SMART CARD NEWS

JULY 1997

Volume 6 Number 7

Holland Leads with Multi-Function Cards

Netherlands PTT Telecom, the largest telecommunications provider in the Netherlands, and Postbank, a subsidiary of the ING Group - one of the three leading banks in the Netherlands - both launched new Smart Cards last month which are likely to spearhead a major breakthrough in the use of multi-function chip cards.

The new cards - Smartscope from PTT Telecom and Giropas from Postbank - are based on the Chipper technology and includes electronic purse, phonecard and other multi-functional features.

PTT has already issued about 100,000 cards and has a target of one million by the end of the year, while the Postbank will have distributed five million Giropasses by the end of the year.

Continued on page 123

July 1997

News

Smart Card Tutorial

Cards on the Cover
CK Tang Combined Store and Credit Card
Page 140
Coventry and Leicester Courts Catering Card
Page 131
Glastonbury Phone Card
Page 130
PTT Telecom's Smartscope
Front Page

How to Subscribe
If you wish to subscribe to Smart Card News please complete the form on page 139

Don't Forget!
Our On-Line Website, containing a Library of Smart Cards and information about the full range of SCN services, can be found at the following address:
http://www.smartcard.co.uk

The International Smart Card Industry Guide 1997
If you would like your company to be featured in the next edition of the Guide please send us your details via fax, e-mail or by using the on-line form at our website.

Important Announcement
Due to office reorganisation the ***SCN*** *telephone numbers have been updated. You can now contact us on a new number:*
+44 (0) 1273 236677*, as well as* ***+44 (0) 1273 626677****.*

Smart Card News is published monthly by Smart Card News Ltd PO BOX 1383 Rottingdean Brighton East Sussex BN2 8WX England
Telephone: + 44 (0) 1273 236677 / 626677 Facsimile: + 44 (0) 1273 624433 / 300991 e-mail: scn@pavilion.co.uk ISSN 0967 196X
Managing Director *Patsy Everett* ***Editor*** *Jack Smith* ***Technical Advisor*** *Dr David B Everett*
Journalist *Anna Ronay BA (Hons)* ***Graphic Designer*** *David Lavelle BA (Hons)*
Editorial Consultants *Dr Donald W Davies CBE FRS, Independent Security Consultant*
Peter Hawkes, Principal Executive Electronics & Information Technology Division, British Technology Group Ltd
Simon Reed, Head of Strategic Marketing for the Orga Group
Printed by Design and Print (Sussex) Ltd. Telephone: +44 (0) 1273 430430.

G&D Acquires Cardtech Inc

Giesecke & Devrient GmbH of Munich, Germany, has bought the US company Cardtech Inc., based near Cleveland, Ohio, which produces 50 million high-security cards a year for over 2,000 customers operating chiefly in the payment systems sector.

Jürgen Nehls, Head of the Cards and Card Systems Division and member of the Board of Directors at G&D, said: "Through Cardtech, the Giesecke & Devrient group gains the access and production capacity it needs to assume a leading role in the strategically important US card market."

As a first step, G&D plans to transfer its Smart Card know-how from Munich to the USA. The installed production line will have an initial annual capacity of 7.5 million cards in three-shifts operation.

***Contact: Ulrike Gaissert**, G&D - **Tel: +49 89 4119-1864**.*

Swindon Test Bed for Mondex

Mondex UK, the electronic cash card company has announced that it will continue its Swindon, UK, Smart Card trial to "test a range of new concepts that have emerged since its launch." It will also be making an announcement before the end of the year about the future of Mondex nationally.

Ron Clark, Chief Executive of Mondex UK, says: "Since launch we have learned a great deal from the Swindon trial about the potential of Smart Cards, which has meant that scope for developing the Mondex technology has gone far beyond our original objective of creating an electronic alternative to cash."

He added there are a host of other developments which are at concept stage and which Mondex would like to explore further in Swindon.

Mondex is being introduced in more than 26 countries across five continents around the world and currently over 450 suppliers and manufacturers are developing applications for Mondex, said Clark.

***Contact: Dan Brockbank**, Mondex UK - **Tel: +44 (0)171 667 6820**.*

Japan's Students Get Smart

A large-scale electronic cash scheme is due to be piloted in Yokohama City University in Japan in November.

The scheme will then be rolled out to Hitotsubashi University and Hosei University in the Tokyo area and Chiba University which lies in the Chiba prefecture.

