NatWest Launch Mondex Global Electronic Cash

National Westminster Bank has developed a new electronic payment service, called Mondex, which uses Smart Cards as an alternative to cash. Innovative features of the system enable customers to top up the value on their cards and make payments by telephone, as well as to hold up to five different currencies individually on the card.

The service will be introduced in 1995 in Swindon in a joint venture with Midland Bank in conjunction with British telecommunications company BT. This will be followed by a roll out to the banks' 11 million customers. The intention is to invite other financial institutions to join the scheme under the name of Mondex International.

Continued on page 223.

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 17 - The Electronic Purse.

CONTENTS

NatWest Launches Mondex

Continued from page 221.

The National Westminster Bank Mondex cashless shopping project is probably the most technically advanced scheme of its kind anywhere in the world offering unequalled facilities for customers and service providers.

While there are many Smart Card Electronic Purse schemes operating or being launched throughout the world, the Mondex concept is a non-accounted open payment system directly paralleling real cash. When a customer pays with a Mondex card the money is paid instantly to the retailer or service provider and the transaction does not go through a clearing system like other Electronic Purse applications. The banks have no records of the transactions and only know the amount issued in the same way as they issue cash.

Mondex is also the first system to offer:

* Twenty-four hour banking and access to electronic money by telephone - either public payphone or a home Smart Card phone.

* A multicurrency card capable of holding up to five different currencies separately.

* A personal secret code number to lock the card, preventing value in the card from being used without re-keying the code.

* An electronic wallet to which value from the card can be transferred for safer keeping at home, and to enable payments to be made from one card to another.

* A personal key ring card reader to check the balance on the card at any time.

Customers can also use the card to make payments over the telephone in the same way as they would pay at a point of sale terminal, except in this case the transfer is carried down the telephone line.

Cards can also be topped up and balances read at NatWest and Midland ATMs.

The Mondex announcement in London this month brought unexpected, strategic announcements from three major payment card issuers. Europay International, MasterCard International and Visa International issued a statement 24-hours before Mondex was unveiled that they had agreed to develop a common standard for the use of Smart Cards at the point of sale.

Two days' later, Europay's Board announced a commitment to introduce Smart Cards as their fraud prevention methodology.

Were they panicked into action by the initiative of NatWest and fear of an eventual global competitor in Mondex International?

Tim Jones, Senior Executive, IT Strategy and Policy, NatWest, who invented the Mondex concept with NatWest colleague Graham Higgins, commented on the announcements: "It is important to register that although Mondex is electronic money it is a completely different product from debit and credit cards.

"Obviously NatWest is a very important member of Europay and MasterCard and therefore we will be following with great interest the movement of the debit and credit card population over to chip cards, but in a business sense it is a different issue from the use of the same technology in Mondex."

Swindon trial

The service will begin with a trial in the town of Swindon (population 114,000) in Wiltshire, England, involving about 1,000 merchants and service providers and around 10,000 consumers, before being rolled out to customers nationally.

NatWest has spent over three years developing the system and has gained practical experience with Smart Cards in the Byte project running at their computer centre at Goodmans Fields, London (SCN September 1992). So far, about half-a-million card transactions have been carried out and technical proving will continue throughout 1994.

Global scheme

NatWest will be actively seeking banking partners

worldwide to establish Mondex as the basis for a global electronic cash payment scheme.

This was emphasised by Derek Wanless, NatWest's Group Chief Executive, who said: "Although Mondex will be launched in the UK, it is a major commercial opportunity for banks everywhere. Mondex is a multicurrency product, capable of holding up to five separate currencies on a card simultaneously.

"It is the intention to invite other institutions in the UK to join Mondex in due course and to recruit major institutions worldwide with the intention of forming a new company, Mondex International, which is capable of becoming a truly global payment scheme."

Chris Wathen, Midland Bank's Managing Director, Branch Banking, said: "The flexibility and freedom that Mondex provides will make the service attractive to all types of user, be they personal customer, retailer or service provider."

Bruce Bond, BT's Group Director of Products and Services Management, said: "Mondex is a major implementation of Smart Card technology and BT is delighted to be working at the forefront of such communication developments. BT believes that Smart Cards will play a key role in providing new and innovative services.

"With Mondex, customers will be able to use BT's extensive pay phone network greatly increasing the opportunities to access cash."

Industry reaction

A spokesman for Barclays Bank, who trialed Smart Card technology in their Darlington Country Club project, said: "We will be monitoring closely the pilot scheme that NatWest and Midland have announced in conjunction with BT. We will ourselves continue to research the viability of that type of card technology and the business opportunities it present for us.

"It is certainly the way forward and one that we will look at closely."

Lloyds Bank said "Mastercard and Visa have announced that they are going to develop a common chip and this is a route we would want to go down."

Welcomed by retailers

The Mondex launch was welcomed by the British Retail Consortium as providing an alternative to cash, which is currently the prime retail payment medium in terms of value and usage. They said the 1995 trial is seen as a key step in establishing customer, retail and bank benefits, and hence the system's commercial viability.

James May, BRC Director-General, commented: "If successful, the Mondex trial should give UK shoppers a better way of paying, and provide retailers with benefits in this the first step towards a cashless society."

Michael Wilsey, Director of Professional Services at BRC, said the system has advantages to retailers, one of them being the built in security to be able to do away with authorisation calls. Hopefully, it will almost mean the end of the cheque over the counter and the arguments over fraudulent signatures.

"The charging arrangements are crucial for any system and this is no exception," he said. "Let's hope they get it right because if it's wrong and it's too expensive for retailers and customers they will walk away from it. The banks will then be left with something they can't use.

