

Lufthansa Introduces Ticketless Travel

Lufthansa, the German airline, has introduced ticketless flying on all domestic flights following the successful testing of its ChipCard with more than 600 frequent flyers on the Frankfurt-Berlin route last year and a positive response from customers.

Heralded as “a major leap into the future of air travel,” the ChipCard integrates contactless Smart Card technology in a card combining ticket, boarding card, customer card and credit card.

Lufthansa Chief Executive Marketing, Hemjō Klein, says: “By introducing chip card technology for ticketless travel, Lufthansa is creating exclusive customer benefits. We are speeding up ground service and at the same time are the first of the world's airlines to utilise touch-free chip card technology in combination with an electronic ticket.”

Continued on page 93

Smart Card News

Managing Director: Patsy Everett

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
Vice President, Chip Card Technology
MasterCard

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 -

CONTENTS

63 Motorola to Produce Chips in US

64 China Orders L&G Payphones

65 P-CARD to be Offered Worldwide

66 Loyalty Cards in Supermarket War

67 Mondex Trial in Canada

68 ecash Payments on the Internet

69 Thyron Terminals for Dubai Taxis

70 PROTON Starts National Roll-out

72 BiPay Smart Card from GPT

73 Data Protection on the Cards

74 CarteS SESAMES '96 Awards

75 Smart Card Diary

76 Electronic Commerce and Payment
Mechanisms - Part 3

80 Multi-Service Puzzle Cards

Lufthansa Ticketless Travel

Continued from page 91

The new card, which has a new chip replacing all previous customer cards, is being issued first to all holders of Lufthansa Senator Cards resident in Germany, followed by frequent fliers with the airline and then to all interested customers. Initially, the card will be available for use on all Lufthansa domestic flights in Germany.

In use, the card will make service on the ground more convenient, easier and faster. Customers book their domestic flight in the usual way, either at their corporate travel office or by telephoning a travel agency and giving their ChipCard number as a reference. Their booking is then stored electronically in the reservations system so there is no need to go to the travel agency to collect the ticket or have it mailed to them as there is no paper ticket involved in the transaction.

Passengers travelling only with hand luggage simply wave the card in front of a Chip-in terminal which then issues a print-out containing all the details concerning their departure gate, boarding time and seat number. At the same time, mileage for the frequent flier programme, Miles & More, is automatically credited to their account.

Passengers with check-in baggage can also use the ChipCard. Instead of using the Chip-in terminals they check in at the normal counters where they obtain their boarding card and baggage label. At many airports, passengers will be able to carry out the final boarding procedure simply by waving their ChipCard over a special reading device installed at the gate.

A total of 37 Chip-in terminals are being installed at all German airports from which Lufthansa operates and more than 70,000 ChipCards have been issued so far with a target of 100,000 by the end of July this year. The new card is the RM8K (1K bytes EEPROM) contactless Smart Card from Giesecke & Devrient which uses remote coupling technology from Mikron of Austria and is designed specifically for applications in identification and ticketing systems.

Contact: *Markus Ruediger, Lufthansa Press and Public Relations UK/Ireland - Tel: +44 181 750 3415. Fax: +44 181 750 3410.*

Motorola to Produce Chips in US

Motorola, the world's biggest supplier of microchips for Smart Cards is to start manufacturing them in the United States at its plant in Research Triangle Park, North Carolina.

The announcement was made at the CardTech/SecurTech Conference in Atlanta, Georgia this month and the company described the move as a major investment in the future of Smart Cards in the US.

Motorola's worldwide headquarters for Smart Card operations is in Scotland where it will remain, but the company has always indicated that it could produce Smart Card chips at many of its international locations and the announcement that it is extending its manufacturing capability to the US will not surprise industry watchers.

Motorola views America as a major marketplace in the near future and its microchips are being used in Visa's reloadable stored value Smart Cards in many parts of the world including Atlanta for the 1996 Olympic Games.

Allan Hughes, Worldwide Smart Card Operations Manager based in Scotland, says the North Carolina plant plans to have capacity to manufacture "many millions" of Smart Card microchips per year by 1997.

"Motorola recognised early on the vast potential for Smart Cards in the US," he said. "With this move, Motorola becomes the first company to address directly what will soon be a booming US market.

"Consumers will soon discover the many ways in which Smart Cards can support them - and make life easier - with card applications ranging from healthcare, personal computer and Internet access, to financial services, telecommunications and building access control."

Motorola also announced that its US Smart Card operation will be located in Austin, Texas where this facility will be responsible for marketing, business management, design, manufacturing and product engineering.

Contacts: *Clare Lucraft/Paul Dawson, Hill & Knowlton - Tel: +444 171 413 3145. E-mail*

pdawson@hillandknowlton.com

China Orders L&G Payphones

A contract to supply 1,000 chip card payphones to China has been won by Landis & Gyr Communications. The Geneva, Switzerland-based company is delivering its Comet 61 payphones equipped to accept second generation (4406-type) pre-paid chip cards to MPT China's Tianjin Telephone Equipment factory for use in field trials across the country.

Li Zhen Hua, Director of the MPT's Tianjin factory says the award of the contract was based on the success of Comet 61 payphones installed at the Fourth United Nations World Women's Conference in Beijing in September last year and their flexibility to accept new emerging payment methods.

Contact: *Adolf Deyhle, Landis & Gyr Communications - Tel: +41 22 749 3355. Fax: +41 22 749 3539.*

Mikron License for Allsafe in US

Allsafe Company, Inc., one of the largest card manufacturers in the access control, time and attendance and parking marketplace, has announced it has signed the first US license agreement with Mikron GmbH of Austria for its HITAG advanced radio frequency identification system.