Eventually the system will be used at 59 campuses, targeting a population of 430,000 students.

The card will be carried by students, teachers and staff who are members of the Co-operative Society. Data stored on the cards will include personal membership information and financial data such as the card's balance. If the card is lost the value held is guaranteed and will be returned to the holder.

Banks will issue cards

To use the electronic cash option a student must open a bank account at one of the participating banks. These include Bank of Tokyo-Mitsubishi, Dai-Ichi Kangyo Bank, three other city banks and regional banks. The banks are responsible for issuing the cards to students.

The card can then be used in participating outlets to purchase a range of goods and services. Aims of the scheme are to cut queuing time for the cardholder and to reduce management costs for those running the Co-operative Society.

Future plans include the possibility of adding further functions such as access control, library membership and the issue of certification documents.

The system and cards have been developed by NTT Data Corporation. Point of sale terminals have been developed by PFU, also a Japanese company.

At present there are no plans to expand the scheme beyond the University environment.

Contact: Masahuru Nagamiya**, Assistant Manager, NTT Data Corporation, UK - **Tel: +44 (0)171 374 0040. Fax: +44 (0)171 374 2275. E-mail: nagamiyam@noanet.nttdata.co.jp

Racom Contracts in Holland

Racom Systems Inc., has been awarded contracts by LOGIN BV of Enschede, Holland, to provide contactless Smart Card systems for three new multi-application programs in The Netherlands.

Initially, Colorado, USA-based Racom will deliver more than 5,000 contactless Smart Cards and associated terminals and communication software for two municipal recreation facilities located in the cities of Schagen and Vlaardingen, a suburb of Rotterdam.

Racom is also supplying cards for a community waste management system shared by the cities of Deurne, Kampen and Zwolle.

Designed in co-operation with LOGIN, the Schagen and Vlaardingen contactless Smart Card systems are used to store electronic money, user identification, and facility management data.

Local children, families and senior citizens in both communities are using the cards to pay for access to swimming pools, lockers and recreation amenities such as tanning salons, saunas and vending machines.

As a result, cash, tokens and keys have been eliminated from circulation, reducing risks and costs associated with cash-based equipment, including theft and fraud.

Facility managers estimate use of the Smart Card's electronic purse alone will annually save tens of thousands of guilders in labour costs per facility, while providing members with more convenient access to recreation facilities and services.

Government sponsorship

The Schagen project, with over 1,000 members, is sponsored by the Dutch government to evaluate the use of Smart Cards for rationalizing recreation management, increasing membership and lowering overheads. There are over 150 similar Dutch municipal facilities, with up to 3,000 members.

The Vlaardingen project is operated by a group of privately owned recreation facilities numbering over 300 throughout Holland.

Smart waste management

The third project is one of Holland's first multi-application waste management contactless Smart Card systems for use in Deurne, Kampen and Zwolle.

Developed in co-operation with one of Europe's largest waste container manufacturers, the system enables residents to deposit household waste into underground bins located near densely populated residential complexes. The cards are used in combination with battery-powered locking systems to open bin doors, track bin use on a user basis and prohibit illegal dumping.

Unlike conventional contact cards, which do not work well in open environments, and RFID cards, which offer read-only functionality, Racom's contactless Smart Cards are completely sealed and programmable. As a result, new community services, such as on-time waste pickup, community access control and recycling programs, can be programmed into the card after issuance.

The system is designed to support over 20,000 residences using up to 200 bins, and targeted for use in over 100 cities.

Contacts: Oliver Gatchell**, Racom Systems - **Tel: +1 303 771 2077. Fax: +1 303 771 4708. Web: http://www.racom.com**. LOGIN - **Web: http://www.login.nl

PC/SC Smart Card Reader

Schlumberger Electronic Transactions is offering its PC/SC-compatible Smart Card reader technology in chip form, backed by development services, to help OEMs speed card-enabled products to market.

It is envisaged that the new product will hasten the arrival of secure Personal Computers, network computers, palmtops, TV set top boxes, modems, keyboards, terminals and other devices which are emerging to support electronic commerce and other networked applications.