"They are very anxious that the charging is done in a thoroughly equitable way so as to bring everyone onboard. It's a bit of a gamble, I think, but it could have a very big pay-off."

Contacts: Paul Lockstone, Head of Public Relations, UK Branch Business, National Westminster Bank - Tel: +44 (0)71 726 1834.

Brendan Le Morvan, Head of Media Relations, Midland Bank - Tel: +44 (0)71 260 8205.

Paul Sharma, Technical Press Officer, BT Corporate Relations - Tel: +44 (0)71 356 5369.

Card Issuers Take Smart Route

Three major payment card issuers - Europay

International, MasterCard International and Visa International - this month took significant moves towards utilising Smart Card technology.

The move by top players in the financial sector, has long been awaited by the Smart Card industry, and will eventually give a massive boost to the wide use of Smart Cards.

First came an announcement from Europay International headquarters in Waterloo, Belgium, that the three organisations had agreed to form a joint working group to develop common technical specifications for the integration of microprocessor chips in payment cards, which they said would "facilitate the worldwide introduction of Smart Cards." The standard will be based on work already done by ISO, the International Standard Organisation, and is targeted for completion first quarter 1994.

Europay to Introduce Smart Cards

In a surprise move two days later, the Europay International Board of Directors announced their decision to introduce Smart Cards as a fraud prevention methodology.

Europay has over 84 million cards and nearly 81,000 ATMs accepting its products, making it the European banks' leading provider of personal payment and related services. It is sole licensor of the eurocheque, CIRRUS, edc and Maestro, and Eurocard-MasterCard brands in Europe.

Referring to the earlier announcement by the three organisations, the statement said they and MasterCard International members would soon have available Card Authentication Method (CAM) and Cardholder Verification Method (CVM) specifications, physical, electrical and data requirements of the chip as well as terminal and interface specifications.

Ron H Williams, Director and Chief Executive Officer of Europay, said research had built a "strong business case" for the chip card.

Card authentication methods combined with cardholder verification methods, and risk management features based on chip technology, provides a solid basis to reduce significantly fraud, counterfeiting and credit risk. With lost/stolen cards and counterfeiting accounting for over 80% of fraud losses, Europay says chip cards will "deal a major blow to fraudsters."

Europay's business case addresses three primary areas:

Fraud and Risk Management:

* CAM - Protects the integrity of the card.
* CVM - Cardholder verification with PIN as today's CVM in both on- and off-line environments.
* Credit risk management parameters can be set by the issuer on a card by card basis and updated whenever the card goes on-line.

Pre-paid/Purse Applications:

* Europay will provide an opportunity for domestic "pre-paid" schemes to expand internationally. This could apply to all of Europay's segmented product range: Pay Now (debit) and Pay Later (credit).

Value-Added Services:

* A new dimension of value-added services, ranging from extended, personalised T&E products, travel information, car rental, hotel services as well as individualised credit control features and services to merchants and banks. Europay's specifications will reflect the growing market demand for these services.

Finally, Europay says that the advantage of chip over mag-stripe technology, watermark or holomagnetics, is its ability to provide a common, upgradable and flexible solution to all of the above applications. In addition the technology can be adapted to include any future cardholder verification methods such as biometrics, while value-added services, pre-paid or electronic purse applications can easily be introduced.

Contact: Philip Andreac, IT Strategy Director, Europay International - Tel: +32 2 352 5400.

Chemical Bank Smart Cards

Chemical Bank and AT&T Smart Cards have announced a strategic alliance aimed at

introducing Smart Card banking applications into the New York City, USA, market.

"We see Smart Cards as an opportunity both to offer our customers greater convenience and control over their funds, and to reduce fraud by providing a more definite customer identification," says Ronald Braco, Chemical Bank's Senior Vice President for Electronic Banking.

The announcement was made at the Retail Delivery Systems conference - the automated teller machine (ATM) industry's largest annual trade show - in New Orleans this month.

It is planned to trial the card with a number of Chemical Bank employees in New York City who will be issued with Smart debit cards that can used for purchases in the bank's cafeteria. They will be able to transfer cash value to the cards from their bank accounts at select Chemical ATMs to be equipped with Smart Card readers.

If the trial is successful, it is intended to expand the trial internally and add other applications to the card. Chemical Bank say that later they will consider offering the new cards to its broader customer base.

Electronic cheque book

Braco commented: "Smart Cards can, and probably will, change the entire nature of consumer banking. We see the Smart Card becoming the primary vehicle for delivering transaction and information services to our customers. A single Smart Card can serve as debit, credit and ATM card, all in one. Customers can access the cards from ATMs, telephones, interactive TV sets, and merchants' point-of-sale terminals."

He added: "The Smart Card could become the electronic cheque book of the future, reflecting all of a customer's payment transactions".

The two companies are considering other ways the Chemical Bank cards might be used in the New York market, including retail, the electronic delivery of government benefits, transit and health care applications.

AT&T's cards are contactless cards with 3K bytes of EEPROM, and are currently being used, for example, in road tolling applications in California, physical access control to buildings in Japan, Electronic Benefit Transactions in Italy, and logical access control to computer systems in the United States.

Upgrade Kits for NCR ATMs

AT&T's NCR division is to supply the Smart Card-compatible ATMs to Chemical Bank.

At the same trade show they announced upgrade kits for NCR ATMs and other self-service terminals that allow the machines to accept AT&T contactless Smart Cards as well as conventional magnetic stripe bank cards. New self-service terminals can also be ordered from NCR with this capability.

