Patient Smart Card Trials in Portugal and UK

A major trial of Patient Data Cards (PDCs) is to be conducted in Lisbon, Portugal, where consideration is being given to issuing all the residents in the Portuguese capital (population 2,128,000) with Smart Cards. In a complimentary specialist trial in Devonshire in south west England, patients issued with cards will include those with learning difficulties and others receiving psychiatric treatment.

The joint project, named Panacea, comes under the European Commission's Eureka research and development healthcare initiative and funding is estimated at between 2.7m and 3m Ecu (an Ecu is US$ 1.15).

Continued on page 83.

Smart Card News

Editor: Jack Smith

Technical Advisor: Dr David B Everett

Editorial Consultants:

Dr Donald W Davies, CBE FRS
Independent Security Consultant

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

Chris Jarman
Orga Kartensysteme

Published monthly by:

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

ISSN: 0967-196X

Next Month

Smart Card Tutorial Part 22 - Multi-application Smart Cards - Continued

CONTENTS

Patient Card Trials

Continued from page 80.

The project follows the successful National Health Service Care Card trial in Exmouth and Exeter in south-west England where patients were given electronic copies of their medical records.

The new project, which is part-funded by over £500,000 from Britain's Department of Trade and Industry (DTI), will develop a universal software

interface enabling the widespread use of PDCs throughout Europe via the adoption of open systems technologies.

It will be managed by the Institute of General Practice within the Postgraduate Medical School at the University of Exeter, under Dr. Robin Hopkins, Project Leader. He said that initially they would use a Bull CP8 Smart Card and then a card from another supplier. As the trials progressed they would test cards from a number of different suppliers.

Key partners in the initiative within the UK include: Bull UK (provider of the original Care Card); Exeter and District Community Health Service NHS Trust; Abies Medical Information Systems, a supplier of clinical systems to the NHS and a major contributor in the original Care Card trial; and Devon Family Health Services Association.

F7, a systems development and integration house specialising in communications and multimedia and based in Lisbon, will provide local project management for the implementation in Portugal.

Key issues

The DTI says: "Panacea is designed to address two of the key issues which have prevented the extensive use of portable electronic medical records to date, namely the incompatibility of proprietary systems and the reluctance of healthcare organisations to abandon existing IT investment or recognise the potential patient benefits.

"Panacea will focus on an open interface, which will be proposed to the European Community for adoption as a standard."

New software tool

The development of a new software tool, known as EuroCare, will allow the PDC to be read and updated at each healthcare location where the patient receives care. This allows authorised healthcare professionals to access the relevant parts of an individual's medical record, reducing the time needed to contact other healthcare providers for missing information.

EuroCare follows on from extensive research work carried out by Bull at its Systems Integration and Services centre in Hemel Hempstead and work within the field of standardisation.

Brian Endersby, Manager of Bull's Healthcare Operations, says: "Although there have been some previous attempts to implement PDC technology involving the medical record, they have tended to be on a very small scale. The DTI funding will give this project the credentials and backing which will ensure that it succeeds."

Pilot scheme

In the pilot scheme, cards will be issued to patients with learning disabilities and to those being treated by the Exeter and District Community Health Service NHS Trust's psychiatric services, in addition to patients registered with General Practice using the Abies Clinical Information System.

Portable computer systems will allow the healthcare professional to access and update the cards wherever the location.

Contact: Dr. Robin Hopkins, Project Leader - Tel:+44 (0)392 403020. Fax:+44 (0)395 269769.

Melbourne AFC Project

An Automatic Fare Collection (AFC) system using Smart Cards is planned for trains, buses and trams in the Melbourne region of Australia.

The first phase of the project is expected to start late this year and include two railway lines, five bus routes involving some 150 buses, and one tram depot with 80 vehicles. Contactless Smart Cards, with a magnetic stripe, will be issued to schoolchildren, disabled people and travellers who normally buy yearly passes. Roll-out of the system is expected to start in 1995.

Currently, printed paper tickets are used on the

US West Telecard Trial

US West Communications has started a trial with its Telecard which can be used in over 120 Smart payphones.

Northern Telecom, Inc., has supplied the payphones, and the cards are the GPM 103 chip card from Gemplus.

various services. The new system will involve ticket vending machines, validators, associated computer systems and management infrastructure.

Onelink, a consortium including ERG Australia, Fujitsu and Maynes Nickless, are expected to be awarded the contract from the Melbourne Public Transport Corporation to develop, implement, operate and manage the system. ERG will provide hardware and overall project management; Fujitsu, the central computer system and associated software; and Maynes Nickless, cash collection and security services.

Gemplus Canadian Subsidiary

Gemplus Canada, a new Gemplus Group subsidiary, was inaugurated in Montreal last month by Marc Lassus, Chief Executive Officer.

The Group aims to take advantage of the potential in Canada, especially in Quebec, for developments in the fields of banking, healthcare, transport, telecommunications and interactive television, and the new company is already engaged in negotiations with several partners in Quebec to develop Smart Card technology and to set up strategic partnerships.

Canada is the 12th country with a Gemplus subsidiary, following the U.S., Argentina, Mexico, Singapore, Japan, China, Great Britain, Germany, Italy, Spain and France.

Contact: Jean Sureaud, Gemplus Canada - Tel: +1 514 876 4200.

SIM Personalisation Centre

AU-System, the Swedish consultancy specialising in data and telecommunications and Smart Card system integration, is developing a new SIM (Subscriber Identification Module) Personalisation Centre for the Swedish GSM operator Telia Mobitel to personalise SIM-cards with subscriber data and services available.

The system supports SIMs and personalisation stations from different suppliers, and uses modern client/server technology based on Windows NT, SQLServer and Visual C++ development tools. It will be sold and marketed by AU-System to other GSM operators and will be available in standalone and LAN-based versions.

Contact: Anders Hardebring, Smart Cards Business Development, AU-System, Sweden -Tel: +46 8 726 7546. Fax: +46 8 19 3322.