Contact: Isabelle Ferdane-Couderc - Tel: +33 (0)1 47 46 70 20. Fax: +33 (0)1 47 46 68 66. E-mail: ferdane@montrouge.ts.slb.com

Japan Moves Towards Chip Cards

Japan is taking the first steps in a longer-term plan to migrate payment cards from magnetic stripe to chip technology. Six hundred Visa cardholders in Tokyo are now receiving the new credit cards with an integrated circuit chip and several restaurants have been equipped with chip card terminals.

The Tokyo launch is the initial phase of a larger pilot being launched in October involving 30,000 chip cards and several shopping malls in Kobe, Japan.

The Kobe pilot will include three types of chip-based Visa cards - CCPS (Visa's Chip Card Payment Service standard) credit cards, CCPS credit cards with the added function of reloadable Visa Cash, and standalone reloadable Visa Cash cards.

A separate phase of this project will launch Visa's first Japanese virtual-shopping site using the Secure Electronic Transaction (SET) protocol

The pilot, called Smart Commerce Japan, is being implemented by Visa, Toshiba and several technology manufacturers. Smart Commerce Japan is supported by the Electronic Commerce Promotion Council of Japan's Ministry of International Trade and Industry.

***Contact: Jeff Perlman**, Visa International Asia-Pacific - **Tel: +65 437 5513. Fax: +65 437 5567**.*

New Smart Card Work Groups

Two new work groups have been set up by the US Smart Card Forum to address interoperability and multi-application.

Jean McKenna, Forum President and Senior Vice President at Visa International, said: "Our new accent on interoperability is being driven by Forum members because it is relevant and vital for their needs."

David Boyles, Senior Vice President of Smart Cards and Interactive Services at American Express and a Forum Board Member, commented: "This is not a competitive issue but a shared imperative. Infrastructure will not define who wins the game; the toughtest competitors will be the best product and service providers and we all have to work together for this industry to move forward."

The Interoperability Work Group will focus on the business and technical issues surrounding the need for standardised interfaces between cards, terminals and slots. The Multi-application Work Group will deal with issues arising when more than one service or product offering resides on a card, including branding, regulatory and legal issues, ownership of the data on the card and customer relationships, security and privacy.

Contact: Smart Card Forum - Tel: +1 813 286 2339. Fax: +1 813 281 8752.

Visa Sets All-time Record

Announcing an all-time record of US $1 trillion purchases by Visa Card customers in the 12 months ended 31 March, Visa International predicted that Smart Cards could account for as much as a third of its card base within five years.

The US $1 trillion record is 23.7 per cent higher than Visa's previous 12-month total of US $824 billion, and Visa's President and CEO, Edmund P Jensen, said this indicated that an increasing number of consumers worldwide were relying on bank cards as the best way to pay because of their convenience and the control they provide in managing personal financial affairs.

He said that debit cards, which draw on a deposit account rather than a credit line, are the fastest growing segment of Visa's business increasing 40 per cent to a record US $305 billion with cards totalling 119 million, up 36.7 per cent from the previous year.

"Within five years, Smart Cards could account for as much as a third of Visa's card base," he said, adding that it had issued more than 20 million Smart Cards globally.

"Smart Cards will literally put a bank in the consumer's pocket and open a whole new chapter in the history of money," he said.

***Contact: Jeff Perlman**, Visa International Asia-Pacific - **Tel: +65 437 5513. Fax: +65 437 5567**.*

Payment Brands Join Forces

The two largest payment banks, Visa and MasterCard, joined forces last month to accelerate the introduction of electronic commerce in Singapore.

An electronic version of a United Overseas Bank Visa card was used to buy French wine and a DBS Bank MasterCard was used to purchase a set of golf clubs from Internet shopping malls in Singapore.

The purchases followed a similar transaction two months earlier in Singapore involving a Citibank Visa card in the first end-to-end Internet purchase involving a Visa card and the SET standard. This first transaction was made possible after Citibank, utilising IBM technology, built its own "payment gateway" connecting the Internet with the banking system.

As a result, local Singaporean banks decided to share costs by having the Network for Electronic Transfers (Singapore) Pte (NETS) develop a similar infrastructure on their behalf, utilising Hewlett-Packard technology. The local banks are shareholders in NETS, which runs Singapore's domestic debit EFTPOS system.

The NETS electronic commerce payment gateway accepts both Visa and MasterCard transactions, which is consistent with the intentions of both payment associations to promote SET as a common, global standard.

The SET technology is to undergo further trials and testing will focus on interoperability to ensure that "virtual" credit cards issued by one particular bank and utilising one SET technology can be used to make purchases at Internet merchants contracted to other banks and using different technology.