The US Buffalo, New York-based company says it will develop and produce HITAG core modules, access control readers to interface to OEM systems and also manufacture HITAG and MIFARE contactless Smart Cards for the US marketplace.

HITAG, an advanced read/write RFID technology, was developed especially for access control, parking, time and attendance, employee card, ski ticketing, vending, customer loyalty and other related markets. Key features include read/write memory, high security using passwords and mutual key authentication, data encryption and memory write protection plus the ability to read and write multiple cards simultaneously with one reader (anti-collision) at operating distances up to 30 inches giving hands-free operation if required.

Mikron is a wholly-owned subsidiary of Philips Semiconductors and its HITAG cards are the same

size as credit cards. Allsafe says the cards can be read and written to using both the HITAG core module as well as the Allsafe ProxRite reader. The HITAG core module (called Prox-In A Can) is available to any OEM who wishes to embed the card technology in their own custom designed readers. The Allsafe ProxRite reader is available to OEMs who wish to be able to read and write HITAG cards utilising an industry standard interface such as Wiegand, RS232 or RS422/485.

HITAG cards can also include a magnetic stripe, debit stripe, bar code(s), barium ferrite insert as well as other card technologies and options. The operating range is up to six inches with the standard reader and up to 30 inches with the long range reader.

Contacts: *Michael L Davis, Allsafe Company - Tel: +1 716 896 4515. Fax: +1 716 896 4241. Email: mdavis@allsafe.com Friedrich Plankensteiner, Mikron North America, Philips Semiconductors North America - Tel: +1 408 991 2101. Fax: +1 408 991 2122. Email fplanke@scs.philips.com Martin Böhrlen, Mikron Austria - Tel: +43 3124 299210. Fax: +43 3124 299270. Email Martin_b@mikron.co.at*

Good Results from SGS-Thomson

French chip manufacturer SGS-Thomson Microelectronics has reported a 32 per cent increase in revenues for the first quarter ended 30 March. Net revenues totalled US \$1.03 billion compared with first quarter 1995 revenues of US \$778.6 million. The company reported a significant increase in net income which rose 64 per cent to US \$175.0, up from US \$106.9 million for the first quarter of 1995.

Pasquale Pistorio, President and Chief Executive Officer, described the results as an outstanding quarter. "Our sales were up in comparison to both the year ago quarter and on a sequential quarterly basis," he said.

He added that with tight control on operating expenses, SGS-Thomson recorded an operating profit margin of 21.5 per cent - the highest in the company's history, and he said it should be noted that SGS-Thomson "continues to be capacity constrained" in most of its leading product

families. During the quarter, the company shipped

P-CARD to be Offered Worldwide

The German P-Card alliance headed by EBS Elektronik Banking Systems GmbH, is to licence its multifunction electronic purse technology worldwide.

Announced last month (*SCN April 1996*), the P-CARD system is being introduced in Germany by a partner association consisting of Krone Kommunikationssysteme, Bad Hersfeld, ORGA Kartensystem, Goppinger Datenservice and EBS and plans to issue 500,000 Smart Cards and set up 3,000-5,000 acceptance points this year.

Angelika Wegner, General Manager, EBS, says the system allows licensing of each interested party (bank, trade, industry etc) for issuing, acquiring, processing, service-providing, terminal and card manufacturing as well as for interfaces. Licences for banks will only be given for the stock in the electronic purse and for clearing.

Licences will be sold by ORGA Consult GmbH who will recruit domestic licence-owners in each country.

The 8K bytes EEPROM multifunction Smart Cards will be available with chips from Siemens (44SLC80) Hitachi (H8/3102) and Philips with the card fabricator to be decided by the issuer.

Contact: *Angelika Wegner, EBS - Tel: +49 611 95 130 0. Fax: +49 611 95 130 99.*

BIK to Process Geld Karte

Transactions for Germany's Geld Karte electronic purse scheme (*SCN January 1996*), will be processed by the Betriebswirtschaftliche Institut der Deutschen Kreditgenossenschaften (BIK) GmbH - a major service provider for co-operative banks in Germany - using Tandem Computers and software from Applied Communications Inc. (ACI).

ACI says its software will enable consumers to load value onto their card from special bank terminals, or buy non-account-linked cards over the counters. It will also collect the spend transactions from the retail outlets at the end of each day for settlement and unspent funds management.

its one billionth Smart Card IC.

BIK has also licensed ACI's ATM and point of sale software to upgrade their current systems to handle the anticipated increase in transactions brought by the Geld Karte project.

ACI is already working on several other Smart Card initiatives with Mondex in the UK, First Union Bank in the US and Visa.

The pilot scheme, launched in the town of Ravensburg at the end of March, is organised by ZKA (Zentraler Kredit Ausschuss) representing the savings, public, co-operative and commercial banks. The Smart Cards are being supplied by Giesecke & Devrient and ODS R. Oldenbourg Datensysteme GmbH and it is expected that around 100,000 will be issued during the pilot. National roll-out is planned for the end of this year.

Contact: *Sandy Bold, Corporate Communications, ACI (for Europe, Middle East and Africa) - Tel: +44 1923 816393. Fax: +44 1923 816133.*

MIFARE PLUS Combi Chip

Mikron of Austria, a subsidiary of Philips Semiconductors, is developing a chip for Combi-Cards called MIFARE PLUS which will combine the benefits of contact and contactless Smart Cards communicating via contacts (according to ISO 7816) and via the contactless radio frequency MIFARE interface at a distance of up to 10 cms between card and read/write device. Mikron says the new chip will be available by the end of this year.

