or a specified telephone account.

A spokesperson for Mercury Communications, a subsidiary of AT&T and BT's main communications rival in the UK, said that they would be incorporating Smart Card technology in their product offerings at some future date, but had nothing further to add at this time.

Separate development

In a separate development, BT are involved in the National Westminster Bank's new electronic payment service, Mondex, which uses Smart Cards as an alternative to cash.

BT has already announced that it will be adapting some 1,000 public payphones with Mondex card readers in Swindon for the Mondex trial starting there in 1995. They will also be providing residential telephones with Smart Card readers for home use.

Supertag Implications for SCs

A "Supertag" automatic identification system in the form of an integrated circuit chip with a printed flat aerial, is set to be launched commercially and may have longer term implications for the contactless Smart Card industry as an identification system.

British Technology Group (BTG) and CSIR, the leading research and development organisation based in Pretoria, South Africa, have announced plans to commercialise the CSIR Supertag system and are seeking collaborations with major semiconductor device suppliers and system integrators to establish a wide range of Supertag based products internationally.

Initially it is seen as an electronic replacement for bar codes holding out the prospect of "reading" in a second the entire contents of a supermarket trolley, while stocktaking could become a simple act of passing the scanner over the shelves to document the contents of a store within minutes.

BTG says that using radio links, Supertag readers are capable of multiple identification and counting at electronic speed. It has a unique anti-clash communications function which enables a group of individually tagged objects to be separately identified and counted even when they are close together. Currently 50 objects per second can be read up to a range of four metres.

The other key characteristic of Supertag is that once read it can be deactivated for a predefined time, enabling it to be used as an Electronic Article Surveillance (EAS) anti-theft device.

The anti-clash communications function allows the chip to be simple and cheap to produce, enabling new types of ID systems to be devised.

Initial applications are seen to be parcel and airline baggage tagging, animal tagging, railway and bus season tickets, car parking and personnel access control.

Contacts: Peter Hawkes, BTG, England - Tel: +44 (0)71 403 6666. Mike Marsh, CSIR, South Africa - Tel: +27 12 841 4004.

Smart Power Customer Card

Midlands Electricity, England, is to introduce a Smart Card cashless prepayment system for its customers.

Called the Smart Power Customer Card system, it is now under trial with the first commercial installations planned for the spring, and a target of 25,000 Smart Card meters installed in the first year.

In a joint development with Landis & Gyr, the system is seen as a replacement for token prepayment metering. At present there are 201,000 token meters in Midland Electricity's region with a growth rate of 30,000 a year. Cashless prepayments are made using encoded token cards sold in a network of around 400 terminals in Midland Electricity Board shops and offices, Post Offices, convenience stores, newsagents and off-licences. The terminals were developed in conjunction with Fortronic, Scotland.

In the new Smart Card system, each card is unique and will work only one meter, making theft and fraud pointless. The card provides a two-way flow of information. Data on consumption is downloaded to the Board's central computer when the card is "recharged" with value, eliminating estimated meter readings and the need for frequent visits by a meter reader.

The new meter, even if it runs out of credit, will not disconnect between 9pm and 9am, and no matter what debt may exist, a supply of electricity is always available for £1. A credit facility means the customer can recharge the card in an emergency.

Meters can be set to operate in three different ways to provide a variety of payment methods.

Many customers prefer the prepayment method of buying electricity. It has also been used by regional electricity companies as a guaranteed method of payment in cases of bad debt, hardship or consistently poor payment.

Contact: Mike Simpson, Metering Development Manager, Midlands Electricity, England - Tel: +44 (0)21 423 2345.

Dual Card Supply for Manchester

ERG Electronics, Australia, were last month actively sourcing a dual supplier for contactless Smart Cards to be used in the Greater Manchester automated fare collection system for public transport in the Greater Manchester area.

ERGE have total responsibility for the design, supply, maintenance and management of the system and 5,000 cards are required to be delivered in Manchester this month to be issued in February for the first phase of the scheme.

GEC Card Technology, who were awarded the contract to supply their contactless cards, had been unable to deliver any cards by mid-December.

It is understood that US supplier Racom, and Dutch supplier Nedap, are two of the contactless Smart Card fabricators being considered.

The total number of cards required in the first phase of the development is 500,000.

Quality Award for Solaic

Remy Dullieux, France Telecom's Director for Industrial Relations, presented the Telecom Corporate Quality award (TQE2) to Francis Lavelle, Chairman and CEO of Solaic, the Smart Card engineering subsidiary of Groupe Sligos, and to Michel Gaumet, Manager of Solaic's plant at Orleans in the South of France. (Photograph on page 1).

The award acknowledges that the quality management procedures implemented at the plant comply with international ISO 9002 standards and are efficient in the manufacture of Smart Cards, including the telephone cards supplied by Solaic to France Telecom.

By the end of last year, Solaic shipped 66 million cards, of which 52 million had embedded microprocessors.

France Telecom is a major consumer of Smart Cards and, in 1993, purchased 100 million phone cards from its suppliers, which include Solaic.

Schlumberger Art Competition

French painter Maelle Labussiere has won the third annual Smart art competition organised by Schlumberger in conjunction with the VISART Association in France. Her work was selected by a French jury of art experts and the winning picture has been printed on a France Telecom Smart Card-based phone card (see page 1).

Euan Baird, President of the Schlumberger Group, presented the award at Montrouge, France, last month, along with a special jury prize to American Alicia Paz, and the encouragement prize to Spanish painter Juan Aguirregoicoa. Four hundred candidates from 35 different countries participated in the competition, with 20 artists being selected to present to the jury.

The competition proposed a visual dialogue between technology and art with the objective of integrating the identity of Schlumberger - a multinational company working in the high technology field - with art. The work had to be capable of being used on the small format of a Smart Card - just 47cm² for the field of artistic expression.

Schlumberger says the Smart Card is a "vehicle for the images of our time" and the Smart Card competition allows post-modernist contemporary art to be appreciated directly by the greatest number of people.

M Labussiere, who is aged 27, graduated in Fine Arts in Paris in 1991. She works with the imprint, the repetition of a motif, superimposed by a frame. Her winning entry is likened to the work of Viallat, however, the official description says "unlike that painter, M Labussiere does not look for regularity - she plays with the accidents of the print. Using large formats and primary colours in acrylic, her work adapts remarkably well to reduction onto a Smart Card."

Schlumberger's 1994 International Art Competition for artists under the age of 30, will be organised in Germany in co-operation with DAAD (Deutscher Akademischer Austauschdienst). The winning painting will be reproduced on a German phonecard.