Visa says that by August, it is anticipated that several thousand Visa cardholders from participating banks in Singapore will be able to make secure purchases from a wide range of local merchants.

By the end of the year, Visa plans to link the electronic commerce initiatives of its Singapore Member banks with similar Visa projects underway in Taiwan, Japan and Korea.

Visa SEC Pilot Growing

Visa is setting a cracking pace on secure Internet transactions with its European Secure Electronic Commerce (SEC) pilot.

The first transaction was carried out by the Bank of Ireland in late May and was followed last month with transactions over the Internet in Spain and Finland. The pan-European pilot will involve 38 Visa members representing over 80 banks across 16 European countries to test the SET specification.

Spain's first live Secure Electronic Transaction (SET) purchase over the Internet was completed last month by Sistema 4B, one of Spain's largest bank card processors, using VeriFone and Hewlett Packard Internet commerce technology. The transactions took place between different consumers and merchant banks using a Visa credit card as part of a SET pilot program. Involved were Banco Santander, a music retailer and a merchant bank; Banco Sabadell. Sistema 4B is to extend this pilot through relationships with its 38 member banks, 30 merchants and 2,000 cardholders. (Visa Espãna, representing 25 members, is to start SET transactions soon, whilst La Caixa has already started testing.)

A separate transaction was carried out in Finland last month by Luottokunta, a consortium of Finnish banks.

Visa expects that SET software will be ready for full commercial roll-out to banks, cardholders and merchants by the end of this year.

Contacts: Ian Gatherum**, Visa International - **Tel: +44 (0)171 937 8111. Fax: +44 (0)171 937 0877. Mark McMurtrie**, VeriFone - **Tel: +44 (0)1895 824031. E-mail: Mark_ml@verifone.com

SET Pilot in Germany by GZS

GZS (Gesellschaft fur Zahlungssysteme), the leading German card processor, is to pilot SET on the Internet starting in October. VeriFone will provide GZS with an end-to-end suite of SET products to offer Internet payment solutions. GZS is to resell VeriFone's payment software to merchants in Germany who wish to establish a retail presence on the Internet.

Open Trading Protocols

Further companies with plans for Internet commerce have joined an effort to establish Open Trading Protocols (OTP) as a global standard for all forms of trade on the Internet.

The companies are Actra, British Telecom, CyberCash, Dot Matrix, Hitachi, IBM, Nokia, Oracle, Sun Microsystems, Unisource and VeriFone.

They join the original group which pioneered the protocols, made up of AT&T, Hewlett-Packard, MasterCard International, Mondex International and Open Market Inc., as well as all of Mondex International's shareholding banks.

The OTP, due for publication this summer, will enable a consistent framework for multiple forms of Internet electronic commerce. The protocols will be freely available to developers and users.

Steve Mott, Senior Vice President Electronic Commerce at MasterCard, said: "We consider OTP to be a significant opportunity in the arena of electronic commerce.

"These proposed protocols have been designed as an open standard and offer a secure trading environment which co-operates with and potentially enhances other payment protocols including SET and EMV96 for debit and credit."

OPT will work with SET based credit and debit transactions being rolled out by a number of organisations.

They will provide a clearly understood SET of rules that cover: offers for sale, agreements to purchase, payment (by using existing payment protocols, such as SET), the transfer of goods and services, delivery, receipts for purchases, multiple methods of payment, support for problem resolution.

Organisations interested in further information are invited to e-mail otp-info@lists.commerce.net

Contact: Gerry Hopkinson**, Head of Corporate Affairs, Mondex International - **Tel: +44 (0)171 557 5016. Fax: +44 (0)171 557 5216. E-mail: Gerry.Hopkinson@mondex.com

Visa Chip Electronic Commerce

Visa last month released a new specification for the secure use of chip-based payment cards over the Internet.

Called the Chip Electronic Commerce specification it combines the EMV (Europay/MasterCard/Visa) chip card specifications with the SET (Secure Electronic Transaction) specification for secure payments over the Internet.

Details of the new specification are available by e-mail request to kkeathle@visa.com

Java Card Forum Expands

Bull CP8 Transac and De la Rue Card Systems (formerly Philips Smart Cards & Systems) have joined the Java Card Forum founded some four months ago by Schlumberger and Gemplus with the active support of Sun.