As both interfaces access the same memory, it will be especially suitable for applications which require both the high security standards required by banks as well as the quick handling needed in public transport applications.

The card can be loaded with value at a bank terminal using contact technology while, for payment, the user can then choose between the contact or contactless interface. In this way various applications can be combined such as an all-in-one City Card with parking, electronic ticketing for public transport and phone card.

Contact: *Alexander Harrer, Mikron, Austria - Tel:*

+43 3124 299 950. Fax; +43 3124 299 2780.

Loyalty Cards in Supermarket War

Supermarket chain Sainsbury, which has lost its market lead to Tesco, is to launch a customer loyalty card in mid-Summer.

A spokesman for the company would not give any details, but Sainsbury's interest in technology indicates that the card could be a Smart Card giving the company more development options than with a magnetic stripe card.

In the fierce supermarket war, Tesco has taken the market share since it launched its customer reward scheme in February 1995. Called the Tesco Clubcard, the scheme enables customers to collect points on the amount they spend and to benefit from promotions and in-store events.

Recently the card was expanded to include purchases at B&Q and Lunn Poly holiday shops and Tesco can now boast of having 8 million cardholders. There is speculation that Tesco is to upgrade from magnetic stripe to Smart Card technology, but *SCN* questions were countered with: "We are always looking at new ways to improve our service to customers."

Sainsbury's have taken the success of the Tesco Clubcard on board and, in the secrecy that surrounds plans to gain competitive advantage, have been developing their own card to attract customer loyalty. A major announcement can be expected within a few weeks.

Gemplus Turnover FF1.5 Billion

Gemplus reports strong financial growth of 37 per cent with a consolidated turnover of 1,482 billion Francs in 1995 compared with 1,084 billion Francs in 1994. But despite this strong increase in turnover, the group's net result of 104.5 million Francs was only marginally up from the 103 million Francs reported in 1994. Gemplus blamed increased competition on prices and delays on major programmes, mainly effecting the phone card, for the slowdown.

Gemplus currently operates in 20 countries and its international presence has been reinforced by the acquisition of DataCard's card production and personalisation centres last September in the United

Email Alex_h@mikron.co.at

States, Germany, The Netherlands, United Kingdom and Belgium, as well as setting up commercial bureaus in Russia, South Africa and Australia. As a result, 88 per cent of the group's turnover came from export orders.

In addition to the acquisition of DataCard's production and personalisation services, 1995 highlights included the takeover of NetOne, a Gemplus partner and customer in South Africa where it has orders for one million cards; and an alliance with Hewlett-Packard and Informix to develop personal Smart Cards.

During the year, the group's monthly production capacity climbed to 25 million Smart Cards and 30 million conventional magnetic stripe cards (an annual total of 660 million).

Gemplus, which celebrated the delivery of its 500 millionth phonecard last year, claims 43 per cent of that market, and 39 per cent of the market for cellular mobile phone SIM cards with more than 95 customers worldwide.

Contact: Flavie Gil, Gemplus Press Office, France - Tel: +33 42 32 56 83. Fax: +33 42 32 51 17.

Floral Design Phonecards

ACC Long Distance UK, a long distance telephone service provider, has announced its first series of limited edition, themed pre-paid payphone cards, called the Flower Collection. The collection started with Anemones and will be followed with Sunflowers in July, Lupins in October and Snowdrops in December.

Each flower in the series will be featured on just 5,000 25 unit cards, 14,000 50 unit cards and only 1,000 100 unit cards.

ACC would not name their card supplier but the pre-paid card has the Siemens SLE4406 40 bits EEPROM chip to secure closed user group applications.

Chris Bantoft, ACC Managing Director says he expects the limited edition cards to create a surge of excitement from card collectors. Cards can be purchased directly from ACC by either calling **+44 1223 577777** or writing to: Eleanor Hardy, ACC

Long Distance UK Ltd., St Andrews House, St

Mondex Trial in Canada

Northern Telecom (Nortel) has announced that it is to supply its Millennium public access terminals and Vista screen phones to Bell Canada for the Mondex electronic cash pilot in Guelph, Ontario, Canada. The trial is being organised by the Canadian Imperial Bank of Commerce and the Royal Bank of Canada working with Bell Canada.

Bob Cheriton, Vice President of Bell Canada's Card Strategy, said: "In addition to giving consumers more payment options, including making their phone calls, very soon people will be able to obtain cash from the convenience of their own home using a Vista screen phone, or from any public location where a Millennium terminal is located."

Tim Jones, Chief Executive Officer, Mondex, welcomed the involvement of Nortel as a significant step in the development of Mondex as a global payment system. "This news is not only important for Mondex in Canada, but for Mondex worldwide as Nortel's technology will help facilitate the acceptance of Mondex around the world," he said.

Both the Vista screen phones and the Millennium public communication terminals utilise large displays and simplified user interfaces which allow service providers to offer a suite of information services to consumers at residential or public locations. Many of these services are currently being offered in a Bell Canada advanced residential screen phone pilot in London, Ontario.

Nortel's screen phone offers new communication, information, entertainment and other transactional services and more than 300,000 are being used for enhanced telephony services such as visual voice mail, caller ID services and home banking.