"These new readers allow banks the flexibility of simultaneously supporting both the conventional magnetic stripe cards and Smart Cards," says Danny O'Brien, Assistant Vice President of NCR's Financial Products and Systems Division in Dundee, Scotland.

"This means upgraded ATMs can still accept mag-stripe cards from other banks, while the bank that owns the ATM can phase in Smart Cards with its customers."

Available first quarter 1994

The reader upgrade kits will be available to selected customers on a trial basis in the first quarter of 1994, and will become generally available later in the year.

AT&T Smart Cards will provide turnkey software to each bank purchasing upgrade kits, as well as technical assistance in developing customized applications for the Smart Cards.

Contacts: Michael Jacobs, AT&T Smart Cards - Tel: +1 908 582 4767; Judy Walsh, Chemical Bank - Tel: +1 212 270 2914; Chris Stellway, NCR Corporation - Tel: +1 513 445 4178.

Italian Play Card System

A pre-paid Smart Card, called the Play Card, is being used in Italy to replace coins in game rooms and casinos, while a more advanced Electronic

Money System which evolved from it can be used in hotels, bars, clubs, discotheques, amusement parks and holiday villages etc.

The Play Card system is available from ELMAC, who are the exclusive distributors for Italy for Paytron, who design and manufacture advanced systems for the control of electronic money.

Paytron's first Electronic Money System (EMS) application was the Play Card which was tested and approved in pilot systems over two years before being put into standard production.

The protected EEPROM microchip can only be accessed to vary the data through password codes. In the case of repeated attempts (up to three times) to transmit wrong code, the chip self-destructs and the card becomes unusable.

Variety of cards

The system is designed to provide security and for the operator to exercise control. There are a variety of cards depending on the application. The Client Card records the equivalent of prepaid amounts of money (credits). Amounts used are deducted from the card and bonus points and winnings are added. (In the Hotel Card System, the card allows the user to make payments for goods and/or services on credit, debited to an expense account and payable later.)

Two further Client Cards are available and can be initialised either as a VIP Card, which allows a more extensive personal credit rating, or as an Order Card, with more limited credit ratings.

Management Cards to access the accounting of the sales outlets are available at three levels. The Card Master allows complete screening of accounting (money collected at the time of access, during the day or during the year; percentages on intakes, discounting operations, etc). This is the key to the whole system present at one outlet or in a chain of commercial outlets, and represents the top level of management responsibility.

The Operator Card allows access to partial accounting and is held by the operator in charge of collecting and controlling the intakes. The Controller Card only allows checking of one cash register.

Paytron say that over 800 of their EMS systems are already in operation in different parts of the world.

Contact: Ing. Tiziano Tredese, ELMAC, Italy - Tel: +39 49 897 6176; Fax: +39 49 897 6179.

Barcelona Baby Card

Babies born in Barcelona, Spain, are given a Smart Card with their name on it. While the babies are not impressed, their mothers like the idea as they can use it with the electronic baby weighing machines that can now be found in many pharmacies.

The card records the date and the baby's weight and enables the weighing machines to print out a chart plotting the baby's progress.

This is just the first step in improving healthcare for newly-born babies in Spain. It is also planned to include information on the baby's height and vaccination record, and it could even be possible to extend the card's role in pre-natal care by including the dates of ultra-sound examinations.

Spanish company Telemat SA developed the baby scales while the application was developed by Jetic, a Gemplus value added retailer in Barcelona which specialises in Smart Card solutions. The card used is the Gemplus GFM 2K bytes card.

Contact: Telemat, Barcelona, Spain - Tel: +34 3 464 3072. Fax: +34 3 464 3464.

Laundry Machines Take Danmont

Meile and Electro-lux, manufacturers of laundry machinery, have installed or are in the process of installing, laundry equipment accepting the Danmont pre-paid card in laundries in a dozen towns and cities in Denmark. One of the latest orders is for eight more laundries in Arhus, Denmark's second largest city.

Nissan Car Life Card

Nissan Carlife Network Company, a subsidiary of Nissan Motors, with headquarters in Tokyo,

Japan, was set up in July 1989 to launch a Smart Card-based customer loyalty and service card which now has 450,000 users.

NTT Data Communications Corporation, which has a 10% stake in the joint venture company set up with an initial capital of Yen 480 million, designed and developed the IC cards and the hardware.

The Smart Card holds the personal identity of the user - name, address and telephone number - and the vehicle history, including service and maintenance records, and payments, making quick and accurate service possible throughout Japan regardless of region or sales channel.

The Nissan card is accepted by all Nissan dealers in Japan and entitles the cardholder to a basic 5% discount, and at the dealer where the card was issued, to an accelerating discount rate according to the number of service visits and accumulated amounts of use of credit.

An important feature is that the cards have credit functions, allowing users to drive without the worry of not carrying sufficient funds in case of an accident. Member cards can also be used at a variety of companies affiliated with Nissan, including travel agencies, car rental agencies, hotels and petrol filling stations.

Member benefits also include Nissan information bulletins, a leisure guide, and complimentary tickets for motor sport events.

Three types of cards

In 1992, NCN signed an agreement with JCB to provide value-added services for its customers by providing them with additional services ie use the cards as a credit card at 2.5 million JCB member stores and leisure facilities in Japan and abroad, and JCB loan services in addition to the Nissan automobile loan plan.

A similar scheme was arranged with Visa in April of this year, bringing the types of cards issued by NCN to three - the Nissan Car Life IC Card (basic functions), Nissan Car Life JCB Card and Nissan Car Life Visa Card.

NCN say there are no current plans for any further tie-up with credit card companies or expansion of services.