School Meals Card

Three schools in Devonshire, south-west England are using Smart Cards in a cashless school meals system.

The Power Card shown on the front page was designed by Devon Direct Services, the catering arm of Devon County Council and is being used in Torquay Grammar School, Ivybridge Community College, and Usscolme Community School.

Copenhagen Card

The introduction of the Danmont pre-paid card system in Copenhagen has been marked with a new Danmont card design (see front page) illustrating the town hall. The background design shows coins becoming cards, which is the theme of the advertisement campaign Danmont are running in Copenhagen.

The design has also been printed on more than 100,000 postcards which are distributed from almost every cafe in the city.

COST Appointment

Hans Christian Anderson, systems developer at Danmont, has been appointed "technical secretary" for the COST Action 225 which works on research and development of security in telecommunications. Participants come from 16 different universities, organisations and leading companies in Europe.

COST stands for European Co-operation in the field of Scientific Technical Research.

Mr Anderson can be contacted at Danmont, in Denmark - Tel: +45 43 44 99 99.

Sharp Electronics (UK) have developed their 3110 series electronic cash register to use Smart Cards in the system developed in conjunction with McCorquodale Card Technology. The cards used are MCT 416 bit re-usable 1^2C bus EEPROM chip cards with PIN code protection.

Benefits

Benefits of the system are seen as:

* Less cash handling
* Speed of operation (no change problems)
* Security
* Parents reassured that money given for school meals are not being misused on other goods.
* Students entitled to subsidised/free meals are not discriminated against as they use cards identical to those carried by other pupils, but electronically programmed with subsidy data.
* The system provides valuable reports and statistics.

The reports can show the number of free school meals supplied, value of meals provided, additions (credit) to cards, deductions (debits) from cards, meal portion analysis to assist stock control, value of staff duty meals, daily and weekly income analysis.

Contact: Bill Waller, Marketing Director, McCorquodale Card Technology - Tel: +44 (0)273 475453. Fax: +44 (0)273 480715.

Shell Smart Cards?

Oil giant Shell is said to be planning to launch a new Smart-Card based promotional programme, according to industry sources.

In a bid to attract motorists and increase its market share in the highly competitive petrol retail business, it is believed to be investing in the region of £20 million in a loyalty programme which it hopes will attract drivers to its forecourts.

It has been known for some time that Shell has been investigating various card technologies, including Smart Cards. It is believed that among major companies who submitted proposals were French Smart Card manufacturer, Gemplus, and Scottish-based Smart Card point-of sale terminal manufacturer De La Rue Fortronic.

If Shell proceeds with the scheme it will give a massive boost to the Smart Card industry in the UK by putting cards in the hands of thousands of motorists throughout the country and give them the opportunity to familiarise themselves with the technology.

A spokesperson for Shell refused either to confirm or deny the project.

CardTech/SecureTech '94

The United States is generally regarded as lagging behind Europe in Smart Card technology and its applications, so delegates at the CardTech/SecureTech '94 Conference and Exhibition last month may have been surprised at the increasing activity in this field.

US Projects to Watch

Delaware Card Project

The Delaware Department of Transportation has been selected by the US Department of Transportation to field test Smart Cards in their fleet of 128 buses on all routes.

Called the Smart DART (Delaware Authority for Regional Transportation) project, the aims are to:

* introduce Smart Cards as fare instruments
* enable local companies to offer their employees the card as a one payment/identification mechanism for a variety of functions such as an ID, physical access control, and paying for cafeteria meals.

Companies have the option of choosing between debit or credit cards.

Henry Dreifus, of Dreifus Associates, said it was estimated that there were over 200 Smart Card projects across the United States at various stages of development ranging from training and pilot test projects to significant planned implementations.

Among those to watch was the US West Corporation public telephone market trial, based on the European technology of prepayment cards, he said. US West intended to apply this technology initially in specific markets to reduce the cost of

current pay phone operations as well as to raise revenue. They were also in partnership with Time Warner in an interactive two-way home services programme which might use a Smart Card in the near future.

Money Access Service (MAC) would launch next year initially in the north east, but then grow to its over 30 million cardholder base with an electronic purse "cash card" for making small value purchases.

Chemical Bank in co-operation with AT&T would offer a cash card based on the AT&T Smart Card to consumers in the New York City area following an internal trial.

The Western Governors Association would issue a tender for a health passport to allow benefit recipients access to numerous healthcare services in five western states along with social welfare benefits, including WIC (Women, Infant, and Children) benefits, food stamps and immunization programmes.

Cellular telephone operators would introduce Smart Card-based digital cellular telephones using the cards to provide secure authentication of the telephone and potentially open the way forward to global roaming.
Healthcare organisations and hospitals were launching numerous patient identification and services cards which would facilitate the admissions processing and improve the speed and quality of care. The programmes were independent of the National Healthcare Card proposal of the Clinton Administration.

The US Defense Department would issue cards for a number of applications ranging from soldier payment to health treatment records (being tested in Among examples of applications was the U.S. Air Force Academy Cadet Falcon Card being developed as a campus style card to integrate a number of existing processes and automated systems.

Each cadet starting with the June 1994 class would be issued with a Falcon Card with a photo, integrated circuit, bank stripe, security stripe and linear bar code. The multi-technology card would provide the cadet with an automated method for dormitory security, laboratory and library access, clothing issue, and other base services. This would dramatically improve the efficiency and accuracy of the Academy's data collection and information management systems.

Hawaii) for medical processing.

Numerous security applications involving network and PC (as well as portables) software, applications and communications would emerge with the advance of low-cost co-processor crypto-engines. Companies, like IBM, Sun Microsystems, Datakey, Microsoft and Cylink were already designing programs with high security Smart Cards.

Automatic fare collection, toll roads and other transportation applications would continue to be implemented. These applications favoured non-contact technology, such as AT&T's toll collection project in the State of California.