Currently there are more than 100,000 Millennium payphones throughout North America. In addition to their Smart card capabilities they feature quick access keys that can be programmed for one-touch dialling of information services, emergency assistance, public service announcements or direct access advertising.

Contacts: Brian Murphy, Nortel - Tel: +1 214 684 8589. John Peck, Bell Canada - Tel: +1 416 581 4253. Joe Clark, Mondex - Tel: +1 416 323 3334.

Andrews Street, Cambridge CB2 3BZ, England.

Mondex Beyond Swindon

The current take up of the Mondex electronic cash card in the Swindon pilot would equate to 2.5 million Mondex cardholders in a national roll-out, claim the operators.

Ron Clark, Chief Executive, Mondex UK, says: "The figures that are coming out of Swindon are well ahead of what was achieved with cash dispensers, credit cards and SWITCH at the same stage and we are extremely optimistic about the future of Mondex beyond Swindon." He said that there are now over 10,000 Mondex cardholders - a figure representing a 21 per cent penetration of the member banks' customer base. To extrapolate these figures nationally would mean 2.5 million Mondex cardholders.

Mondex has issued the following statistics:

The average amount loaded onto the card is between £25-£30 broadly mirroring how people use their ATM cards.

Most purchases are for less than £5, the most frequently purchased items being newspapers, fast food, confectionery, bus fares and car park tickets.

Higher value transactions are largely seen in supermarkets - the biggest single collectors of Mondex value - followed by department stores and petrol stations.

Mondex has now become the preferred method of payment according to 66 per cent of cardholders in a sample survey, with cash slipping to 32 per cent.

An overwhelming 85 per cent are either satisfied or extremely satisfied with Mondex and 77 per cent feel that Mondex is safer to carry than cash. A total of 90 per cent found the card easy to use.

In a major marketing push, a variety of local businesses are offering Spring discounts to Mondex cardholders in Swindon which should further boost the number of cardholders and transactions while demonstrating the versatility of the promotions which can be offered via the card. Money saving offers for cardholders include discounts at pubs, restaurants, cinemas and for car hire; points and tokens at petrol stations and cheaper local bus fares.

Contact: Gerry Hopkinson, Band & Brown

Communications - Tel: +44 171 704 2010. Fax;
ecash Payments on the Internet

EUnet, Europe's leading provider of Internet services, has launched ecash which enables consumers to make and receive payments securely over the Internet.

The system has been launched initially in Finland and EUnet, working with major banks, intends to roll-out the service during 1996 in more of the 41 countries in which it operates.

Merita, Finland's largest bank, already processes over three million account holders with access to its Solo payment service. This now allows users to visit a "virtual ATM" on the World Wide Web and withdraw money directly from their bank account into their ecash "purse." With this money they can make electronic payments to each other as well as to on-line merchants.

Merchants already accepting ecash range from popular magazines and newspapers to those selling stock quotes and GSM paging through email. DigiCash says that soon, while travelling anywhere in Europe, consumers will be able to dial a local number and pay for Internet access via EUnet Traveller, using ecash.

EUnet's Managing Director Wim Vink, says: "We are delighted to be the first Internet Service Provider in the world to make the benefits of ecash fully available to Internet users. We see the ecash system as a major enabling technology that will make electronic commerce into an effective new way of doing business."

Matti Karvonen, First Vice President of Merita Bank, comments: "Merita has around 200,000 customers who already use terminals for their daily banking. We believe that the number will increase with the introduction of ecash and Solo payments."

Using ecash

Using ecash is like using an ATM. When connected to it via a PC over the Internet, the user authenticates ownership of the account and then requests the required amount of ecash to be withdrawn. Instead of being issued with bank notes, the customer receives digital cash which is stored on the hard disk of the PC.

+44 171 226 9742.

To make a payment, the customer confirms the amount and the payee and then the ecash software transfers "coins" of the correct value from the PC direct to the payee.

Pilot in Germany

In another development this month, DigiCash and Deutsche Bank announced that they are to launch a joint pilot project in Germany to test the use of electronic cash on the Internet.

The project will enable the bank's clients to pay for information (ranging from magazine articles to stock quotes), services (from database searches to help desk support) and tangible goods (from mail order to pizzas) using any PC with access to the Internet.

Dr Wolfgang Johannsen, Head of Deutsche Bank's Department for Technological Development, said: "In launching this pilot project, Deutsche Bank aims to test the possibilities of innovative payment forms and procedures and to expand their range of Internet services."

ecash was used last Autumn by Mark Twain Bank to issue the first ecash dollars in the United States.

Contacts: Paul Dinnissen, DigiCash, Amsterdam - Tel: +31 20 665 2611. Fax: +31 20 665 1126. Graham Wilson, EUnet, Amsterdam - Tel: +31 20 623 3803. Fax: +31 20 662 4657. Timo Nikinmaa, Merita Bank, Helsinki - Tel: +358 0 1654 2471. Mr Schumacher, Deutsche Bank - Tel: +49 69 910 33406. Fax: +49 69 910 33422.

Cassamat Electronic Purse

Cassamat, the electronic purse card launched in October 1994 by a federation of 52 rural banks in Italy (Raiffeisenverband Südtirol), is growing steadily with over 36,000 cards issued and a target of 70,000 by the end of 1997.

The card (see front page) is available to bank account holders and tourists in the Selva di Val Gardena and Merano areas. The system was developed by Italian company VERON SpA and uses their C-Less (contactless) cards with an SGS-Thomson 3K bytes EEPROM ST 16623 chip.