Membership charge for each card is Yen 1,030, plus an annual charge of Yen 1,278 for the IC Card and Yen 2,317 for the JCB/Visa IC Cards. The validity period is five years.

The Smart Cards, supplied by NTT Data Communications Systems Corporation, are produced by Dai Nippon Printing Co. Ltd using chips supplied by Hitachi.

Contact: Julia Smith, Corporate Communications, Nissan Europe, The Netherlands - Tel: +31 20 516 2222.

Danyl Supplier for MAC Project

Danyl has been appointed exclusive Electronic Point of Sale supplier of certain vending-related products to be used with the MAC Stored Value Card project in the United States.

MAC, the Money Access Service network, is owned by Electronic Payments Services Inc., the largest processor of ATM transactions in the US.

The MAC Card (SCN December 1992) is a Smart Card electronic purse application. After loading the card with dollar value at a MAC ATM or a cash-to-card machine, cardholders will be able to use the card instead of cash at designated fast food restaurants, convenience stores, pay phones, toll gates, vending machines, mass transit stations, parking garages, and other locations.

Contact: Robert J Merkert Sr., Executive Vice President, Danyl Corporation, USA - Tel: +1 609 234 8000.

Banks Supporting Danmont

Banks in Aalborg, Denmark, are introducing the Danmont pre-paid card to their business customers, and will also be approaching providers of public services such as parking meters, telephones and newspaper dispensers.

Electronic Tolling for UK

The British Government is to introduce an electronic tolling system on UK motorways within five years, said John MacGregor, Secretary of State for Transport, early this month.

Vehicles will not need to stop or slow down, and tolls will be worked out automatically and either charged to the road user's account or deducted from a pre-paid Smart Card on the vehicle.

The Government is also to talk with the construction industry and others to identify a list of potential DBFO (Design, Build, Finance and Operate) road projects which could provide private sector investment.

"By the New Year we will start the formal process of consultation with the private sector on relevant technology," said Mr MacGregor. "This can include, for example, in-vehicle tags or Smart Cards and roadside sensors. These systems will be tested in laboratories and a high speed test track. Complete systems will then face more gruelling tests on a motorway itself. These tests will begin within a year."

The Government was keen, he said to avoid traffic diverting from motorways to other roads so charging at levels well below those used in other countries. An illustrative maximum for cars of 1.5p a mile would mean a charge of only £1.50 for travelling from London to Birmingham. Proceeds of charging would be applied to construction and operation of the charged network, and the Government would take into account the relationship between tolls and existing motoring taxes in setting their respective levels.

The motorway network carries 15% of all road traffic and 30% of heavy goods vehicle traffic, he said. It was vital to keep these arteries flowing for the country's economic prosperity and to prevent traffic spilling onto roads not designed to cope with it.

Electronic tagging systems are already used in Britain, for example, on the Dartford River crossing, but Mr MacGregor's announcement that Smart Card technology is also being considered is good news for the industry.

A number of electronic tolling systems using Smart Cards are already in use or being planned in various countries.

In Italy, the Telepass autotoll system designed for Societa Autostrade, the Italian company responsible for most of Italy's motorway system, uses AT&T contactless Smart Cards and has been in operation on the motorway between Milan and Como since mid-1991.

The Swedish National Road Administration has initiated a road toll test scheme called ADSW - Automatic Debiting System for Sweden. The test site is an urban arterial road near Gothenburg and the system uses Gemplus Smart Cards.

France also plans to automate the toll system on its motorways. USAP, the French umbrella organisation of France's eight motorway companies has awarded a contract to a Swedish/French consortium with full-scale installation work scheduled for 1995. The system will use Smart Cards. Also in France, the Prado-Carenage Tunnel constructed under the Mediterranean port of Marseilles, opened this Autumn and uses Gemplus Smart Cards for the automatic collection of tolls. The tunnel is a privately-funded venture to be paid for by the tolls paid by users.

In the United States, a Smart Card-based electronic toll collection system is being installed on three new toll roads in Orange County, California. The project will use AT&T contactless Smart Cards.

However, in addition to the lead that Smart Cards have taken in electronic motorway charging, a strong attraction for the system operators will be the versatility of the Smart Card. The development of multi-application cards and the Electronic Purse, give it a clear advantage over other systems. With the same card it is possible for the cardholder to use it to pay for petrol and oil at motorway service stations, snacks and meals in the cafeteria or restaurant, purchases in shops, telephone home, fax the office, while off the motorway it can be used for drawing cash at an ATM, parking, tickets for public transport, etc.

Contact: Department of Transport - Tel: +44 (0)71 276 0800.

The Mondex system which will be trialed in Swindon, comprises the Mondex cards, key ring readers, electronic wallets, specially adapted ATMs, Mondex telephones (public and/or residential), and merchant Point of Sale terminals. Specifications will be available to all potential suppliers who, subject to type approval, will be able to market any Mondex product.

Mondex card

The Mondex card stores electronic cash value and is the key to the system. The Smart Cards are ISO ID1 standard size and are fabricated by Dai Nippon Printing Co., in Tokyo, and supplied through SPOM Japan. They incorporate an Hitachi H8/3101 chip with 10K bytes of ROM, 8K bytes EEPROM and 256 bytes RAM. The chip has sleep mode capability,

The development team spent much time examining the reliability of Smart Card chips before selecting Hitachi. In the Swindon trial the cryptography will be symmetric, but it is anticipated that Hitachi will be invited to build a custom chip which will have asymmetric capability such as RSA and DSA..