All four are now said to be actively engaged in marketing, developing and enhancing interoperable products compatible with the Java Card API standard.

The Forum is inviting strategic partners to join from the financial service, telecommunications and information technology fields and claims 15 have joined so far, with more expected in the coming weeks.

The Forum has formed a Business Committee to promote the standard and accelerate its deployment in key markets with the first Java card applications expected to be launched before the end of this year, and widely deployed in 1998.

Three markets have been singled out for early attention - banking, telecommunications and information technology. Pay television, health, transportation and entertainment industries are also seen as major adopters of the Java card technology.

Contacts: Michel Roux** (Gemplus) President of Business Committee - **Tel: +33 (0)4 42 36 56 54. Java Card Forum Web site: http:\\www.javacardforum.org

Loyalty Card Chips from Siemens

Siemens Semiconductors has announced that it is developing a new series of low cost Smart Card IC products designed specifically for use in loyalty schemes such as frequent flyer, petrol forecourt and retail schemes.

For entry-level applications, Siemens says it will develop a low cost, secure microcontroller, called the SLE22C02S with 6K of ROM, 256 bytes of EEPROM and 128 bytes of RAM with a die size of less than 4mm² for embedding in Smart Cards.

It is also extending downwards in both size and cost its range of secure memory ICs. Based on the SLE 4442 and 2K bits of secure memory, it is introducing the SLE 4441 and SLE 4440 with 1K bits and 512 bits of secure memory respectively. All of the new devices will use an identical interface for maximum flexibility.

"With the introduction of this new series, I believe we firmly dispel the perception that Smart Cards are too sophisticated for loyalty-based applications," said Graham Nott, Manager for Chip Card ICs in the UK. "We expect the market for card-based loyalty schemes to quickly get Smart!"

Contact: David Close**, Marketing Communications, Siemens plc - **Tel: +44 (0)1344 396313. Fax: +44 (0)1344 396721.

WH Smith Introduces ClubCard

WH Smith, the retailing group, is to introduce a loyalty card to 400 stores. At present the cards are magnetic stripe and there are no plans to migrate to Smart Card technology.

A spokesperson for the company said WH Smith felt it had achieved the functionality of a Smart Card system without the cost. Each time a card is swiped at the point of sale Head Office is automatically dialled to obtain the customer's details.

(With a Smart Card system operating off-line, however, the cost of the phone call is negated. The card, containing the customer's identity, becomes a portable database bought to the point of sale by its holder.)

The term 'Clubcard' is also used by Tesco who have some 9.5 million loyalty card members. WH Smith explained that research has shown the term is now considered generic and was considered suitable for the company.

WH Smith is to issue three million cards initially with more to follow according to demand.

Contact: Liz Harlowe,** WH Smith. **Tel: +44 (0)1793 562128.

Schlumberger Reorganises

Schlumberger has formed a new organisation, Test & Transactions, to focus on its high-end electronics and transactions businesses. The new group will consist of two divisions - Electronic Transactions and Automatic Test Equipment - and will be headed by Irwin Pfister, Executive Vice President and former President of the ATE division.

ATE, based in San Jose, California, designs and manufactures equipment for the testing of semiconductor devices as well as testing complete electronic assemblies for the telecommunications and automotive industries.

Carlos Lazalde has been promoted from Vice President and General Manager of Test Systems to President of ATE.

Electronic Transactions, located in Montrouge, France, offers Smart Card-based solutions and services, cards, terminals, development tools and support in open configurations for operators, developers, integrators and distributors around the world. They're providing both turnkey solutions and a full range of tools and services for telecommunications, banking, retail, mass transit and parking, healthcare and networks.

Claus Kampmann, previously President of Geco-Prakla in the Oilfield Services business, takes over as President of Electronic Transactions.

Contact: Isabelle Ferdane**, Electronic Transactions, France - **Tel: +33 (0)1 47 46 70 20. E-mail: ferdane@montrouge.ts.slb.com. Beverley Bird**, ATE - **Tel: +1 408 437 7264. E-mail: bbird@san-jose.ate.slb.com

Correy Shopping Catalogue

Right:
Two images from "The Correy Electronic Catalogue" [Correy]

Below Right:
The 1997 Glastonbury Festival in Somerset, England [Smart Card News]

Correy have released a new fully secure multi-media catalogue system for electronic shopping that is designed to exploit the positive elements of the Internet. It is called The Correy Electronic Catalogue and was developed in Israel in 1996.