These, said Mr Dreifus, were just a few of the numerous projects that were leading the way into mass commercial entry in the United States.

Card Projects in the Military

The US Department of Defense Microcircuit Technology in Logistics Applications (MITLA) programme had sent a clear message to industry that microcircuit-based Automated Identification Technology (AIT) services were part of its modernisation initiatives, said Mark Reboulet, Programme Manager.

Instead of developing unique military standards, the DOD continued to participate and embrace national, international and industry standards, and the MITLA programme would continue to pursue microcircuit-based AIT applications to automate source data collection in various functional areas.

Falcon Card

Following a site survey by Systems Resources Corporation in December 1993, a contract was issued to implement the Falcon Card and plans were underway to export the methodology to West Point.

Mobility Processing System

An Automated Mobility Processing System (AMPS) was developed under contract to the Air Force by Applied Systems Institute. It used the Micro Card Technology ICC and the Epson memory card to streamline the mobilisation of personnel and cargo.

The ICC, initially loaded and updated from a central personnel database, was used to report arrival time at the unit, verify eligibility for deployment, provide accountability for aircraft boarding, and provide automated records in the deployed location.

The AMPS had undergone three proof-of-concept phases with the final phase being completed in June 1993. It was operational at Wright-Paterson Air Force Base, Ohio, and at F-117 wing at Hollerman Air Force Base, New Mexico.

The system was turned over to Air Force Logistics Management Agency for inclusion and adoption as an Air Force wide system. Testing was currently underway at Seymore Johnson Air Force Base, South Carolina, to test AMPS interfaces to several Air Force systems.

Soldier Readiness Card

An Army Soldier Readiness Card (SRC) was designed to support personnel accountability, readiness, movement control and essential battlefield Personnel Service Support functions.

A proof-of-concept system developed by SYSCON Corporation included an ICC carried by the soldier, a Telxon handheld ICC and PCMCIA terminal, and a notebook computer. The Personnel Service Support functions supported included: medical treatment, combat pay and casualty evacuation.

The system was undergoing field testing with the 82th Airborne, at Fort Bragg, North Carolina.

Wyoming EBT Project

Wyoming was to carry out an Electronic Benefit (EBT) pilot project using a Smart Card for a combined Women, Infant and Children (WIC) benefits and Food Stamp demonstration, said Joseph Terry Williams, State of Wyoming.

"The understanding underlying this pilot," he said, "is that while the agencies National Food Stamp EBT System proposes to use on-line technology with magnetic stripe access cards, the Food and Nutrition Services will conduct a targeted EBT research programme using alternative technologies to ensure that other possible technologies are not foreclosed.

Follow-up testing was planned with the Multi-technology Automated Reader Card (MARC) programme.

Contact: Mark Reboulet, MITLA Programme Office - Tel: +1 513 257 4118.

MARC Project

Multi-Technology Automated Reader Card (MARC) programme was initiated by the Department of Defense to explore the feasibility of such a card and to begin to move towards a "one card per soldier" concept, said Michael Noll, Office of the Assistant Secretary of Defense.

The background was that functional requirements for Smart Card technology within the DoD were numerous and demonstration projects of individual Smart Card applications were multiplying throughout the Department. It was clear that when the cost of multiple applications was shared by a single infrastructure, cost-effectiveness could be substantially multiplied.

The prototype test concept included requirements for a joint Military services environment, the addressing of both peacetime and wartime functions and the risks associated with the use of Smart Card technology under battlefield conditions; involve both soldiers and their families; and be large enough to demonstrate the feasibility of Department-wide implementation.

Plans were being finalised for the test of US Pacific Command activities on the island of Oahu, Hawaii.

"The Wyoming demonstration will serve as the Agency's test of Smart Card technology in a rural environment where food stamp and WIC benefit delivery is integrated into the same system."

The contract had been awarded to National Processing Company with Anderson Consulting as the subcontractor. National Cash Register would supply the retail equipment and services.

The pilot would include 2,100 Food Stamp households and 1,700 WIC participants in Natrona County. An estimated 46% of the WIC participants were also eligible for Food Stamps so the one card would be used by those households to manage benefits from both programmes. They would shop

at the 45 authorised retailers in Natrona County. A further 3,500 WIC participants in the six counties of south east Wyoming would also use the card in shopping at 30 additional WIC retailers.

The pilot would run for 38 months, he said. Acceptance testing was scheduled for October this year and then it was planned to proceed with implementation by equipping the retailers and issuing cards to the participants with full implementation by early summer 1995. The operational phase was scheduled for 22 months.

Set Back for Smart EBT

Payease, the largest Electronic Benefit Transfer (EBT) pilot application using Smart Cards in the United States and involving some 13,000 low income families in Dayton, Ohio, (SCN April) 1993) has come to an end. Although successful and widely expected to be extended throughout the state, the Dayton pilot is being converted to on-line mag stripe due to cost considerations.

The news came from Lee Jones, Financial Management Service, US Treasury, who said: "A wide spread Smart Card infrastructure is practically non-existent in the U.S. From a practical and political standpoint, it is not the government's role to establish a new banking/financial infrastructure by placing Smart Card access terminals nationwide nor can it be cost justified. As Smart Card technology becomes the universal financial infrastructure, however, you can be sure that EBT

BT's research had shown that the two most attractive applications were finance and telephony. BT had implemented a calling card application with Visa and had recently announced its participation in the Mondex electronic cash project together with Britain's National Westminster and Midland Banks.

The effect of these three initiatives, GSM, Phone Card and Mondex, in the UK would be to produce a Smart Card infrastructure which could be used for many other applications, she said.

The attraction of the multi-application Smart Card to the telephony operator lay in being able to offer customers a means of identification and validation which was user friendly, portable, a tangible representation of the operator's service, and provided a platform for delivering a range of products.

will follow."