The card uses a secure value transfer protocol with an underlying digital signature scheme independent of cryptographic algorithms so it will work with any algorithm and security is upgradable. NatWest says they will use whatever security it deems appropriate for each stage.

A personal four-digit code known only to the cardholder can be used as a protection device to lock the card. Once locked, the value in the card cannot be spent without re-keying this secret code, so the card has no value if lost or stolen.

The maximum value that can be held on the purses will be decided by the currency managers. This may vary between the currencies but will be applied for all purses globally. It has been suggested that the maximum value is likely to be not more than £10,000 (or equivalent) in order to meet regulatory requirements.

Payments can be made off-line so there is no need for the cardholder to sign anything or enter a PIN number, or for on-line authorisation. The customer's card is inserted into the terminal and the value is instantly moved from the card to the terminal. And for moving money, for example, between friends on the telephone, you just do it like making a payment in a shop. However, to access his or her account at the bank on the telephone the cardholder will be asked to identify

himself with a PIN.

The card is a multi-currency product, capable of holding up to five separate currencies simultaneously.

Cards will be available from the NatWest and Midland banks. Cardholders will be able to use a Mondex telephone or a NatWest or Midland adapted ATM to withdraw electronic money onto the card to pay for goods or services at participating Mondex merchants.

The merchants could pay their staff using Mondex, pay for stock from the cash and carry, and bank with the card using a telephone.

Electronic wallets

Pocket-sized electronic wallets will show cash available as well as providing a record of the last 10 transactions on the card. It can also be used, for transferring money from one card to another, for example, to pay the milkman or the window cleaner, or for transferring cash into the wallet for safer-keeping at home. These innovative units, designed to be low-cost devices, are being made by Panasonic (Matsushita Electric Industrial/Matsushita Battery) and Oki Electric Industry Co.

Key ring readers

Low-cost Key rings with a reader to display the balance on the card are being made by Panasonic (Matsushita Electric Industrial/Matsushita Battery) and Texas Instruments. They will be available to all cardholders.

Mondex telephones

Mondex telephones will be supplied by British Telecommunications (BT) who will be adapting some 1,000 public payphones with Mondex card readers in Swindon for the trial. In addition they will be providing, via an undisclosed supplier, residential telephones with Smart Card readers for home use.

ATMs

NatWest and Midland Automatic Teller Machines (ATMs) at which cardholders can top up the value on their cards will be supplied by NCR.

Point of Sale terminals

Point of Sale terminals will come from a range of suppliers. Retailers will not have to account to the bank for each individual transaction; their terminal will simply accumulate the total value of Mondex transactions which can be banked electronically by telephone at any time.

Benefits

Consumer benefits are 24-hour electronic cash via Mondex phones which may be available at home, in shops or at work, and a convenient alternative to cash that is inherently safer to carry.

Retailers and other cash handling businesses will benefit from an efficient, faster, and more secure way of handling money that is economic to operate.

Tim Jones, Senior Executive, IT Strategy and Policy, NatWest, said: "Swindon is really about allowing consumers and merchants full access to the product to see what they make of it and see from that what the pricing should be and how we should roll it out.

"It may be, for example, that the card and the key ring together form the basic package. We could then offer further packages at rental rates that might include some of the other things like wallets

or phones, or offer the phones and wallets as optional purchase extras.

Philips Order for Sweden

An order to supply 2,100 PE112 Smart Card readers to Sweden has been awarded to TRT Philips Smart Cards & Systems, France.

Selected by AU Systems, the integrator of the Swedish Police "Allterminal" project, to supply their DX RSA Smart Card, Philips has now been given the order for the next part of the tender involving the readers.

The PE112 reader is already successful in banking applications and has a track record with over 20,000 units operational in the field.

From the existing range of PE112, a new PC-integrated version is due to be released in the course of 1994, allowing the Swedish Police to meet all their requirements.

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

Chase Offers Enhanced Security

The Chase Manhatten Bank has enhanced security on transactions for corporate cash management customers using IBM Personal Security Smart Card technology.

The bank announced this month that it is offering IBM Personal Security cards to generate message authentication codes to verify transaction integrity.

Over the last few years Chase has offered the Chase InfoCash MicroStation enabling customers to use their personal computers to dial-in to the bank on-line. They can monitor balances and transaction activity in their bank accounts, initiate funds transfers and obtain various other services. DES, the Data Encryption Standard cryptography verifies the authenticity of the sender and individual transactions.

Now increased security is available to customers using the IBM Personal Security IC card which provides secure storage of data (up to 6,000 bytes), DES cryptographic processing and key storage, as well as a flexible access control system that can assign different access rights for up to four card users. Only the designated customer can the use the card and the application to perform on-line transactions with the bank.

Contacts: Gene U Rao, The Chase Manhatten Bank - Tel: +1 718 242 2543; Bob Page, IBM - Tel: +1 704 894 1729.

Japan Orders 1.8m Cards

Gemplus Card International is supplying 1.8 million Smart Cards to NTT Data, the largest Japanese systems integrator, to be used as customer loyalty cards for one of the biggest petroleum companies in Japan.

The MYDO Card is aimed at ensuring the loyalty of motorists to the company's chain of 9,000 service stations. The card totals petrol bonus points which customers may exchange for various gifts.

The microprocessor card meets NTT Data S-type specifications (0.5K bytes EEPROM, Feal algorithm and T=14 protocol). It also offers an Electronic Purse option which will in the future make it possible to rent a car or pay for a room or other services.

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, at their Orleans plant.

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 this year, Solaic will have shipped 66 million cards, of which 52 million have

embedded microprocessors. In 1993, France Telecom purchased 100 million phone cards from its suppliers, which include Solaic.