Contact: Isabelle Ferdane-Couderc, Schlumberger, France - Tel: +33 1 47 46 70 20.

Common Utility Card "Remote"

Proposals for the development of one Utility card for transporting credit to gas, water and electricity budget payment devices is described as "quite remote" by Stephen McKeivitt, GEC Meters, in a presentation on the WaterCard Smart Card budget payment system (SCN May 1993).

Speaking at IBC's Smart Card Europe Conference in London last month, he said this provision would only require the agreement of all the Utility providers on a common structure and all equipment providers to use this standard, but the chance of this happening in the next five years is quite remote, he said.

In any case more crucial questions have to be answered such as - Who takes priority when a payment is made - which Utility? How do you take credit off the card and transfer it to another Utility - "I made a mistake I want to pay for electricity not water!"

An easier solution is where a customer has a variety of cards each accepted by a common payment terminal which provides a far more flexible, reliable and lower cost solution. This also allows the product to develop in other related applications without being restrained by the costs of a complicated card infrastructure.

Manchester Project Appointment

Mike Hill, Marketing Manager for the Greater Manchester Passenger Transport Executive, has been appointed Commercial Director of Pre-payment Cards Manchester Ltd.

PCM is the joint venture company set up between GMPTE and ERG Australia to install the automated fare collection system on public transport and to extend the use of the contactless Smart Card, in particular an electronic purse function, into other areas.

Pre-payment Cards Manchester Ltd is at Huntingdon House, Princess Street, Bolton, BL1 1EJ. Tel: +44 (0)204 385196. Fax: +44 (0)204 384806.

Payment Metering Initiative

An industry initiative to agree a common approach to the provision of payment metering systems based on Smart Cards for the public utility customer services - gas, electricity and water - will take place at The Belfry, Sutton Coldfield, near Birmingham, England, on 9 February.

The event is being chaired by Landis & Gyr and it is expected to be attended by major companies supplying meters, point-of-sale terminals, Smart Cards and services together with representatives of public utilities already running or planning such schemes.

The objectives are to encourage suppliers to make equipment to a common specification so that users will be able to select from competing products knowing that they have been given "type approval" and will be compatible with their own and other systems; and to promote wider use of the Smart Card architecture amongst the utilities.

Contact: Martin Pollock, Marketing Director, Landis & Gyr, England - Tel: +44 (0)952 677661.

Smart Payphones for Morocco

Two Schlumberger Smart Card payphones have been approved by ONPT (Office National des Postes et Telecommunications) for connection to Morocco's public telephone network.

The TF08 for covered indoor environments and the PF08 for outdoor and street applications are part of Schlumberger's Smart Card phone family with over 100,000 installations to date in 50 countries.

"Smart Card technology is very suitable for private operators because of its intrinsic security, and the very high operating reliability achieved by dispensing with coin handling Mechanisms," says Abdellah Nasreddine, Schlumberger Area Manager for Morocco.

The PF08 payphone accepts payment by Smart Cards, magnetic stripe credit cards or phone cards. It is compatible with a PC-based

management system which can be used to monitor the network, raise alarms in response to malfunctions or attempted fraud, and to download information such as changes of tariff. The TF08 offers the same basic functionality in a form ideal for covered sites such as hotels, restaurants, commercial centres and waiting rooms.

Contact: Abdellah Nasreddine, Schlumberger Area Manager for Morocco - Tel: +33 1 47 46 70 29. Fax: +33 1 47 46 63 47.

Carte Moneta Offers Visa

Carte Moneta Smart Cardholders in Italy will soon be able to use their card to make purchases and withdraw cash while abroad following an agreement with Visa International.

SETEFI SpA, set up in 1989 by the Confcommercio Association representing one million retailers to develop the Moneta system (SCN June 1993), have decided to offer Visa services to their customers in Italy. The Carte Moneta will continue to function as a Smart Card in the SETIFI network which has some 12,000 EFT terminals installed.

Lebanese Electronic Purse

An Electronic Purse, called the LINK Card, is being promoted by some 19 banks in Lebanon's first Smart Card project. The participating banks control over 50 per cent of the market.

The system was developed by LINC, Lebanese Interbank Card, and French EFT consultants SG2. As the US Dollar is used as well as the Lebanese Pound for business transactions the system offers a mono or a dual currency card allowing the cardholder to make payments off-line in the chosen currency or currencies. The banks have an initial target of 10,000 cardholders.

Dassault Automatismes et Telecommunications, France, have provided the software and supplied 800 TPC 232 EFT terminals for retail outlets and bank counters. The cards are from Gemplus Card International, France.

Contact: Valerie Lorcin, Dassault A.T., France - Tel: +33 1 30 81 28 17. Fax: +33 1 30 81 22 24.

Health Cards in Germany

German health cards will put more Smart Cards into the hands of more people than in any other country in the world, including France with its Smart French Bank Cards, said Chris Jarman, Managing Director of Orga (UK), speaking at IBC's Smart Card Europe conference in London last month.

A massive 79.1 million electronic medical certificate cards are being issued in a phased release. In such volumes they will cost DM2 per card per year.

There are two types of card. The main one is the health insurance card which is being distributed in millions and should not be confused with the other type, the patient card, which is for specific medical applications.

Health insurance card

Health insurance cards are primarily payment cards and contain basic details to facilitate payment for health services provided. It will hold the name of the insurance company, the name, status, address, health insurance number and date of birth of the insured person, and a validity time. These 256 byte memory cards, do not have a PIN and there is limited control of access to data.

All insured people will have a health insurance card and about 14.5 million were expected to be issued by the end of last year (1993) to insurance companies with about 75% of that total issued to patients in advance of the cards being used by doctors and dentists.

A survey of over 4,000 insured people showed that 89% thought the card was a very practical solution, nearly 95% found card handling easy, and over 45% wanted to use the card for additional functions.

Patient card

The patient card has a microprocessor with 8K bytes of EEPROM and has a Hitachi chip. Applications can be added, and confidential data is protected by encryption and PINs. Sub-sets of information are available to access, for example, in the case of an accident emergency.

There will be a variety of patient cards, for example, diabetic cards, cancer rehabilitation cards, vaccination record cards and high risk patient cards.

These cards are being issued to 147,000 doctors, dentists and a number of specialist hospital facilities in the first phase, with the remainder by the end of 1994. The cards have a four-year lifecycle.