Future Trends in Telecoms

Smart Cards would have a major role to play in the complex future world of telecommunications making it significantly easier for the user to interface to the network and allow the development of large numbers of value added services, said Pat Chapman-Pincher, of BT, the British Telecommunications company.

In Europe, she said, the application of Smart Cards to telephony had two key drivers - the new generation of digital mobile phone networks and the pay phone card. The last few years had seen phone cards moving towards simple chip cards in several European countries. These cards were now becoming more complex and beginning to support multi-function applications.

Initially these would tend to be telephony, as for example, the Deutsche Telekom combined GSM and Payphone card, but increasingly they would be multi-application and multi-country.

There was activity in developing a pan-European phonecard which would allow customers to roam across Europe using a card bought in their own home markets, and there were trials of multi-application cards taking place throughout the world which combined telephony with other applications.

It was possible to envisage certain service sets, for example, an entertainment card that allowed access to a certain set of videos (dependent on the holder's subscription), gave access to local cinema clubs and information lines, and contained both electronic purse and credit facilities.

A traveller's card might support a mobile phone, access to travel information and booking services, local parking access and the means to pay for such services.

"As user's journey across the networks of the future," said Ms Chapman-Pincher, "it is the Smart Card which may provide the key to the service set that they have chosen and eventually become a passport to a virtual world."

MasterCard Appointments

MasterCard International Inc. has announced the appointment of two Senior Vice Presidents in the field of Smart Card technology.

Robin Townend, R&D Manager at Barclays Bank in the UK, has been appointed Senior Vice President Chip Card technology effective 1 July, and Diane Wetherington, former President of AT&T Smart Cards, has been appointed Senior Vice President, Chip card Business/Marketing, effective 6 June. Both will be based at MasterCard's New York City headquarters and report to Executive Vice President Philip P Verdi.

These new positions have been created, says MasterCard, "to evaluate the potential for, and deliver recommendations on, the use of chip technology in the payment services industry."

MasterCard President and CED, H Eugene Lockhart, "We have gathered substantial research on the capabilities of the chip for pre-paid applications as well as for fraud prevention. An important part of that process is confirming how chip technology will enhance the profitability of our global membership. Diane and Robin will lead our efforts in this important area, so that whatever path we take toward chip technology will be the path that best serves our members."

MasterCard has nearly 22,000 member financial institutions worldwide and, in 1993, 210.3 million MasterCard credit cards generated more than $322.6 billion in transaction volume at 12 million acceptance locations.

The two new Senior Vice Presidents have a high profile in the industry and international recognition for their many years of experience in plastic cards and Smart Card technology.

A career banker with Barclays bank in the UK, Mr. Townend specialised in plastic cards for the last 20 years and is responsible for R&D focusing on the business applications of emerging card and related technologies. He has been instrumental in the implementation of various card programmes including the Dallington Country Club multi-functional Smart Card and pioneering Barclays work on biometric identification.

He is Chairman of the association for Payment Clearing Services (APACS) IC Card Working Group in the UK and the UK's representative on European Committee for Banking Standards and the International Organisation for Standardisation (ISO) Working group developing international banking standards for Smart Cards.

Ms. Wetherington was with AT&T for 11 years and for the past three years was President, Smart Card Systems and Solutions and responsible for establishing AT&T's Smart card business. She had responsibility for R&D, sales, product management and manufacturing. Under her leadership, AT&T was successful, for example, in establishing applications in automatic road tolling, and an alliance with Chamical Bank to conduct Smart Card banking stored-value cards in New York City.

Medical Emergency Card

A citywide healthcare Smart Card system is being introduced in Oklahoma City involving equipping ambulances, fire department vehicles and hospital emergency departments with card readers so that medical personnel can immediately access vital patient data and make treatment decisions with knowledge of the patient's pre-existing medical history such as heart disease, diabetes, or drug allergies.

Paramedics can take the patient's Smart card and insert it into a Palmtop PC equipped with a card reader and access medical history necessary to make critical decisions. Similar action can be taken when a patient seeks care at the emergency department of a hospital.

If the patient is unconscious or disoriented, medical personnel can obtain information from the card

informing them who to notify in the patient's family and who to call to obtain more medical information.

This is the first such Smart card system in the United States and is attracting interest from many parts of the world.

Called +MediCard, the system has been developed by Advantage Data Systems (ADS) who are installing hand-held Smart Card readers in emergency response vehicles and PC-based readers in hospital emergency departments under agreements with Midwest City Regional Hospital Ambulance Service, Nichols Hills Fire Department, Oklahoma City Fire Department and Oklahoma City area hospitals. It will serve both emergency and general admission functions. Initially, 12 local pharmacies will act as +MediCard service centres. Physician offices, clinics and other healthcare facilities are also involved in the network.

When placed in a reader, +MediCard allows medical personnel to instantly access the patient's medical history: medication records, drug allergies, the names and telephone numbers of physicians, family or friends, and other information necessary for making treatment decisions, completing admission forms, and generating insurance bills.

Dr. Kent Webb, founder of ADS and a general and vascular surgeon in Oklahoma City, says:"In some emergency situations patients are often unable to receive the best quality of care when providers have to make split-second treatment decisions without any knowledge of an individual's pre-existing medical conditions. With +MediCard, medical personnel now have immediate access to a reliable and accurate Patients, who are +MediCard members, do not have to fill out long, complicated forms or have to remember detailed medical information when entering the healthcare system and they can be confident that they are providing the medical professional with an accurate picture of their personal medical condition.

Insurance forms are also easier to complete using the information stored in the card, thus eliminating possible mistakes.

Healthcare providers

Participating healthcare providers benefit by a decrease in time and effort required to obtain information from patients and reduce administration costs on processing patient forms.

Coupling the +MediCard Network with medical billing software allows for real time billing of services rendered and eliminates costly paper methods.

Pharmacies can review current medication listings and provide patient counselling on drug interactions or redundant medication prescriptions.

medical history, even if the patient is unable to provide it."