**Contact: Luciano Cavazzana, VERON SpA - Tel:
Thyron Terminals for Dubai Taxis**

+39 2 4821 5231. Fax: +39 2 452 4701.
future.”

Nigel Cullum, Sultan Special System's Regional Office Manager, says: "There is set to be a rapidly rising trend towards off-line mobile transactions, especially with the in-built security of Smart Card transaction processes. To this end, Thyron have developed a product that virtually has every conceivable functionality built into what is unarguably the most compact device in the world, the Financer terminal which can be used for retail payment, home banking, home shopping, transportation and all other mobile applications in the card field."

**Contact: Rohit Patni, Sales & Marketing Director,
Thyron - Tel: +44 1727 875800. Fax: +44 1727
875891.**

Emirates Bank International Limited (EBIL), which launched the disposable Stored Value Card NEW CASH in Dubai last February (*SCN March 1996*), has selected Thyron's portable hand-held Financer terminals to process NEW CASH card payments within mobile applications.

EBIL has agreed to install the Financer terminals in the new fleet of executive taxis being operated by the Dubai Transport Corporation (DTC). Thyron has worked with local partners, Sultan Special Systems of Dubai, to develop and install the terminals in the taxis to enable passengers to pay for their journey's using the NEW CASH cards. Initially, 200 Financer terminals have been installed and it is expected that over a period of two years the terminal volume will approach 6,000 units as the DTC taxi fleet grows.

The Financer terminals communicate with the EBIL host system for NEW CASH transaction collection and reconciliation into merchant accounts.

Abdulla Qassem, Business Analyst with Emirates Bank, envisages that the Financer terminal, due to its small size and off-line transaction processing capability, will be used "in the majority of mobile applications from taxis to small market stall traders who require a low-cost electronic payment terminal that will accept NEW CASH Smart Cards and also process standard credit and debit cards in the

New Chip Card Acceptors

Amphenol-Tuchel Electronics has redesigned the C702-1 Push-Matic series chip card acceptor to offer an optional locking switch. This new addition to the product range gives the design engineer the locking signal indicating that the contact carrier has locked in the end position and the chip card is fully inserted.

The design has two switches, one is integrated in the contact block assembly and detects card present while the new locking switch is actuated by the locking mechanism.

The range is available with 5, 12 and 24 volt solenoids, incorporates landing contacts and will achieve 500,000 card insertion cycles. Applications include EFTPOS, vending machines, banking and retail terminals.

Contact: Ralf Stegmann, Amphenol - Tel: +49

7131 929-0. Fax; +49 7131 929-400.

PROTON Starts National Roll-out

The National roll-out of PROTON, the Belgian electronic purse, starts this month in the cities of Namur, Mons, Gent and Mechelen. This will be followed by Brussels, Antwerp and Liège in September with all large and medium-sized towns to be covered by the end of 1997.

Banksys, operator of the Belgian network for electronic payment - Bancontact / Mister Cash - says the necessary infrastructure will be in place by early 1997 to combine the Bancontact / Mister Cash and PROTON functions on a single card for all banks which wish to do so.

The PROTON reloadable chip card, which can contain up to a maximum of 5,000 francs, was successfully tested in Wavre and Leuven. As roll-out begins, the card can be obtained in almost all bank branches in the country and the system is available to all merchants and closed user groups such as companies, universities, large schools, hospitals to replace cash money in restaurants, shops and vending machines on their premises.

Currently, Banksys and Belgacom are looking at recharging the PROTON card at public payphones. Banksys has already developed an intelligent terminal, the C-ZAM / Phone which enables cardholders to recharge their cards from home.

Banksys says that town administrations are interested in replacing their old parking meters with new ones able to accept PROTON. A prototype of

a portable parking meter is currently under laboratory testing and will be made available if there is market demand.

PROTON technology has been sold to Interpay for the Dutch electronic purse, Chip Knip; to Telekurs for the CASH electronic purse in Switzerland; and to Brazilian company Mitel for use in the Banco do Brasil electronic purse pilots. Finally, Australian company ERG signed a contract for the Quicklink consortium whose card, based on PROTON, is being piloted in Newcastle, New South Wales, Australia. ERG has also acquired a licence for Hong Kong and New Zealand.

Hardware and transaction prices are as follows:

Terminals: Purchase: 15,000 to 17,000 francs
(depending on model)
or a lump sum: for shopkeepers: 140 BEF / month
(4 night transfers included) for
20,000 BEF turnover
for vending machines: 250 BEF /
month (4 night transfers included)
for 12,500 BEF turnover
Commission on the transferred amount:
0.7% for shop terminals
2% for vending machines
transfer to bank account during the
day: 20 francs - at night: 8 francs.

**Contacts: Youri Tolmatchov, Communication -
Tel: +32 2 727 6666. Fax: +32 2 727 2727. Jean-
Benoît Van Brunnen, Product Manager - Tel: +32
2 727 6372. Fax: +32 2 727 6767.**

BiPay Smart Card from GPT

GPT Card Technology is to demonstrate its new BiPay Smart Card combining both contact and contactless Smart Card technology at the CardTech/SecuriTech '96 exhibition in Atlanta, Georgia, USA, this month.

The demonstration will illustrate the secure transfer of value from the contact purse area of the card to the contactless purse area, enabling a single card to be used for many different applications.

Paul Seward, General Manager of GPT Card Technology, explained: "The card has been designed to provide the customer with the flexibility of a contact Smart Card, for use in electronic purse applications for example, and the convenience of a contactless card which is ideal for fast moving applications such as mass transport ticketing.