It is estimated that Germany will require 80 million cards for the healthcare field every two years.

Bull Electronic Purse System

Bull CP8 has developed a comprehensive offer for Electronic Purse systems compatible with TB cards, ISO and CEN standards.

The CC60 1K byte EEPROM card is the basic cashcard of Bull CP8 with secure payment and loading functions including mutual authentication between card and terminal using the DES algorithm allowing any kind of cash payment application.

The CC1000 8K byte EEPROM card can perform DES encryption and is compatible with CC60 and also with TB1000 cards and can combine the Electronic Purse function with other multi-file applications.

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

Street Walkers Promote Danmont

Street Walkers are being used in Copenhagen to promote the Danmont pre-payment Smart Card system. However, they are not the prostitutes to be found in the less salubrious parts of the Danish capital but specially trained people who will be handing out promotional leaflets.

The marketing campaign in Copenhagen involves advertisements in national and local newspapers and on local radio stations. Metropolitan parking tickets will also carry advertising for the new means of payment.

SA Interbank Card Standards

Standards for the implementation of a common Smart Card system throughout the local financial industry have been drawn up by the South African Interbank Smart Card Group.

This development was explained by Peter Bonfrer, an applications consultant within the ABSA Bank Management Services and Technology Division and represents ABSA on the Interbank Smart Card Technical Committee.

Speaking at the recent Plastic Cards Conference in Johannesburg, he said that motivating reasons included the need to present a card based service to the full market spectrum, to control current fraud problems, and the reducing cost of chip based technologies.

Business as well as technical issues were considered during the standards development. The standards cover the immediate future, which will encompass principally the pilot and short-term phases, prior to addition and/or modifications being adopted.

Today plastic cards were available to a small percentage of the South African population, credit worthiness and fraud being the two main reasons for this. As the Smart Card is capable of verifying its own PIN and credit limits as well as process transactions, it is possible to issue anyone with a card that can be used as an alternative to cash and other current payment mechanisms.

The use of electronic money is far more secure than real cash for both the client and the merchant. All funds received by the merchant can only be deposited in the merchant's account and funds on the card are PIN protected.

Historically, banks have attempted to replace cash with plastic card based transactions. This has not been successful for a variety of reasons: credit cards depend on credit worthiness of the cardholder, thus excluding a sector of the community; and debit cards depend on a well-established data communications infrastructure, not available at this time in South Africa.

Smart Cards present a vehicle whereby credit worthiness or data communications infrastructure

are not issues, therefore, it is felt that the facilities presented by Smart Cards place them in the same arena as cash.

Smart Card capacity now enables multiple independent applications on one card, allowing the banks to issue cards with differing products to each customer depending on their requirements. These products could be both banking and non-banking.

It was decided to implement a DES-based security system and migrate to Public Key Cryptography in the future due to the lack of availability of PKC cards today.

Common mask

Participating financial institutions will implement a common mask for the pilot phases. As needs change, it will therefore be the prerogative of each bank to develop their own masks in the future. Transactions agreed are:

- Funds transfers between the two purses within the card as well as transfers between the card based purses and host based accounts.
- Off-line payment at point of sale. The structure of this transaction is such that host computer intervention is not required unless indicated by certain protective parameters within the card.
- Clients will be able to select and change their PINs. A PIN change can occur without host intervention given that the old PIN has been successfully presented. Should the old PIN not be available, alternative host computer based methodologies have been provided.
- The major purse on the card (commonly referred to as the Secure Card Account or SCA) is PIN protected to assure security.
- The minor purse (known as the High Speed Self-Service or HSSS) does not require a PIN for access and would typically apply to low value transactions.
- Common File Management approach

The initial protocols that will be supported will be T=0, an established ISO protocol, but as soon as a T=14 card is introduced, the terminal software will be adapted to suit.

Security is an issue that consumed the most time in the standards development and the process for the pilot has been established as follows:

DES the Data Encryption Standard algorithm will be built into the Smart Card, the transacting terminal as well as both the Issuer and the Acquirer host.

RSA - this public key algorithm has been included for three reasons: its growing level of acceptance in the industry as a reliable algorithm, the decreased complexity of key management and the increased power of processors to handle the mathematical complexity of the algorithm. The process will cover only the issuer host and the transacting terminal. The reason for not applying the process to the client cards is that such cards are at this time still in the development process and will not be sufficiently tested in time for the system pilot exercise.

Card costs

The costs of the client card is in the arena R10-15/card (US\$2.90-US\$4.40). This card would be capable of providing the required functionality as specified in the standards.

Implementation costs of a Smart Card system will present to the financial industry an additional estimated cost of R44,5 million (US\$13 million) over the next five years. This cost refers only to a card supply and security implications on the affected terminals. Figures used are based on an eventual card and security module population (after five years) of 6.9 million and 135,000 respectively. System development, administration, etc costs are not included.

Telephone Cards in South Africa

Telkom South Africa launched a public cardphone service based on chip cards in September last year and plans to have 20,000 units installed by April 1996, according to Allister Dawson, Senior Manager Payphone Products, Telkom South Africa.

The cardphone service is planned to compliment the existing population of around 50,000 public coinphones, and is seen as particularly suitable to provide public telephone services in remote areas where vandalism and violence is prevalent.

The cardphones, designed by GPT in the United Kingdom, are manufactured locally by Telephone Manufacturers of South Africa. It is planned to have 5,800 units installed by April 1994, 14,000 by April 1995, and 20,000 units by April 1996.

The GPT cardphone is designed to operate with phonecards using the Siemens SLE4409, 104 bit EEPROM memory chip.

Estimates of the number of chip cards required over the next five years are:

	No. of cards sold annually	Cumulative total
1993/94	1,000,000	1,000,000
1994/95	7,500,000	8,500,000
1995/96	10,500,000	19,000,000
1996/97	19,000,000	38,000,000
1997/98	22,000,000	60,000,000

These figures are based on the assumption that 1,000 phone cards will be sold for each operational cardphone annually. The initial four million cards are being supplied via Telephone Manufacturers from GPT.

The Telkom pre-paid phone card can be loaded with up to 20,000 tokens, which are decremented during use. At present, each unit decrement represents 5 cents, allowing a maximum of R1000.00 (US\$2,929) to be loaded on a card.

The cardphone, with the card reader, key pad, alpha numeric display and connection to the telephone network, could also be used as a multiple applications terminal to perform a number of transactions. Potentially they could provide the user with additional services such as providing credit balance information, remote account payment and funds transfer, while cards issued by other service providers could be regarded as being loaded with cash and be used as payment for various services such as payphone, bus, rail and taxi services, retail cards, bank cash purse and vending machine services.