Membership of the scheme costs a one-time payment of $30 plus an annual fee of $12.

Benefits

Patients

Members who are injured in fires or accidents, or who suddenly become ill, can be treated by paramedics in rescue units who have been able to obtain information about their pre-existing medical condition from the Smart Card. In addition, even if they are unconscious, the hospital can identify who they are and notify a member of their family or a friend in case of emergency.

automated billing methods and the +MediCard system supplements this by downloading data without the information being entered manually. Also, as patients carry their medical information, many redundant prescriptions and medical tests are avoided thus saving needless expenditure.

Contact: Baron Blakley, Executive Director of Marketing, Advantage Data Systems - Tel: +1 405 752 5550. Fax: +1 405 752 5605.

The insurance company

The insurance industry is rapidly moving towards

US Health Card Lobby

The Smart Card Industry Association (SCIA) is lobbying decision makers on Capital Hill as well as consumers across the country to push for the incorporation of Smart Card technology in the Clinton Healthcare proposals.

President Clinton has made healthcare reform a major issue of his administration and proposes that each citizen should be issued with a Health Security Card carrying electronically readable information

The SCIA has launched what it describes as its "most aggressive" public relations campaign to heighten Smart Card awareness in both the consumer and government areas. They are using Neptune Associates in the promotional campaign and The Hoffman Firm to get their message across to government and media and industry analysts.

Conference topic

The Health Security Card was also a topic at last month's CardTech/SecureTech '94 Conference. Daniel Maloney, Director, Washington Information Systems Center, Department of Veterans Affairs, said that two major documents released by the administration described the card.

"The Health Security Act" proposed legislation HR

3600 (1342 pages), proposed that the card contain information encoded in electronic form, including the identity of the individual, the health plan, any policy in which the individual is enroled and other necessary information," he said.

"These statements are found in Health Security Act HR 3600, section 5105, page 853. The Health Security Act does not mention a specific card technology such as magnetic stripe or Smart Cards. This is very appropriate since the legislation is intended to be in effect for a long time. Specifying technology in such a law could result in a requirement to use a technology in the future when a newer solution would be better."

The second document, "Health Security, The President's Report to the American People," was not legislation but meant to communicate in plain language the intent of the proposed reforms.

Not a Smart Card

In chapter 5 on page 48, it stated: "The Health Security Card will not be a Smart Card - which carries information in a computer chip - a national identification card, or a credit card.

"It does not hold sensitive information such as medical records. It's simply a way to streamline the billing process, reduce paperwork for doctors and patients, and assure people that they have a comprehensive set of benefits that can never be taken away."

Also on page 48, the statement was made: "Like the cards that activate bank teller machines, a magnetic strip will provide basic registration information, including identifying the health plan in which you are enroled. A personal identification number will authorise access to insurance information, reducing the process of registering and billing, but maintaining your privacy."

Under the proposed Health care Reform, he said, the main function of the card was to identify the patient. Exploration of new, higher technology cards could be encouraged to better serve patients and to streamline administration.

As these technologies were successfully tested, the minimum national standard for the card could be modified, said Mr Maloney.

European experience

The European Community had obtained a large base of experience with Smart Cards and card related applications.

"We should all strive to learn as much as possible from this experience so that we can make the most appropriate use of this technological tool to solve our healthcare problems," he said.

In order to arrive at a final consensus on the characteristics of the Health Security Card, additional consultations would be held with multiple groups including government officials, healthcare providers, and standards groups, including the National Institute of Standards and Technology.

New Publications

Datamonitor is to publish a new report on the Smart Card industry in Europe with forecasts to the year 2000.

Advance news from the publishers of key findings include the European Smart Card market is currently forecast to grow in volume terms at over 20% per year to 2000, whilst the value of the market in 2000 is predicted to be 25% greater than in 1994.

On electronic purses, the report says they could generate large profits for the banks issuing these cards, but may also threaten the traditional role of banks.

It points out that funds withdrawn from the cardholder's account to charge up the card do not have to be paid out by the bank until a retailer registers the transaction. In the meantime, banks can lend out those funds to borrowers, so generating a profit.

Some electronic purses allow the transfer of funds between cards, without recording the transaction. Such anonymous transactions, says the report, may lead to a reduction in the role of the banks if the electronic purse not only replaces cash, but also decreases the use or credit and debit cards and cheques.

It says that in March 1994, Visa International established an electronic purse standards group, involving purse operators from around the world, but points out that it excluded Mondex, the joint venture of NatWest and Midland Banks with aspirations for a global electronic purse.

"Opportunities in European Smart Cards" is available from Datamonitor, 106 Baker Street, London, W1M 1LA, England. Tel: +44 (0)71 625 8548. Fax: +44 (0)71 625 5080. Price £695.

New studies

Retail Banking Research has announced that it is producing six new studies providing independent comprehensive and authoritative information and analysis in the world of payment cards and branch automation.

These are: "Future of Prepayment Cards: Markets, Technologies and Opportunities," with a comprehensive independent analysis of the markets, technologies and opportunities in this new aspect of banking.

"Payment Cards in Europe: International Survey and Analysis," providing detailed statistics and analyses of the card payment business in every western European country, and considers the state of development of each type of card, the issuers, and the processors.

"Future of Payment Cards: Strategic Analysis and Forecasts," which develops an earlier study and provides forecasts for each of the individual major card markets in Europe.

"Future of Self Service in Banking: Forecasts to the year 2000." Based on face-to-face and telephone interviews with leading banks in five countries, this report forecasts trends in self-service set against the changing regulatory and competitive environments in each country.

"ATMs and Cash Dispensers 1993: International Survey and Analysis." An annual report on ATMs and cash dispensers it is a reference source for major manufacturers of ATMs in Europe and the USA as well as for banks and card companies.

"Information and Transaction Terminals 1993." A report on self-service from statement printers to deposit terminals to multi-function machines.