Bull CP8 Markets Crypto Card

Claimed to be the fastest asymmetric cryptographic ISO card in the industry, the Crypto Card is now being marketed by Bull CP8 who developed it with Siemens as part of the European Commission's Esprit project.

The Crypto Card has the new SLE44C200 chip developed by Siemens (see review in SCN April 1993) for Smart Card applications using security algorithms for authentication, encryption and digital signature of electronic transactions. These functions can be implemented independently of one another within the applications.

The card uses three types of algorithms - DES, RSA and Zero Knowledge (Guillou/Quisquater). Bull CP8 says that the RSA algorithm can be performed on 512 bits keys in less than 0.3s in the card without using the "Chinese Reminders" theorem and therefore giving the highest level of security.

Bull CP8 developed the operating system which manages the user memory as a tree of directories. The root directory is called the Master File and is mandatory. Each directory supports a number of Elementary Files which can be of four different types (secret, access control, public or working files).

These files, which are optional, differ in their contents and the way they may be accessed. Directories and files can be added at any time during the active life of the card. They can also be invalidated to end their use.

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

Smart Card Payphones

The Publimatique range of Smart Card payphones from Monetel, France, include both a rugged design for outdoor phone booths and others in a plastic cabinet for protected sites inside buildings.

In the IPT 400/700 ranges, the payphone benefits from the ruggedness of coin operated payphones designed to combat vandalism. With the use of the Smart Card and simplified reader, the payphone can be powered by the phone line alone. The card reader complies with ISO standards and is capable of accepting debit or prepaid card, subscriber card, and IC bank cards.

Smart Card indoor payphones in the IPTi 400/500 range are identical in performance to those for outdoor sites, but the cabinet is made of plastic and can be placed on a table or wall-mounted.

Monetel, based in Valence, France, is a subsidiary of Ascom, Switzerland.

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

Hand-held Terminal from Thyron

Thyron has announced a hand-held terminal, called the Financer, which accepts Smart Cards and magnetic stripe cards. Targeted at the retail and mass consumer payments markets, it will be available in volume from the first quarter of 1994 at a cost of between £75 to £200 depending on the number of functions required.

The Financer provides low-cost, on-line EFT (Electronic Fund Transfer) based on the APACS40 on-line credit/debit card transaction authorisation and collection standards. Suitable for applications requiring access to on-line services or transfer of payments using plastic cards, Thyron says the device is ideal for personal and small business banking, home shopping, loyalty schemes and lottery etc.

The terminal offers secure memory via an integrated circuit which can be used to provide cryptographic functions such as DES. It incorporates a 34-key pad, a multi-line LCD display and a number of security-protected interfaces, including a full telephone capability and an internal V21/V22 modem. Infra-red and/or RS232 serial interfaces enable the terminal to communicate with peripheral devices such as workstations and point of sale terminals.

Contact: Rohit Patni, Marketing Director, Thyron, England -Tel: +44 (0)727 875800.

New Publications

The Advanced Card Report: Smart Card Primer, by Dr Kenneth R Ayer and Joseph F Schuler, published by The Schuler Consultancy, USA. Tel/Fax: +1 301 869 6920. Soft cover, 139 pages, price $175 in the US and $190 abroad.

Joseph Schuler is President of The Schuler Consultancy and past CEO of Gemplus Card International Corporation and founder and former General Manager of the Smart Card and Systems Division of DataCard Corporation. Kenneth Ayer has been involved in market research in electronics for more than 10 years.

The book is intended as a practical introduction to advanced card technology, how they are being used and how they might be employed in the future.

The technologies generally used with cards are reviewed with the aim of providing a basic understanding of what the technologies can do and how they are used, and covers magnetic, optical and integrated circuit card types. There is also a comparison of card technologies including cost, security, memory size, durability, reliability and programmed logic capability.

The authors discuss the issues that should be kept in mind when considering card applications with a section on the cost of IC card systems including card production, personalisation, distribution, terminals, software, monitoring and licensing.

A further chapter reviews the general uses that advanced cards serve such as payment systems (credit, debit and prepaid), automated teller machines, information storage (medical records and loyalty programs), access control (physical and logical), and multiple applications.

This is followed by an examination of various applications drawn mainly from Europe and Japan such as telecommunications, health care, financial services, education, government, transportation, utilities, retail, travel and entertainment.

In conclusion, the authors point out that there is no right or wrong technology; just right and wrong applications of technology. Each has it

benefits and limitations. Application requirements should define the card technology, not vice-versa.

An appendix lists some of more than 400 US IC Card patents, and another lists some of the major firms in the advanced card industry.

1994 Advanced Card and Identification Industry Sourcebook, published by Personal Identification News (PIN) - Tel: USA +1 301 881 3383. Price $125: free to paid subscribers to PIN.

The 192-page Sourcebook, combining two previous titles - the IC Chip (Smart) Card Industry Directory and the Biometric Industry Directory - contains detailed descriptions of over 340 leading technology suppliers, systems integrators and consultants and over 50 pages of market reseach and background information including forecasts of IC chip card production through the year 1996. Technologies covered include Smart Cards, biometrics, optical cards, electronic photo ID systems, radio frequency ID, and cryptography.

Pre-payment Card Potential

Pre-payment cards for transactions under £10 in value will create a massive market worth almost £60 billion a year, according to Nigel White, Payment Strategy Unit, Association for Payment Clearing Services (APACS)

He told delegates at the European Payments '93 Conference, in Edinburgh, Scotland, last month that if we made the assumption that the potential market for pre-payment cards are face-to-face transactions under £10 in value, then less than 20% of current debit or credit card purchases were for such low values. Thus the impact of the pre-payment card on the existing card market was likely to be relatively small.