Range of cards

GPT will also be demonstrating a range of microprocessor contact Smart Cards designed for specific industry sector applications. These include the GPT Loyalty card, the GPT Leisurecard, designed to hold personal and club membership details whilst allowing value to be added or deducted as necessary.

Also on display will be the GPT Healthcard which is capable of holding a patient's personal and health insurance details and full medical history. Different levels of access to data stored on the card is obtained using PIN codes and an additional PIN used to allow medical records to be updated.

The secure transfer of electronic cash via two GPT-designed Mondex payphones will also be demonstrated.

GPT Card Technology is part of GPT Payphone Systems, the world's largest payphone company. The card division looks set to add a combined contact and contactless card to its three core technologies GPT Imprint Magnetic (GIM) cards, GPT Integrated Smart (GIS) cards and GPT Integrated Contactless (GIC) cards.

Contact: Lisa Bush, GPT Press Office - Tel: +44 115 943 3687.

Industry Guide Available Now

The *International Smart Card Industry Guide* published by, and only available from, Smart Card News Ltd., is now available.

This second edition, even more comprehensive than the first internationally acclaimed publication, is essential reading for everyone in the industry. It contains the key information you need to function in a fast-moving industry - information on the latest/major projects, including electronic purses; and a directory of companies with descriptions of their products and services together with contact names, numbers and addresses.

In addition there are feature articles on the technology, patents and intellectual property rights, and an extensive glossary.

The book is an essential reading and reference book if you want to keep up to speed on Smart Card technology.

Priced at only £125 plus postage and packing, the Guide is the single most important Smart Card reference book to have on your desk.

Subscribers to *Smart Card News* can obtain the Guide for £70 including postage and packing.

To order: write, telephone, fax or e-mail Smart Card News Ltd - details on inside front cover of this

newsletter.

Data Protection on the Cards

Smart Cards offer a huge potential to the public but this will be lost unless public trust can be guaranteed by giving individuals control over personal information, says independent think-tank Demos.

Its report, the first comprehensive analysis of the policy issues raised by the rapid proliferation of Smart Cards in financial services, business, telecommunications and public services such as health and social security, warns that the benefits will only accrue if there is public trust that Smart cards will not be "big brother's little electronic helpers."

The report points to growing fears about how sensitive information could be accessed by employers, insurers and others. It says four out of five Britons feel anxious about how personal information is used and 80% of Americans say that they have lost control over information about themselves.

The authors offer a strategy away from what it describes as the "unhelpful" polarisation of the debate between civil libertarians and authoritarian government and business interests in promoting the benefits of Smart Cards.

They argue against any government-provided multi-functional identity card as proposed by Home Secretary Michael Howard, but point out that the government has yet to announce if it will introduce an ID card and if it will be a Smart Card.

Strengthening protection

The report proposes strengthening data protection law, for example, unless the data subject expressly consents to a specific use or disclosure of personal information, that use or disclosure should not be permitted except in the core functions of government concerned with security and law enforcement. Data subjects should have the right of independent access to their records, and there should be measures to control data matching.

It argues that individuals should be able to buy "blank" multi-functional Smart Cards with privacy-respecting architectures from agencies that they trust and decide for themselves what information

and data will be loaded.

The researchers say that there should be a wider use of privacy-enhancing technologies such as encryption and argue that there should be regulation to encourage a voluntary system of independent, non-governmental registries that would hold, on a confidential basis, companies' and individuals' cryptographic keys. Government law enforcement agencies would need a court order on the basis that they had strong reason to believe a crime was involved to gain access to these keys

On the cards, by Perri 6 and Ivan Briscoe, is available from Demos, 9 Bridewell Place, London EC4V 6AP, UK. £9.95 (plus 60p p&p). **Tel: +44 171 353 4479. Fax: +44 171 353 4481.**

New UK Benefit Payment Card

Peter Lilley, UK Secretary of State for Social Security, has announced that 19 million people are to be issued with plastic payment cards for claiming benefit. These will be linked to a computer system which will contain personal details, such as relatives' maiden names, and holders may be asked random questions to ensure that they are who they say they are.

The cards will not be Smart Cards, but Mr Lilley says the computer network will be a "smart" system capable of using Smart Cards in the future. The new system will be phased in this Autumn for the payment of benefits and utility bills.

At the same time, the Commons Social Security Committee reported that as many as one in five claims for housing benefit could be fraudulent, costing UK taxpayers up to £2 billion a year.

The Committee called for an immediate investigation of all private landlords who receive more than 20 housing benefit payments each week, and for a task force to establish the extent of fraud over national insurance numbers after evidence that millions of inactive numbers still exist.

The report also wants a review of the Data Protection Act which some investigators say is hampering data matching schemes where benefit claims, tax and employment records can be compared.

Housing Benefit Fraud: Third Report of the Social **CarteS SESAMES '96 Awards**

CarteS '96, the leading plastic card conference and exhibition in Europe, is creating the SESAMES '96 awards for the year's best innovation and application.

The contest is open to all companies in the global plastic card technologies and applications sector.

A panel of judges will be formed consisting of five journalists from the trade press in the United States, United Kingdom, France, the Asia Pacific region and Germany. Eurocard / MasterCard is the official sponsor of SESAMES '96 which is also being supported by the Smart Card Club in the UK and the Smart Card Forum in Germany.

A spokesperson for CarteS said: "The SESAMES '96 contest represents a major and exciting event in the market for plastic card technologies and applications and will provide an outstanding showcase for all of the year's new applications and innovations."