Contact: Retail Banking Research, London - Tel: +44 (0)71 495 8871. Fax: +44 (0)71 493 0539.

Smart Card Diary

Bankcards with Chips, Palais Ferstel, Vienna, Austria, 16/17 May.

Speakers from eight different countries will discuss chip card payment systems, including the electronic purse, and their use in public transport, road pricing and the retail industry etc. Contact: a la Card Conference Services, Germany - Tel: +49 40 66 86 09 17. Fax: +49 40 270 80 66.

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

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

Cards & Technology '94, Hamburg, Germany, 16/17 June.

An a la Card symposium. Contact: Hans H Huber, a la Card Conference Services, Germany -Tel: +49 66 86 09 16. Fax: +49 40 270 80 66.

Developments, Applications and Implementation Strategies in Smart Card Technology, Sheraton Walker Hill Hotel, Seoul, Korea, 16/17 June.

US Conference Card

An official U.S. CardTech/SecurTech Conference Smart Card (shown on the front page) contained an electronic purse with $5 of value which could be used at vending machines at the Prepaid Card Showcase.

It also contained encoded information showing that the delegate was entitled to collect one copy of the 1,100 page conference proceedings. The conference and exhibition was held in Crystal City, Virginia, last month.

A chance to hear about the Smart Card market in Korea as well as technology issues and applications. Contact: Elsa Dana, Centre for Management Technology, Singapore - Tel: +65 345 7322. Fax: +65 345 5928.

Plastic Card Fraud & Security, The Cumberland Hotel, London, England, 16/17 June.

International speakers include representatives from Europay International, Banksys, APACS, Visa UK, and New Scotland Yard. Contact: AIC Conferences - Tel: +44 (0)71 329 4445.

ESCAT 1994 (European Smart Card Applications & Technology), Hotel Inter-Continental, Helsinki, Finland, 7-9 September.

Smart Card applications and user experiences from international speakers from ten countries. Contact: Congrex - Tel: +358-0-752 3611.

Vehicle Leasing Study

A feasibility study to investigate how modern technology can be used to improve the monitoring, authorisation and payment of fleet repairs and maintenance has been launched jointly by the British Vehicle Rental and Leasing Association (BVRLA) and AT&T ISTEL.

Five senior leasing members of the Association, which represents more than 1,300 companies in the vehicle leasing, fleet management and short-term rental industry, and AT&T ISTEL have agreed joint funding of the study.

Robert Mercer, of the BVRLA Leasing Committee and Project Co-ordinator, said: "This project is intended to identify the technologies which can be developed into an efficient and cost-effective system.

"With the administration of repairs and maintenance accounting for a significant proportion of a leasing company's overhead, modern communications technology should provide opportunities to reduce waste, improve efficiency and ultimately cut costs to customers."

The initial study is expected to last three months and will start by reviewing how each leasing company operates, identifying what changes to procedures maybe required and determining how flexible any eventual system needs to be.

Technical considerations will include the types of point-of-sale device required, transaction authorisation techniques, data input, output, storage and communications requirements and the definition of interfaces with existing systems. Smart Card technology will be amongst those examined in the study.

Contact: Robert Mercer, Project Co-ordinator, BVRLA - Tel: +44 (0)21 733 5752.

Name Change for NCR

NCR (Manufacturing), the Dundee, Scotland, based subsidiary of AT&T, has taken on the Group corporate identity and is now known as AT&T Global Information Solutions (Scotland).

Smart Card Tutorial - Part 21

Multi Application Smart Cards

Wherever you go the talk is all about multi application or multi function Smart cards. First of all we should have a go at defining the difference between multi function and multi application. Here I'm going to use the old fashioned computer terminology. Multi function referred to a tool that could implement different operations for a single client. Multi application referred to a tool that could implement different operations for different clients. If we stick to this terminology the commercial and security issues are readily apparent. The multi function card has a defined single owner who can set the commercial rules for use of the card and define the necessary branding issues. Most of the more complex applications to date have been along these lines in that the functions have all been defined by one provider or there has been a substantial cooperation to share the management of the Smart Card.

It is the multi application card that is really the more interesting. Here we have a Smart Card that is no more than an application carrier for the various application providers. These providers ideally should be totally unrelated. This raises a number of interesting questions,

a) Who owns the card ?
b) How is branding defined ?
c) What are the rules of application provision and operation ?
d) What happens when the card expires ?

These are just the surface of the commercial problem. One should not expect to see the general purpose multi application card take over the world just yet. We could carry on discussing these issues for some time but lets examine the technical issues more carefully. These issues can be summarised as follows,

1) How is the security segregation between applications enforced ?
2) How do applications authenticate the carrier ?
3) How does the carrier authenticate the application?
4) How are the co-residence rules enforced ?
5) How do you know what application exists on the card ?
6) How do you invoke the required application ?

The world of ICC Standards has really only addressed the last two of these questions with ISO 7816-4 (Inter Industry Commands for Interchange) and ISO 7816 - 5 (Numbering Systems and Registration Procedure for Application Identifiers).

These standards provide the following tools,

- An application identity registration scheme
- A directory file
- A file select command

We have mentioned previously the ability for application providers to register their applications. KTAS (Denmark) are providing the necessary administrative services although potential applicants should note that request for an application Identifier should be placed through their National Standards organisation.

The Application Identifier is made up of two parts,

- RID (Registered application provider identity)
- PIX (Proprietary application identifier extension)

It is of course the allocation of RIDs that will be undertaken by KTAS. Of greatest interest are applications intended for International use where the RID is defined to be of the form,

Axxxxxxxxx (all elements hexadecimal - 4 bits each)
(total 5 bytes or 10 hex digits)

The registered application provider may choose to add the optional PIX of up to 11 bytes (22 hex digits max)

The total application identifier (AID) is defined as follows,

AID

RID (5 bytes)	PIX ($\leq$11 bytes)

This size of AID allows for significant scope in defining International Applications.

David Everett

Next month - Multi application Smart Cards continued.