A key feature of the catalogue's design is the integration of advanced Smart Card technology developed by Fortress U&T. Using Crypto-chip technology allows the vendor to safely authenticate a customer's orders and payments when placed via the Internet using their full RSA Electronic Signature Customer Card and reader.

The low cost Smart Card Keyboard Reader, specifically developed by Fortress U&T for this system, is manufactured by Elonex PLC and requires no 'hard installation' as it simply shares the PC keyboard port.

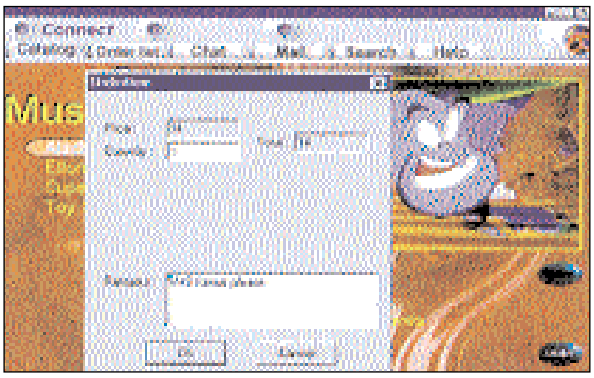
At the front end of the system full multi-media presentations that form the catalogue are put onto CD-ROM. The customer can then view the goods and standard prices using their PC. This reduces the need to go on-line and saves time waiting for images and media-data to download. The shopper only goes on-line to 'chat' directly with a shop assistant or check latest prices, availability, special offers and to order and pay for goods.

Initially it is expected that the catalogue will be used primarily by retailers to order goods from their suppliers. Eventually the system will be used by the end customer to order goods from the retailer.

Gaby Vago, Managing Director of ICTS, the system's integrators, believes that the catalogue's high levels of security and versatility mark the beginning of a new era in electronic shopping.

He said that due to the medium used, the catalogue works equally well for any type of merchandise or service. As the catalogue allows pictorial, video and audio demonstrations of products the customer could listen to extracts from a piece of music, examine static goods from different aspects, see moving goods in action or even sample the view from the window of possible holiday accommodation.

Vago told *SCN* that Correy was currently in discussion with at least 27 UK companies about the system which is currently in use in Israel.



Contact: Garry Malone,** ICTS. **Tel: +44 (0)171 637 7876. Fax: +44 (0)171 580 7875.

Glastonbury Phone Card

British Telecom issued 15,000 limited edition Smart phonecards to commemorate the 1997 Glastonbury Festival in Somerset, England.

Held almost every year since 1970, the festival welcomed over 90,000 people this July. Attractions included music, circus, comedy and many alternative technologies.

A BT spokesperson said that the phonecards "sold out really quickly" and are expected to be a popular design with collectors.

New Terminals for Tesco

Left:
Tesco's SNIkey touchscreen Point of Sale terminal [Siemens Nixdorf]

Siemens Nixdorf Information Systems Limited has won a £60 million, three-year contract to supply Tesco's next-generation point of sale technology.

Simens will provide Tesco with an upgradeable pentium-based systems infrastructure that will support the delivery of value-added customer services at the point of sale using advanced touchscreen and thermal printer technology.

Under the contract Simens Nixdorf will provide implementation and on-going support for up to 13,000 lanes in 568 Tesco stores. The contract also marks the sale of Siemens Nixdorf's 100,000th BEETLE modular point of sale system.

A spokesperson for Siemens confirmed that the terminals had the capability to be upgraded to Smart Card technology in the future.

Tesco run a loyalty card scheme called Clubcard which has some 9.5 million members. It also offers customers financial services.

Contact: Paula Schmidt**, Siemens Nixdorf - **Tel: +44 (0)1344 850881. E-mail: pschmidt@sni.co.uk

Smart Jurors

Smart Cards have been on trial in Coventry and Leicester Courts Catering Departments for the past two months. The aim of the system is to provide jurors with a Smart Card for all catering expenses during their jury service.

The UK Court system requires 12 men and women to form a jury and to agree a verdict on cases taken before the Crown Court. Jurors are are not paid for this public duty.

Smart Card International claims the system has been successful in reducing jurors out of pocket expenses and has improved loyalty in the Courts catering outlets. The system operates as an automatic 'refreshing' cash purse and is set to refresh twice a day.