SIM Portable Examiner

Cardinal (UK), independent Smart Card development specialists, have launched Simplex, a handheld portable terminal for the testing, examination and modification of Subscriber Identity Modules (SIMs) which are Smart Cards used in the Global System for Mobile Communications (GSM) and Personal Communication Networks (PCNs).

The device enables analysis of all existing European GSM and PCN standard SIMs, including full size and plug-in modules. Cardinal says that simple software upgrades will ensure that future system cards can also be analyzed.

Simplex is delivered as a complete solution with its own screen display, keypad, mains adaptor, battery charger and carrying case.

The standard RS232 cable supplied also allows connection to any IBM compatible PC for software upgrades or connection directly to any IBM PC compatible printer for hard copy output.

The menu display allows users with different abilities and requirements to analyse the chosen SIM elements, for example field and test engineers can perform complex fault investigation whilst the service provider or mobile outlet can perform simple screening "health checks." Cardinal will provide six month's telephone support and warranty.

For sales and distributor enquiries, contact Simon Reed at Cardinal (UK) - Tel: +44 (0)442 236665. Fax: +44 (0)442 236604.

EFToMAT Terminal

The Ascom EFToMAT terminal is modern and functional in design and the housing is available in white, green, yellow or red. The card is inserted vertically or horizontally, depending on the position of the card reader. It can read all the usual cards - magnetic stripe and Smart Cards, credit and debit cards, as well as store cards. The retailer decides which cards the system will accept.

Up to 93 terminals can be connected via Local Area Networks (LANs) to a K93 concentrator. This device can handle as many as 20 different card issuers via the X.25 protocol.

Manufactured by Monetel, the French subsidiary of Ascom, Switzerland, the terminals are in use, for example, in the Swiss PTT Postcard electronic purse project.

Contact: Peter Wullschleger, Corporate Communications, Ascom, Switzerland - Tel: +41 31 999 6724. Fax: +41 31 999 6208.

New Danmont Card Design

Danmont's latest pre-paid card design, pictured on page 1, combines drawings of services and a crossword puzzle spelling out the name of the service in Danish. Services available using the card (with the Danish name indicated in brackets) are: coffee (kaffe), parking (parkometer), Danmont (smapengekort) laundry (montvask), snack (snack), newspaper (avis), kiosk (kiosk), stamp (porto) and telephone (telefon).

Buscom Fare Collection System

Buscom Oy, the Finnish automatic fare collection system company, now has 10 schemes in operation in Finland using some 61,000 contactless Smart Cards. In addition it has installations in Norway on the Trondheim region ferry (Fosen Trafikklag) and installations are in progress in Denmark (Faaborg Nartrafik).

A key advantage of the Buscom proximity card system is the speed of boarding times which are critical cost and service factors in mass public transportation. At the same time the proximity card is a convenient and easy to use ticket for passengers who simply hold it up to the reader which reacts even if the card is inside a wallet. Add quick, detailed and accurate reporting on passenger numbers and cash flow and it is easy to see why so many transport operators are turning to Smart Card technology.

Veli Heikkinen, Managing Director, says 1991 was the turning point in the development of mass-transportation ticket systems. At the congress of the International Union of Public Transport in Stockholm Buscom Oy presented its ticket system based on proximity technology which was the

first and unique in the world. This year (1993) in Sydney at the corresponding congress there were eight manufacturers of tickets system and seven of them presented non-contact solutions.

Passenger information was important, he said, and until now information had been incomplete and arrived late. It had been based on various calculations carried out over specific periods and was expensive and not completely reliable as it was affected by random influences such as the weather.

By using a Smart Card ticketing system, accurate information could be obtained quickly on:

- * cash flow
- * passenger numbers
 - by routes
 - by times
 - by types
 - by stops etc

This information was used in monitoring payments, traffic planning, planning of effective equipment usage, automatic daily passenger calculation, cash clearing, cost allocation, and reporting to associated organisations.

The system

In December 1991, the first Buscom equipment was installed for trial use and in January 1992 a

Buscom Proximity Card Installations in Finland at January 1994

system covering an entire town came into operation in Oulu in Finland.

In use the passenger simply holds the card up to the card reader mounted beside the driver. Each card is identified with a fixed data field, for example, the card number, which cannot be changed after manufacture.

When passengers show their card in front of the reader an accepted transaction is displayed by a green light, A yellow light informs the passenger of low validity on the card, while a card with no validity displays a red light signal and triggers a buzzer which informs the driver of an unacceptable card.

At the depot there is a microcomputer for data entry, updating and reporting. Data is transferred from the vehicle equipment to the depot using credit card sized card which collects the data from the card reader on the vehicle. At the depot the card is inserted in a card reader and the data

Location	Buses Equipped	Cards in Use
1 Turku (Trial)	20	2,000
2 Oulu	130	17,000
3 Helsinki (Trial)	4	1,000
4 Ahvenanmaa	20	1,000
5 Oulunsale	Numbers included at 2	Numbers included at 2
Kempele	Numbers included at 2	Numbers included at 2
Haukipudas	Numbers included at 2	Numbers included at 2
Muhos	Numbers included at 2	Numbers included at 2
6 Porvoo	70	5,000
7 Kuopio	103	11,000
8 Varkaus	30	5,000
9 Jyvaskyla	90	11,000
10 Lahti	70	8,000

downloaded to the computer. Reports are produced for management use such as cash flow monitoring, passenger monitoring, various income and cost reports and reports required for other associated groups.

Buscom proximity cards are used in some 11 sites in Finland (see diagram), and also in Trondheim, Norway, in a fully integrated multi-mode (speedboat, ferry and buses) proximity card based fare system involving around 6,000 cards of which 2,000 are used in ferry traffic.

In Faaborge, Denmark, proximity cards are replacing the existing magnetic card pass system. Seven hundred cards have been issued, primarily for school children, but with some multi-ride type special applications.

The Buscom system was used in the demonstration pilot scheme by London Transport buses in December 1992 when 1,000 cards were issued.

Awards

The Buscom proximity card was selected as the Most Innovative Smart Card of 1991 at the European Smart Card Applications Technology Conference, while the Finnish Design Association chose the Buscom reader as the winner of the Pro Finnish Design Award selected from products from all applications and industries.