The closing date for entries is **30 June, 1996**. Persons wishing to obtain entry forms or additional information should contact *Patsy Everett, Director, Smart Card News, UK - Tel: +44 1273 626677. Fax: +44 1273 624433.*

Cryptocontroller from Siemens

Siemens Semiconductor Group has announced the new SLE 44CR80S cryptocontroller for Smart Cards and claims new standards in terms of memory capacity and integration density.

It says it is the first company to pack 17K bytes of ROM, 8K bytes of EEPROM and 256 bytes of internal RAM as well as a 540-bit coprocessor for rapid processing of asymmetrical crypto algorithms onto a chip area of less than 15 mm².

The cryptocontroller is designed for applications such as banking, electronic commerce via the Internet and high security applications.

Siemens says power consumption is typically 3mA when operated at 3V. In sleep mode without an external clock applied the current drain is even reduced to as low as 35µA. The chip can be

Security Committee 1995-96; HMSO £11.50.

operated at 3V and 5V and frequencies of up to 5 MHz (7.5 MHz on request) without external clock dividers.

The EEPROM can be programmed with a page width of 32 bytes at a rate of 3.5 ms per page. This combined with the 76.8-kBaud data rate additionally supported by the CPU produces a fast data interchange via the serial interface.

The 540 bit crypto-coprocessor supports all known modular arithmetic based crypto algorithms. It also offers short execution times of 220 ms for an RSA 512 bit standard encryption or of 450 ms for 1024 bit RSA employing the commonly used Chinese Remainder Theorem.

Siemens says the SLE 44CR80S is already available in engineering samples with volume production scheduled for summer 1996.

Contact: Corporate Communications, Siemens AG - Tel: +49 89 234-0. Fax: +49 89 234-2824.

ORGA Smart Road Show

ORGA Card Systems (UK) is hosting a UK-wide educational Road Show for businesses and individuals who want to improve their knowledge and understanding of Smart Cards.

A total of six one-day seminars will be held from 9-16 July at venues in Scotland, the North-West, North-East, Midlands, South-West and London. The seminars include presentations on Smart Cards, their applications in various business sectors such as banking, leisure, retail, security and telecommunications, and demonstrations of systems and equipment.

The nominal cost is £25. Book by fax: **+44 1491 410295**.

SuperPass Leisure Card

Innovatron Data Systems has installed its FUNCHIP Leisure system for the management of a leisure centre in Les Balnéades in France.

Some 4,000 reloadable Smart Cards (see front page) have been issued with an electronic purse for

purchases in Les Balnéades' shops and with units to

Smart Card Diary

Plastic Card Payment Systems, Siam Intercontinental Hotel, Bangkok, 4/5 June.

Conference focussing on standardisation, electronic purse applications, loyalty cards etc and an overview of card systems in Thailand and Asia. Centre for Management Technology: Ms Sukita, Bangkok - Tel: +662 266 7767-8. Fax: +662 237 2189; Ms Sheelah John, Singapore - Tel: +65 345 7322. Fax +65 345 5928.

Passenger Distribution '96, Kuala Lumpur, Malaysia, 24/25 June.

A conference organised by IATA to explore enabling technologies and develop a common vision of the future distribution system. Leanne Donohue, IATA Seminar and Exhibition Services, Switzerland - Tel: +41 22 799 2757. Fax: +41 22 799 2674.

Driving Strategic Change in Purchasing Through Procurement Cards, The Cavendish Square Conference Centre, London, 8 July.

A separately bookable one day workshop, A Practical Guide to Implementing your Procurement Card Scheme, takes place on 9 July. ICM - Tel: +44 171 436 5735. Fax: +44 171 436 5741.

Cards Australia '96 Conference & Exhibition, Sydney Convention & Exhibition Centre, Sydney, Australia, 20-22 August.

Three-day trade exhibition and a multi-streamed conference organised by the Asia Pacific Smart Card Forum and AIC Exhibitions to cover Smart Cards, Stored Value Cards and electronic purse, co-branded/loyalty cards and procurement cards. Erika Morton, AIC Exhibitions, Australia - Tel: +61 2 210 5704. Fax: +61 2 223 9216.

ICMA 6th Annual Card Manufacturing Expo, Bermuda, 21-25 October.

The annual gathering of the International Card Manufacturers Association which has taken "The Globalisation of the Plastic Card Industry" as this year's conference theme. Lynn McCullough at ICMA - Tel: +1 609 799 4900. Fax: +1 609 799

pay entrance charges.

Sligos Sustains Recovery

Groupe Sligos showed a net income of 88.7 million French francs, equivalent to a net margin of 2.1%, for the year ended 31 December 1995.

The Groupe says that 1995 was a watershed year shaped by sustained recovery thanks to a return to break-even of the Information Systems business whose turnover increased by 7% over the year; a refocusing on the Group's four core businesses and the divestment of CMG.

It reports that early this year all of the business segments won new contracts in promising areas such as healthcare in France, the production of phonecards in China, secure Internet transaction payments systems, and large information systems for the European Union and for French water utilities.

It forecasts that the current year should see a continuation of growth, investment and recovery.

Contact: Boris Eloy, Groupe Sligos - Tel: +33 1 49 00 96 33.

80% of UK Payments are in Cash

Cash still accounts for over 80 per cent of all payments in the UK and most people obtain their spending money from one of the UK's 21,000 cash machines, says the Association for Payment Clearing Services (APACS).