However, transactions under £10 in value represented nearly 90% of all non-regular personal cash purchases, a massive 28 billion transactions per year worth almost £60 billion.

A pre-payment card which could capture just one tenth of these current cash transactions would account for over two times the current volumes of credit and debit card purchases combined.

Smart Card Diary

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

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

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 attracting over 700 delegates from more than 40 countries. 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: 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 proceeded 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 10 April 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 European 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.

Fall in Plastic Card Fraud

APACS, the Association for Payment Clearing Services in the UK, has announced that the cost of plastic card fraud for the first six months of 1993, fell by £15 million to £71 million, compared with £86 million in the same period last year.

Key elements in reversing the fraud trend included:

* co-operation between banks and building societies and retailers to increase card authorisation at the point of sale, particularly in high risk transactions

* safer delivery of cards to cardholders,

* the Card Watch publicity and education campaign.

Lorna Harris, Head of APACS's Fraud Prevention Unit, said the results were encouraging and added: "APACS is now looking to technology to provide a lasting industry-wide solution to the problem of plastic card fraud."

Speaking at the European Payments '93 Conference in Edinburgh, Scotland, last month, she said that the Plastic Fraud Prevention Forum was researching and trialing different Card Authentication Method (CAM) technologies and they were expecting some very clear answers in 1994 on the most appropriate direction for the industry. PFPF were also looking at Cardholder Verification Methods (CVMs).

In the long term (1996 onwards) there was the prospect of using biometric technology to certify the cardholder, possible methods including finger-scanning and dynamic signature verification.

Contact: Richard Tyson-Davies, Head of Public Affairs, APACS - Tel: +44 (0)71 711 6200.

Smart Card Tutorial - part 16

Cryptography and key management (continued)

The difference between symmetric and asymmetric cryptographic algorithms is most obvious when examining the various key management architectures of the two types of algorithms. This month we will build up a typical asymmetric structure in a similar fashion to that used previously for the symmetric case.

We have frequently intermixed the terms asymmetry and public key in order to maintain correspondence with the term used in the general literature. The concept of a matching public key (PK) and secret key (SK) will be used constantly in this discussion but clearly the actual use of the public key will be decided by the designer or a particular security system. Such keys may well be publicly available whilst in other situations their confidentiality may be maintained as an additional security feature. In the case of RSA this public key relates to the modulus since the public exponent is normally chosen as a global constant. This exponent is often chosen to take the value of 65,537 ($2^{16}+1$); Fermat's number F_4) or 3 (F_0; (2^1+1)

In both cases the numbers are chosen as particular primes which results in a small number of multiplication when calculating the exponent. The value of 3 is obvious whilst 65,537 in hex is 10001. Every 1 bit in the exponent adds an additional multiplication when calculating the exponential. Although the discussion that follows here assumes the RSA algorithm for calculating digital signatures the arguments presented are equally applicable to other signatures schemes such as the DSS (Digital Signature Standard).

Let us first look at the single authentication method presented last month but this time using the RSA algorithm as shown in fig.1. Here the terminal sends the ICC a random number R. We should note also that the point of using a random number is only meant to portray data that cannot be predicted by an attacker or more to the point represents data for which he is unable to precompute the response. In practice the terminal may present a number of data fields including perhaps the current time. The ICC enciphers the random number R using its secret key SK as the exponentiator (R^{sk}Mod N). The result of this computation Y is returned to the terminal which then uses the matching PK to check for correspondence with the supplied R (i.e check if R = Y^{pk}Mod N).

In this simple example we have assumed that all the ICC's contain a common secret key whilst all the terminals store the matching common global public key. Clearly the system is exposed if one can determine the secret key of any ICC. An attack on the terminal to expose the public key has no value although the ability to change the key allows an attack that we will discuss later.

We can improve the security segregation by having a unique key in each ICC. In this situation (fig. 2) it is necessary for the terminal to know the matching public key. In the scenario shown in the figure the ICC could of course just present its public key to the terminal for checking the signature. There is of course a snag and it relates to the authenticity of the public key presented by the ICC. If no checks are made on the genuineness of this public key then an attacker could make up his own secret key and public key pair and would be guaranteed to pass the test.

This leads us towards the basis of all cryptographic systems, the centre of trust. If two unknown parties wish to correspond then there needs to be a common point that they are both prepared to trust. The role of this trusted entity is to either supply cryptographic keys or to vouch for the authenticity of a key generated by the particular entity. This centre of trust is often referred to as a global key centre (GKC) because its primary role is concerned with the key management of the particular security system.

GraphicContainsDatafor

PostscriptPrintersOnly.

GraphicContainsDatafor

PostscriptPrintersOnly.

GraphicContainsDatafor PostscriptPrintersOnly.

In a public key system this GKC has its own secret key and public key pair. It uses the secret

GraphicContainsDatafor PostscriptPrintersOnly.

key to produce a signature for the public keys of the participating entities. This signature is often referred to as a key certificate. We have used PK^{*G} as a representation of a key certificate on PK produced by the entity G. It is now only necessary to distribute the public key of the global key centre (PK_G) to all the terminals. In fig.3 we show how this can operate. The ICC now sends to the terminal its public key PK_i and the certificate (produced by the GKC) for this key PK^{*G}_i. In checking the response to the random number challenge the terminal carries out two operations. In the first instance it checks the authenticity of the public key presented by the ICC using the public key of the GKC (checks $PK_i=E_{PKG}[PK^{*G}_i]$).