Buscom systems are integrated into the systems of Thorn Transit International of the UK, and Monetel SA of France where Buscom sells its equipment, particularly in proximity card technology, on an OEM basis.

Technical specifications

Construction	EEPROM Chip and coil
Card size	86 x 54 x 1.6 mm
Signal interface	RF inductive
Reading time	30 ms
Read/writing time	200 ms
Reading distance	approx. 100 mm
Number of rewritings	Over 10,000

Contact: Veli Heikkinen, Managing Director, Buscom Oy, Finland - Tel: +358 81 551 4366. Fax: +358 81 551 4766.

Gemplus Turnover 740 MF

The Gemplus Group reports a turnover growth of 50% to reach 740 MF at the end of its fifth full trading year on 31 December 1993.

Export sales represent 65% of group turnover. During 1993, the Group, which has a factory in Stuttgart, strengthened its position in Germany with large orders taken in the telecommunications industry (public and mobile) and in the health sector (insurance cards and readers for the medical profession).

Major contracts were signed for telephone cards with nearly all the Latin American companies, an "electronic purse" card contract was signed in America (the MAC project), and microprocessor cards worth tens of millions of Francs were delivered in the Japanese market.

Production capacity doubled in the French plants at Gemenos and La Ciotat (14 million cards per month at the end of 1993), a card personalisation centre was opened at Sarcelles, near Paris; and VeriGem, a joint venture company, was formed between Gemplus and the VeriFone Company in the United States to develop and market SmartCash, Smart Card electronic purse applications worldwide.

A 150 MF capital holding was acquired by German industrial investor (QUANDT) which has interests in the plastic magnetic cards sector and a strong presence in the North American market; while Innovatron continued to shed its commitment selling two-thirds of its shares in the capital of Gemplus Card to the Paribas Group, so reducing its holding to 0.78%

The Group's turnover target of one billion Francs in 1994 is described as "realistic" by company directors.

New Card Manufacturer

S-Card, in northern Jutland, has been certified as card producer to the Danmont system.

The first Danish card manufacturer, S-Card has installed equipment to embed the IC chip modules in the plastic cards.

Smart Card Diary

Smart Cards - Asia '94, Marina Mandarin, Singapore, 24/25 January.

The 5th annual conference dealing with the latest trends and developments plus case studies is preceded by a workshop on 21 January on Planning, Implementing & Marketing Smart Cards. Contact: Ms Elsa Dana, Centre for Management Technology, Singapore - Tel: +65 345 7322.

Lafferty's Cards & Payments Convention, Hotel Intercontinental, Frankfurt, Germany, 7-10 February.

The Convention includes the International Smart Card Conference on 8 February (afternoon) and 9 February (morning). Contact: Dianne Crannage, Lafferty Conference Administration Centre, Dublin, Ireland - Tel: +353 1 671 8022.

The 1994 Pan European Digital Cellular Radio Conference, The Athens Concert Hall, Athens, Greece, 15/17 February.

Now in its eighth year, the conference is a major forum for the world's GSM industry. The conference will deal with commercial, marketing, operational and administrative issues as well as user requirements and experiences, while the optional technical seminar on 17 February, at the Athens Hilton Hotel, includes network management, type approvals and the development of value added services. Contact: Tania Starley, IBC Technical Services, London, England - Tel: +44 (0)71 637 4383

Smart Card '94 Conference and Exhibition, Wembley Conference Centre, London, 15-17 February, 1994.

Two conference streams per day - day 1 - market overview/leisure and finance and security; day 2 - the Electronic Purse and technology & standards; day 3 - communications/network services and transport and travel. The conference is preceded by a Smart Card tutorial on 14 February. Conference Secretariat - +44 (0)733 394304.

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

Three days of seminars on technology and applications, 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.

ACT Supply Clearing Centre

A £1.5 million computer centre to clear payments in the Greater Manchester Smart Card automated fare collection project is being supplied by ACT Financial Systems, the Birmingham-based company who are Europe's biggest supplier of financial software. ACT software solution runs on a Hewlett Packard hardware platform, also being supplied by ACT.

The Manchester project involves equipping 2,700 buses and 130 rail stations with card readers and ticket machines and around 700,000 cards are expected to be in use by 1996. It is also planned to extend the automated fare collection system from its public transport base into local authority applications and an electronic purse.

Transactions will be processed by the new central computer centre which will provide the information for settlements to several hundred service providers, merchants and point-of-charge outlets without the involvement of banks as GMPTE is a licensed deposit taker.

Prepayment Cards Manchester Ltd will be a subsidiary to the Executive with the same licensed deposit taker status.

Contact: Phil Dobson, Executive Manager, ACT Financial Systems, England - Tel: +44 (0)21 455 6111. Fax: +44 (0)21 456 5579.

Smart Card Tutorial - Part 17

The Electronic Purse

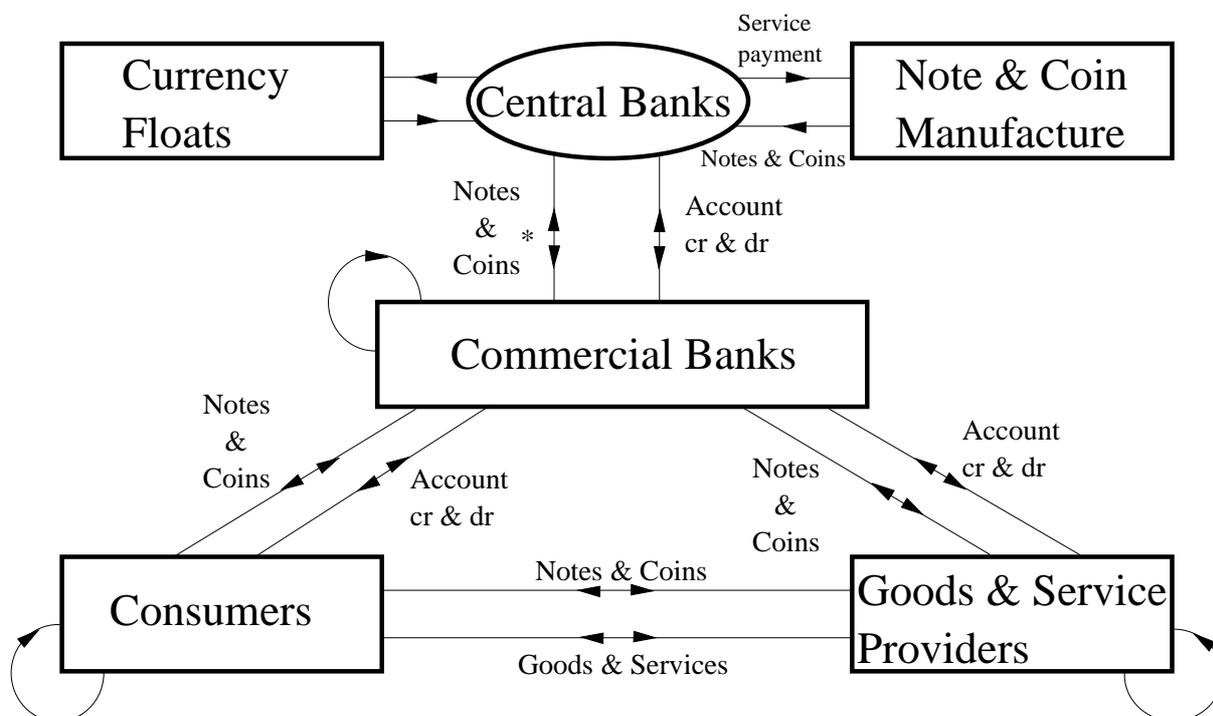
The term electronic purse is used to describe a wide range of business scenarios where a Smart Card is used to represent the holding of a financial asset. In this part of the tutorial we will examine the more common situations and discuss the various models that arise. We can generalize these architectures in three ways,