RSA - 129 Factorisation for $100

In 1977 Scientific America published a challenge posed by the public key mathematicians for factoring a number of 129 digits. Some 17 years later using 600 volunteers operating over the Internet with some 1600 computers in 20 countries over 8 months the challenge has been met. The reward for breaking the puzzle was $100 (which will be donated to FSF). Amongst the 1600 computers were several massively parallel processors (including an MP2 rated at 60,000 MIPs). The final set of data using 2 Giga bytes of memory was solved on a MasPar MPI belonging to Bellcore in New Jersey (USA). The formal announcement on the Internet by the coordinators Arjen Lenstra (Bellcore), Derek Atkins (MIT), Michael Graff (Iowa State University) and Paul Leyland (Oxford University Computing services) is reproduced here in an annex.

The question here is what does this do to RSA and in particular the favourite key size of 512 bits (155 digits). Before we attempt to answer this question we should remember that a designer can set the security of the algorithm to any arbitrary strength by choosing the size of the modulus. However the longer the modulus the longer the decipherment operation. For all practical purposes the encipherment operation with its small exponent (e.g 3) can be ignored. In the same way that advancement in technology allow such attacks they also enable the designer of security systems to use longer keys. So the real crux of the argument centres on who wins the technology race, the designer or the attacker. One must also ask the question as to whether the form of attack described here can be realistically applied to a commercial security system.

The general work function for factorisation can be defined as follows,

$$W(N) = \exp (K . (\text{Ln } N)^{\alpha}. (\text{Ln Ln } N)^{\beta})$$

Where N is the number to be factorised. Different factorisation algorithms result in different values for K, α and β. Until a few years ago the best work function for factorisation was believed to be based on values for α and β of 1/2 with K approximately equal to 1. The multi polynomial quadratic sieve method (MPQS) as used in this latest attack was based on these figures. The number field sieve (NFS) developed by Pollard, Lenstra and Manassewas a major discovery in that α = 1/3 and β = 2/3. The designers were able to attack special numbers of the form

$N = r^{e} \pm s$ (Cunningham numbers with Small r and s)

In 1990 they factorised the ninth Fermat number ($2^{512} + 1$) of 155 digits. For this form of numbers the value of K in the equation above was found to be 1.526. It has not been found possible (yet) to achieve the same value for general numbers and at the current time K has been optimised at 1.902 (Coppersmith). In the table below we show the comparison of work functions for different sizes of moduli. It seems likely that the quadratic sieve has reached the limit with RSA - 129 and accordingly we would expect any new attempts to be based on the use of the number field sieve method.

One of the coordinators of the RSA - 129 challenge has proposed that a number of 1024 bits would be about 20,000 times as hard (memory and CPU cycles) to factor compared with the current breakthrough, only time will tell.

Factorisation Work Functions

N	2^{429}	2^{512}	2^{576}	2^{768}	2^{1024}
(Number of Digits)	129	155	174	232	309
Quadratic Sieve (QS) $\exp (1.0.(\text{Ln } N)^{1/2}. (\text{Ln LN } N)^{1/2})$	7.10^{17}	$6.7.10^{19}$	$1.7.10^{21}$	$1.3.10^{25}$	$4.4.10^{29}$
Number Field Sieve (NFS) $\exp (1.9. (\text{Ln } N)^{1/3}. (\text{Ln Ln } N)^{2/3})$	$3.5.10^{17}$	$1.0.10^{19}$	$1.1.10^{20}$	$5.7.10^{22}$	$6.4.10^{25}$

For comparison we should review the DES algorithm with its key size of 56 bits. Assuming that breaking the algorithm depends on key exhaustion then on average the work function is proportional to $3.6.10^{16}$. We can of course considerably increase this work function by using the triple DES mechanism (encipher with K_1; Decipher with K_2; encipher with K_1).

To put all this in perspective for our Smart Card arena we need to point out another little complexity faced by the attacker. Public key systems are so called because you can publish the public key being used by the various entities. For an International directory service that is of course necessary. However if for example we were using RSA for an electronic purse scheme, then there would be no need to ever publish any public key being used by the scheme. This seems to make the whole problem somewhat more difficult.

Annex - RSA-129 Announcement on the Internet

We are happy to announce that
RSA-129 = 114381625757888867669235779976146612010218296721242362562561842 9\
3570693524573389783059712356395870505898907514759929002687954354 1
= 349052951084765094914784961990389813341776463849338784399082057 7 *
3276913299326670954996198819083446141317764296799294253979828853 3

The encoded message published was
9686961375462206147714092225435588290575999112457431987469512093081 62\
9822514570835693147662288398962801339199055182994515781515 4

This number came from an RSA encryption of the `secret' message using the public exponent 9007. When decrypted with the `secret' exponent

1066986143685780244428687713289201547807099066339378628012262244966 31\
0631259117744708733401685974623065539685445132771090536060 95

this becomes
2008050013010709030023151804190001180500191721050113091908001519190 90\
618010705

Using the decoding scheme 01=A, 02=B, ..., 26=Z, and 00 a space between words, the decoded message reads

THE MAGIC WORDS ARE SQUEAMISH OSSIFRAGE

To find the factorization of RSA-129, we used the double large prime variation of the multiple polynomial quadratic sieve factoring method. The sieving step took approximately 5000 mips years, and was carried out in 8 months by about 600 volunteers from more than 20 countries, on all continents except Antarctica. Combining the partial relations produced a sparse matrix of 569466 rows and 524338 columns. This matrix was reduced to a dense matrix of 188614 rows and 188160 columns using structured Gaussian elimination. Ordinary Gaussian elimination on this matrix, consisting of 35489610240 bits (4.13 gigabyte), took 45 hours on a 16K MasPar MP-1 massively parallel computer. The first three dependencies all turned out to be `unlucky' and produced the trivial factor RSA-129. The fourth dependency produced the above factorization.