Having checked the authenticity of the ICC's public key the terminal can then check the response to the random number challenge using the public key of the ICC. It should be noted that the ICC needs to store both its own public key and secret key and additionally the key certificate supplied by the GKC.

We can now examine the primary key management operation for the security scheme. In fig.4 the GKC generates a unique key for each ICC which is derived from the reference number

GraphicContainsDatafor PostscriptPrintersOnly.

of the chip and the system master key. This reference number (shown as ID) and the unique key are loaded into the EEPROM of the chip. In general it is also necessary for bilateral authentication to take place between the ICC and the GKC which we will discuss in more detail in a later part of the tutorial.

The asymmetric key management system is somewhat different and clearly there are many different ways of initiating such a scheme. In fig.5 we show an attractive approach where the ICC generates its own public key and matching secret

key. The role of the GKC now relates to producing a key certificate to be stored in the ICC and presented to a corresponding entity as required. In this situation it is not necessary to reveal the secret key of the ICC to any party. The key is generated, stored and destroyed all within the particular ICC. There is however a price to pay for this security advantage. Apart from the relevant software code necessary to generate the public key/secret key pair there is an enormous performance overload at the GKC in the time required to generate the keys. Even with microcontrollers incorporating a numeric co-processors we need to allow about 30 seconds or so just for this initialisation operation. On a production line this parameter also limits the throughput to 120 cards per hour on a serial feed. Clearly this is a significant problem and one that needs a conceptual rethink of the ICC personalisation and initialisation process compared with the personalisation of existing magnetic stripe cards.

David Everett

Next month The electronic purse.

Smart Cards Speed Skiers

Smart Card contactless ski passes are speeding skiers through access control points to ski lifts at two Austrian winter resorts.

Skiers using the CassaNova Smart Card system from ELIS of Austria, have the advantage that they do not have to insert the ticket into a slot reader while carrying skis, poles and wearing gloves. The Smart ticket, which can be carried in a ski suit sleeve pocket, is read by a proximity card reader. The tickets can be programmed for limited access or for a specific time period.

Currently some 20,000 cards have been issued in the ski resorts of Bad Kleinkirchheim and Schneebarenland (Planneralm-Loser/Altaussee/Riesneralm). The tickets are issued at points of sale where data such as type of ticket, validity period, and number of points is written onto the ticket. For visual inspection a photo is mounted onto certain types of tickets. Customers pay a refundable deposit.

Skiers at the entry to a ski lift, simply present the ticket to the access control terminal which contains a card sensor. The necessary data is read by the terminal, and if the ticket is valid this is indicted with a green light and the turnstile controlling access is released.

Access control terminals and points of sale in certain areas are connected via a network to a local host computer. Data is transferred periodically from the host computers to a central computer on disks. Thus the income from the different points of sale to the different providers of the various services is controlled.

The contactless card used is the MDS-W001 CO7 with 128 bytes of EEPROM user memory and a typical operating range of 10 cms.

ELIS, based in Vienna, Austria, is a wholly-owned subsidiary of Tactel, a subsidiary of Tadiran, Israel's largest electronic concern, and the CassaNova ticketing system was installed by Fa. Systems Computer & Software HmbH.

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

Chip Security for UNIX LANs

Orga Card Systems UK has announced X-Secure, a UNIX Security Card (USC) which allows users to protect their personal workstations from unauthorised access.

Standard UNIX log-on procedures are replaced by a Personal Identification Number (PIN) check and authentication of the chip card by the system.

Paul Hill, Marketing Director of Orga UK, said: "The Smart card is an ideal authentication medium for UNIX systems. It provides the user with a mobile key that can only be used by one person. Even if other people know the PIN, only the current owner can use the card."

In addition, the same card can be used for other functions such as company ID card, for payment in the canteen, an ID card for the telephone, and as a key to Electronic Data Processing (EDP).

An Application Program Interface (API) which is based on the X-Secure server is provided to implement particular chip card applications. An application is connected to the server by means of the API and this makes the data on a chip card accessible to the applications. This means X-Secure server and X-Secure client act as a gateway for access to chipcards in Local Area Networks (LANs).

Contact: Paul Hill, Marketing Director, Orga UK - Tel:+44 (0)491 410997. Fax:+44 (0)491 410295.

---

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

M&S Smart Discount Card

High Street retailer Marks & Spencer has introduced a Smart Card as its new discount card for staff to replace books of vouchers.

The chip card, from McCorquodale Card Technology, was successfully trialed in stores in Kingston and Kensington and has been issued to 60,000 staff and qualifying retired staff. Some 300 M&S sites are involved in the scheme.

The card is pre-loaded with the staff member's discount allocation. As purchases are made, the discount credit is automatically deducted from the card. The cards are rechargeable and will be reloaded with discount units every six months.

Independent consultant Lillian Moshe developed the system in conjunction with the information technology group at M&S starting in April of this year and the first trials started in the two stores in the same month. The success of the trials led to a decision to roll out the project in July and this has now been completed.

PIN pad style terminals with Smart Card readers were supplied by Dione Developments, of High Wycombe, and the data management service was provided by EWA, of Chelmsford.

M&S say that the benefits are seen as a service to staff as customers and the elimination of the administration of paper vouchers.

Card details:

Type		Contact
Fabricator		McCorquodale
Dimensions		ISO ID1
Contact location	Front	
Chip manufacturer		SGS-Thomson
Chip type		Memory
Memory type		EEPROM
Memory capacity		256 bytes

Contact: Robin Bennet, Project Manager, Marks & Spencer, England - Tel: +44 (0)71 268 5133.