- a) Closed prepayment systems
- b) Open prepayment systems
- c) Electronic money

The business model is very different between these architectures and accordingly that leads to different requirements for the technical infrastructure that allows the business to operate. Before we start it is useful to hold in our minds the classical model for the use of cash as shown below. It is important to notice immediately that the model is multi currency. In the real world we are faced with a range of currencies that exist

within the various entities defined. Any participant may be holding one or more currencies at any particular point in time. Equally obvious is the fact that these notes and coins are constantly recirculating amongst the various entities. The only exception here is the reluctance of central banks to accept coins which leads to a significant operational problem for the commercial banks. The distribution of notes and in particular coins is an expensive overhead.

The manufacture of currency is organised by the central banks. They are responsible for the security which underlies the use of their own particular notes and coins. In practice the actual manufacture of the notes and coins is contracted out to a manufacturer with the appropriate skills and security resources. The coins and notes are distributed on request to the commercial banks with the appropriate adjustment of accounts. At this point in time the notes and coins take on a value equivalent to their denomination which results in the creation of an asset float which relates to the total value in circulation. The central banks have a liability for the value of the float.



*Coins in general are not recirculated with the Central Banks

It is interesting at this point to reflect upon the matter of counterfeiting. The rules of the game are quite clear in that no entity wishes to accept a counterfeit note or coin. The central banks quite clearly will try to avoid the reimbursement of any counterfeit note in the distribution chain. If a consumer inadvertently accepts such a counterfeit then like a hot potato he will probably try to pass it on (I hope that I have not totally misjudged the morality of the average consumer). The commercial banks have the same problem but the morality issue is overpowered by the legal requirements. If the bank teller spots the note as a counterfeit then he will confiscate the note to the detriment of the customer. Whilst all this may seem academic it serves to highlight the security issues and also gives a first indication of the problems that surround the near perfect counterfeit note. As long as the central bank can detect the counterfeit then someone else in the chain will lose. Whilst few provable figures exist it is generally accepted that the American notes are one of the easiest major currencies to counterfeit. Such discussions often lead to an examination of the advantages that electronic money might offer in this respect.

Closed Prepayment Scheme

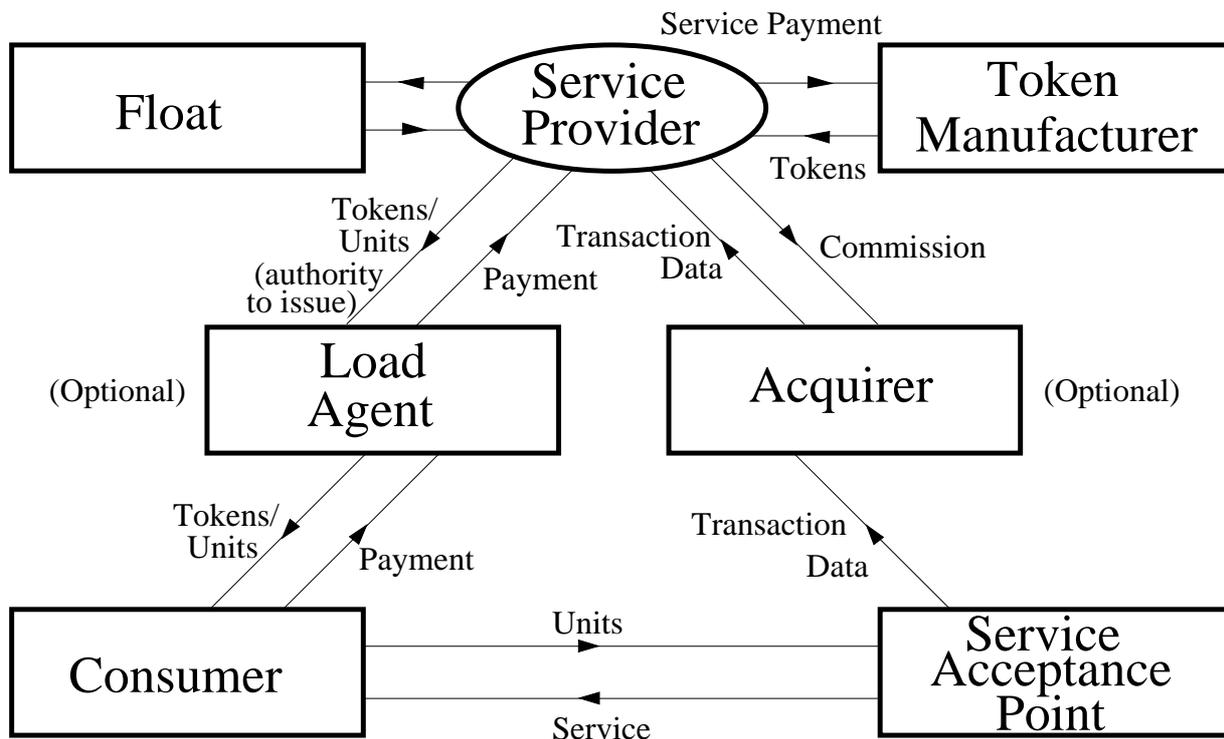
This concept is well established and used in most developed countries within the utility sector. The use of telephone prepayment cards is well known

and other utility organisations such as gas, electricity and water are involved with the use of prepayment tokens. The model for this scenario as shown below is the simplest and technically the easiest to achieve. The first important point to notice is related to the flow of the electronic units. The concept of bidirectional flows has gone. The units flow from the service provider to the consumer and thence to the service point where they are collected. From the service point the necessary records flow back to the service point for reconciliation against the float. In general these units are not redeemable and the float always (assuming adequate security) shows a surplus. This is due not only to the time difference between acquiring units and using them but also because of losses by the consumer through inefficient use of the tokens. Analysis of throw away telephone cards provides an indication that this gain to the service provider can be substantial.