Last year almost a quarter of the £1.4 billion withdrawn each week from cash machines was taken out on a Friday while on an average Sunday only about £88 million is withdrawn making it the quietest day of the week for withdrawals despite the introduction of Sunday trading.

In 1995 there was a 10 per cent increase in both the number of withdrawals made from cash machines and in the average amount of cash withdrawn. Banks and building societies installed over 700 new "remote" machines sited at various busy locations such as supermarkets and railway stations.

Contact: Richard Tyson-Davies, Head of Public

Affairs, APACS - Tel: +44 (0)171 711 6234. Fax:
+44 (0)171 256 5527.

Electronic Commerce and Payment Mechanisms Part 3

Authentication

This is a primary security property that is used to assure the receiver that a message comes from the purported originator. The fundamental security service is to authenticate the correspondent party as part of an access control security service. In its simplest form we are used to the use of passwords.

The receiver in this situation verifies the identity of the other party by checking the validity of a supplied password. There are a number of problems here, in the first instance if we use a static password then any listener on the line could overhear the password and reestablish an apparently genuine link at some later time. This problem can be avoided by using dynamic passwords where for each session a new password is used. These passwords can be generated algorithmically by using one way functions or can more simply be applied by pre-storing tables of passwords. The second problem relates to the security of the password at the host site. Clearly the passwords of all authorised users must be stored in a secure way. Again the use of one way functions allows the host to store the passwords as the output of this one way function where the inverse function of computing the password is deemed practically infeasible.

In the example quoted it is necessary for the user to provide a secret as the core of the authentication process. A better approach is to provide proof that the user has knowledge of a secret without actually revealing the secret. Fiat and Shamir first proposed an identity verification technique based on zero knowledge proofs. In other words the verification process does not provide any knowledge about the stored secret. Quisquater and Guillou proposed a simple explanation of this concept by describing a "secret cave" shown in *figure 5*.

Here we have a cave with a secret door joining two apparently dead end passages. The owner of the secret knows how to open the door joining the two passages A and B. The prover and verifier start off by standing outside the entrance to the cave. The prover rushes into the cave and travels down one of the passages A or B. The verifier

then comes into the cave and stands at the point X where the two passages A and B diverge. He calls out to the prover and requests him to emerge from an arbitrarily chosen passage A or B. Because the prover knows how to open the secret door connecting the two passages he can always emerge from the selected passage. Of course the verifier can only be sure with a probability of 0.5 that the prover knows the secret because that is the chance that the prover just selected to travel down that passage. However, if you repeat the experiment enough times and the prover always manages to emerge correctly then the verifier can be readily assured ($1:2^{\text{number of trials}}$) that the prover does indeed know how to open the secret door.

You can also see that no knowledge relating to how the secret door is opened needs to be revealed to the verifier. The mathematical equivalent of this process is shown in *figure 6*.

This identity verification technique suffers from one major problem. When the prover and verifier return to the office there is no way of proving to a third party whether the prover succeeded in the experiment. Indeed you would have to take a trusted observer with you which is not a desirable condition. The use of a challenge/response protocol takes us a little further down the road. This technique is the basis of many authentication processes and is described in term of *figure 7*. The verifier sends a random number challenge to the prover who applies a cryptographic transformation of the random number using his secret key. The resulting cipher is returned to the

verifier for checking. If the cryptographic algorithm is symmetric then the checking process will need to use the same secret key. For an asymmetric algorithm however the verification process uses the matching public key.

In the case of the asymmetric algorithm not only has the prover satisfied the necessary authentication process but it is possible for the prover to demonstrate this to a third party. Only the prover has the secret key used to generate the cipher whilst the public key used to check the response can be distributed to any other party for checking.

The property of non-repudiation is also achieved here since the prover cannot subsequently deny his actions. Symmetric algorithms however still suffer from a few short comings since the prover could deny having created the response because the verifier has the same cryptographic secret key and could have invented the whole message exchange. Thus the evidence to a third party relies on trusting the verifier. Even worse, for a third party to verify the correctness of the challenge response he needs to be provided with the same secret key.

In practice the application of such authentication techniques need to ensure that the possibility of replaying previous message exchanges can be avoided. This is usually accomplished by including additional data fields into the challenge data so that in addition to the random element a time stamp or sequence number is built into the cryptographic process.

Multi-Service Puzzle Cards

DANMØNT has announced that the first of 5,000 new card-operated payphones from Tele Denmark are now being installed throughout the greater Copenhagen area and by Christmas 1997 all card payphones in Denmark will accept the DANMØNT electronic purse card as means of payment.

To "celebrate" the start of this major installation of card payphones and to inform everyone who buys a DANMØNT card about the many opportunities they have for using their cards in different environments, DANMØNT has issued four cards forming a Multi-Service Puzzle (see below) showing the different services the card can be used for - telephones, parking meters, vending machines, laundrettes, POS terminals in kiosks, stamp vending machines etc.

The cards, supplied by Philips Smart Cards & Systems of France, each have a value of DKK 100. Information on card use is also written on side two of the cards together with information about the other three cards in the series.

DANMØNT reports that in 1995 it issued 258,887 cards mainly with the values of DKK 100 and DKK 200 and in the same period the cards were used 2.1 million times. Since the start-up of the system in 1992, the yearly increase in transactions has been over 100 per cent.

So far, more than 120 different designs have been issued during the last four years, attracting interest from collectors all over the world.

Contact: Henning N. Jensen, Managing Director, DANMØNT - Tel: +45 43 44 99 99. Fax: +45 43 44 90 30.