Neuron Chip Smart Card

Motorola and Smart Card manufacturer US^3 have announced the first Smart Card containing a Neuron IC.

The card can be used in a variety of networking applications, including Smart building applications deploying LonWorks network technology.

"This Smart Card brings a new level of features and capabilities to the Smart Card market," said Al

Moulton, Director of Marketing, LonWorks Products Operation for Motorola.

"Over 700 companies are currently using LonWorks technology to develop intelligent networks for distributed control, sensor and monitoring functions.

"With the addition of a Smart Card based on a Neuron IC," he added, "companies will gain the ability to easily program their application into a Smart Card. They can also modify or change the application, when necessary, in lieu of replacing the card."

More EEPROM

The Neuron IC comes from the factory with a 48-bit serial number making each card unique. In addition, the Neuron IC contains in ROM the LonTalk protocol which has an application function library and authentication routine for secure communications.

Having the protocol in ROM gives the customer more EEPROM for specific application code and data.

Functionality is also enhanced by using three on-chip processors to divide the workload in a network environment. While one of the processors supports the customer specific application, the other two processors handle the network protocol.

The Smart Card contact interact to the Neuron IC mechanically complies to ISO standard, making existing reader and interface hardware capable of supporting the Neuron IC with the minimum of modification.

Eight contacts used

Eight contacts are used: two for power, two for communications, and one each for clock, reset, I/O, and service. The Neuron IC communicates with the reader using differential signals, allowing it to "talk" to one or more other Neuron ICs in the reader.

Rapid integration

Tom Templeton, General Manager of US^3 says: "The very concept of the neuron IC, being a very powerful, field programmable, application neutral processor makes it very synergistic with Smart Cards. We expect the integration of these technologies in the market place to be very rapid."

LonWorks intelligent distributed network, developed by Echelon Corporation and licensed to Motorola, continues to gain market acceptance for intelligent building and home control applications.
It offers both a powerful and flexible network capability over different media and at different data rates.

Some typical network configurations are; 4800 BPS to 1.2M BPS on twisted pair; 9600 BPS on power line, 1200 BPS to 9600 BPS on RF, and 1200 BPS to 9600 BPS on telephone lines.

Motorola's LonWorks Products Operation is a business unit within the MOS Digital-Analogue IC Division, in Austin, Texas.

US^3, located in Santa Clara, California, is the largest Smart Card manufacturer in the United States and a major supplier of Smart cards in Scandinavia and in the UK.

Among other contracts, US^3 supplies the Smart viewing card used by British Sky Broadcasting (BSkyB) which early this year reported that paying subscribers has reached over 3.25 million.

The company offers a wide range of Smart card products, hardware, engineering and manufacturing services, and is represented in Europe by Cristel UK Ltd. Litton House, Buckingham Street, Aylesbury, HP20 2LL. England

Contact: Terry Warmbier, Cristel UK - Tel:44 (0) 296 393134

Card Europe Launch

Card Europe, the Association for Smart Cards across Europe, has announced that it held its inaugural meeting in London last month when 15 early members, including Marks & Spencer, TSB Bank, and London Transport, met to set the initial strategy and to create its UK chapter. Officers of the UK chapter were elected and its meeting schedule set for the rest of the year.

In a statement, Card Europe said that members felt that there was a major requirement for a Europe wide, user led Smart Card association. System operators, scheme implementors and system integrators advocated the need for a strong voice for Smart Card users in order to successfully lobby for the type of product that they wished to sell, at a price they felt was saleable.

It was hoped that as a talking shop for its members drawn from many different industry sectors, that unique incompatible systems would no longer be produced by the major players and that interoperable systems with multi-service capability would become the norm.

There was a fear that without an association like Card Europe, many incompatible singe function Smart Card systems would appear on the market, each with its own card and each requiring its own unique reader terminal.

The Association hopes that membership will grow rapidly throughout Europe so that it will have a positive influence on decision makers.

Contact: Alan Liebert - Tel: +44 (0) 923 897477. Fax: +44 (0)923 897414.

Newspaper Vending Machine

Residents in the French towns of Poissy and Issy-les-Moulineaux, have been able to purchase the French newspaper Le Parisien from vending machines using pre-paid memory cards.

Innovatron and Seprotec, who have both been involved in the development of the card and the technology involved, have adapted an automatic vending machine manufactured by the Swiss company Journomat.

In the first trials, they distributed 20,000 throwaway Solaic 256 EPROM cards, and installed 38 vending machines in Poissy, and 40 in Issy-les-Moulineaux.

The pre-paid cards, which cost 45F, enable the cardholder to purchase 10 editions of the newspaper. The purchase is made by inserting the card into the machine to pay for the newspaper which is released when the card is withdrawn.

Available 24 hours a day, the vending machines provide a quick and easy service, and figures show that 70% of sales of newspapers take place between 5am and 8am before many of the kiosks and newsagents are open.

With only one point of sale for every 2,600 people in the Paris area, and one for every 1,600 in the provinces, Le Parisien decided to introduce the vending machines to provide an effective way of increasing their sales outlets.

Contact: Genevieve Boeuf, Communication, Innovatron, France - Tel: +33 1 40 13 39 40.

Danmont at Rail Stations

Passengers travelling on Danish State Railways (DSB) in the metropolitan area of Copenhagen now have the opportunity to make small purchases using the Danmont pre-paid card instead of coins.

DSB restauranter og kiosker has installed 26 Danmont terminals from Siemens Nixdorf at kiosks and fast food outlets at 14 stations. Kurt Mikkelsen, Director of Purchasing, says: "We have a remarkable large number of small amount payments every day, and consequently it is natural for us to provide this new service for our customers so that they can take part in the very exciting development within payment systems."

Contacts: Henning Jensen, Managing Director, Danmont - Tel: +45 43 44 99 99. Kurt Mikkelsen, Director, Purchasing, DSB restauranter og kiosker - Tel: +45 86 13 14 11.