The next consideration here relates to the design of the token,

- passive
- active
- disposable
- reloadable

Most telephone cards are passive in that they store a data field reflecting the current value of



the card. When the card is used this value decreases according to use. The security of a basic magnetic stripe card is really non-existent since a perpetrator may easily copy the data stored on a new card and produce an arbitrary number of counterfeits. In Japan this is currently causing a major fraud problem which may result in the move to other techniques such as the Smart Card.

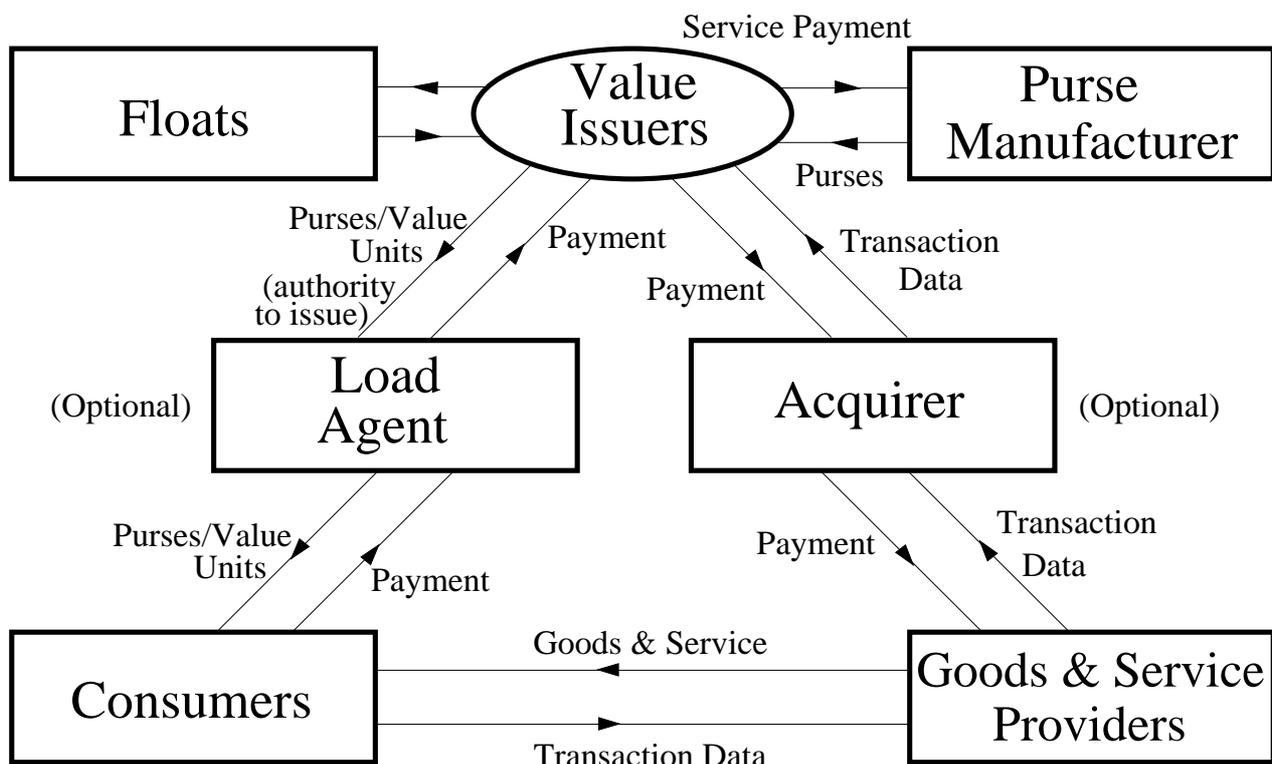
A basic integrated circuit (ICC) Card can also be implemented as a passive memory device and when used in this mode offers little advantage to the magnetic stripe card. A rewritable memory device using say EEPROM would be easier to defraud than a magnetic stripe card. Many of the memory ICCs however offer a protected memory mode where it is necessary to enter a PIN to unlock the memory access.

The problem here is that the access control mechanism is relatively primitive and by default must be common to all service points. It is difficult to imagine that these basic passive memory devices will ever offer adequate security except in very controlled environments. (Such as

that offered by closed prepayment schemes). It should be noted here that telephones (for example) are permanently connected to the service provider which allows a range of security mechanisms not available in the more general off line environment.

The active token opens up more powerful security techniques and in particular the ability to achieve bilateral authentication. Clearly there is a significant cost increase in the use of a microcontroller ICC. As a rule of thumb the microcontroller card is likely to cost 2 - 3 times the cost of a memory card. In real terms for a mature volume scenario we are probably comparing 50p with about £1-50.

Whilst many utility card schemes use disposable cards there is no inherent technical reason why a reloadable card scheme should not be implemented. In many cases the business driver is for a disposable card and this is particularly relevant to telephone payment schemes. However these are significant changes taking place in the world of telecommunications which will probably change the picture. As mentioned previously the



telephone service providers have the particular advantage of an on line link. This is not the case with other utilities such as gas and electricity. It should also be noted that it is still necessary to recover transaction information from the meter and it is this factor in particular that defines the overall technical architecture and its security requirements. What must be very clear is that the security requirements for a reloadable card scheme are more severe and therefore are intrinsically more expensive to implement.

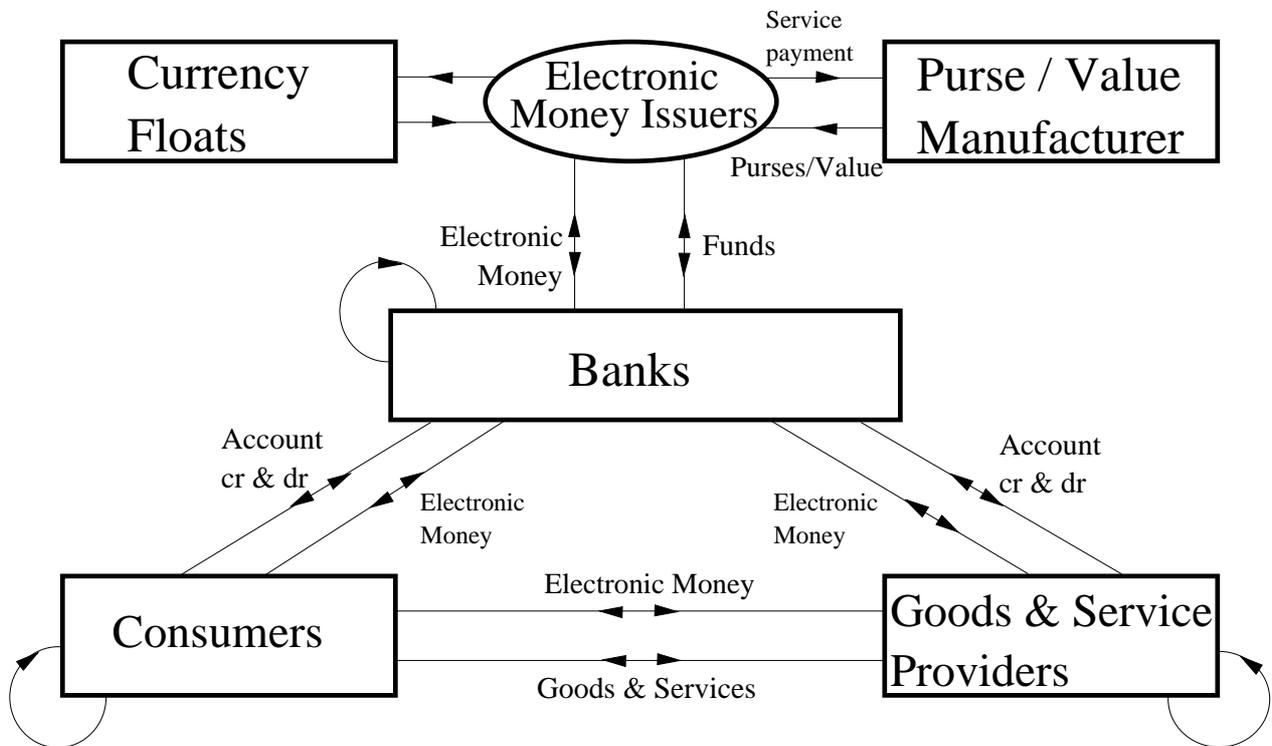
Open prepayment systems

Flexibility is the antithesis of security. From a business point of view one would like to achieve maximum flexibility for the operation of a prepayment scheme and this is the core of our discussion when comparing an open prepayment scheme with an electronic money scheme.

A model for the open prepayment scheme is shown on page 15. There are in fact many

similarities with the closed prepayment model. In this case the transaction records are acquired and transmitted back through the system to enable a clearing operation to take place. This is often compared as the electronic analysis of the traveller's cheque. In the model electronic value is shown moving in an anticlockwise direction. It is clear that this in no way maps our model of real cash. The security requirements are none the less stringent.

The model shows a general architecture for which there are a large number of possibilities in terms of commercial implications. Open prepayment schemes are still in their infancy and none have yet been applied on a international scale. The general implementation of such a model is predicated on a clearing between the value issue and as such the issuers of electronic value and its recovery requires the preservation of issuer identification. The optional load agents role arises due to the need to simplify the practical operation of the system. Neither the local agent or acquirer



are intrinsic to such implementations but the mechanisms by which value clearing operates is likely to result in these roles which could of course be undertaken by a common agency.

Electronic money

On page 16 we show a model for electronic money. A comparison with the previous model for cash shows the similarity between the two approaches. With reference to the standard open prepayment model we can see instantly that the concept of clearing is removed if we assume that the electronic money for each currency is issued by one logical source. This is of course the case with real notes and coins.

The model also shows the same bidirectional flows for electronic money as for cash. In a general sense the electronic money circulates inter and intra the entities.

We announced in last month's SCN the Mondex electronic money scheme. It is clear that this is based on the primary model shown here.

The security architecture is quite different for each of these models. Next month we will develop a security model for these various purse models and develop an approach for the various implementation paths. It is however important to note that these models represent a general case. A particular implementation may invoke various restrictions to meet a particular business need. As an extreme case the removal of bidirectional flows on the electronic money prepayment model could lead to a commercial equivalent of the general open prepayment model.

Next month - Security and the electronic purse.

David Everett

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

UK £375

International £395

Please invoice my Company

Cheque enclosed

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

Name _____

Name _____

Position _____

Address _____

Company _____

Address _____

Card No. _____

Expiry date _____

Tel. _____

Signature _____

Fax. _____

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

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

Aladdin Cards for EuroDisney

New cards depicting characters from Aladdin are being used by Sega Amusements Europe in the Cashcard payment system at their video games centres in hotels at EuroDisney in Paris following the success of their Beauty and the Beast Cards.

In eight months, Cashcard Systems, England, have supplied over 250,000 cards for the project. The Beauty and the Beast cards were fabricated by Schlumberger, Cashcard's development partner, but the Aladdin cards come from TRT Philips Smart Cards & Systems as a EuroDisney preferred supplier.

This is a significant number of cards in the time-scale and enhances the business case for the use of "throw-away" memory cards in the leisure industry. Part of this success must be due to the

visually attractive designs on the cards making them souvenir and collectors' items.

Cashcard Systems have also made a breakthrough in the amusement machines sector following a submission to The Gaming Board who have now withdrawn opposition to the use of Smart Card technology on Section 34 Amusement with Prize (AWP) machines, subject to certain conditions being agreed between the Board and the British Amusements and Catering Trade Association (BACTA).

A particular requirement is to provide a separate recording of cash and token values, and to ensure a high level of security and data integrity. Cashcard argued that the microchip-based Smart Card allows the isolation and management of many different fields in its memory.

"This is excellent news for the industry," said Cashcard's Chief Executive, John Kelly. "The Smart Card advantages of reduced cash-handling, increased security and sophisticated data capture are now available to all amusement machines products. We shall be working with BACTA to have the guidelines in place as soon as possible."

Contact: John Kelly, Chief Executive Officer, Cashcard Systems, England - Tel: +44 (0)707 396939. Fax: +44 (0)707 391819.