The card works in conjunction with Sharp point of sale equipment and Smart Card International's application software built into EPOS internal ROMs. CCM (South West), the Sharp distributor and Smart Card Consultants, are installing the system. Hardware used in all Court installations consists of Gemplus GCR 400 terminals using a 2K bit memory card. To date 5,000 cards have been issued with further orders to follow as more Courts go smart.

Smart Card International told *SCN* that the system has been accepted by the Southern region, Midland and London area Courts. Roll-out will take place over the next six months.

Contact: Bob Cuthbertson,** Managing Director, Smart Card International. **Tel: +44 (0)1482 650999. Fax: +44 (0)1482 52271.

Prima Card

Below Left:
The Prima Card [Gemplus]

The Prima Card is a multi-application loyalty scheme which operates in the retail sector. The scheme is running in Zwolle in the Netherlands with 19,500 cards from Gemplus in circulation. The cards can be used to collect points at four outlets: C&A, Esso, Edah (a supermarket) and HEMA (a department store).

Contact: Jaap Reiter**, Edah. **Tel: +31 49257 1564. Fax: +31 49257 1483.

The FEI's Smart Policy

Right:
Keith Wood,
a consultant in the FEI
[Bull CP8]

The Federation of Electronics Industry (FEI) is a trade association for the UK IT, electronics, communications, office equipment and furniture sectors. It is recognised by the Department of Trade and Industry (DTI) as the major trade association in electronics and influences the European Trade Associations, the European Commission and UK government policy making and regulation.

The FEI offers members a dynamic and unified platform from which to put forward ideas for change through strong lobbying committees. It is also a direct source of vital information, authoritative statistics and sales leads. Most importantly the FEI is committed to ensuring their industry flourishes within the highly competitive international arena.

SCN met with Keith Wood, a Consultant in the FEI, to find out what they are doing on behalf of the Smart Card industry. He told *SCN* that the FEI's first recommendation had been for the government to set up a UK Smart Card Forum. The Forum's first meeting was held in April of this year (*see SCN May 1997*) and an agenda has been established for the immediate future. Recommendations include the government building a close relationship with Europe with a view to setting up a European Smart Card Forum.

Keith told *SCN* that he hopes the Forum will press the government to get co-ordination and take the lead in multi-application Smart Cards. He identified some of the major issues as; common specifications and standards across Europe and the world, national and international regulations, system access, protection of personal data, encryption systems and electronic identification. He believes operators must come together on the essential issues such as identity and privacy.

Keith is currently working on a two-day Roundtable to be held in the UK and attended by European guests. He has received letters of support for this project from across Europe and 35 people have already confirmed their interest. The group is due to meet on 1 and 2 October in London.

The aim is to bring together senior representatives of European companies and organisations with interests in Smart Card developments to discuss the potential benefits of forming a European Smart Card Forum.

The FEI is requesting papers from those attending on subjects such as "essential common items of specification," "intropera bility" and "biometrics." It is hoped a European Forum will develop from such discussion.

The FEI is, however, aware that Smart Card technology will not remain simply a European issue. As Keith Wood commented recently at a seminar hosted by Bull CP8: "It is no use the UK doing their own thing without reference to the global scene." For this reason the FEI is forming relationships with both the US Smart Card Forum and Australia's Asian Pacific Smart Card Forum to build a global link.

Keith Wood stressed his belief in what he personally, and the FEI as a whole, are doing on behalf of the Smart Card industry. He said he was prepared to persevere in the battle for global standards and interoperability and added, in an ideal world, individuals should be asked to carry no more than two or three cards to cover everything.

Contact: Keith Wood**, Consultant, FEI - **Tel: +44 (0)171 331 2000. Fax: +44 (0)171 331 2040. E-mail: kwood@fei.org.uk

Schlumberger Cards in HK

Schlumberger Electronic Transactions is supplying reloadable Visa Cash Smart Cards to the bank of China Group and Standard Chartered Bank for the latest phase in the roll-out of the stored value card scheme in Hong Kong.

IRIS Plant will Produce 60m Cards

IRIS Technologies has completed its new 320,000 square foot headquarters and Smart Card manufacturing facility in the National Technology Park in Kuala Lumpur, Malaysia, which will have an initial capacity of producing 60 million contact Smart Cards per year.

In addition, a contactless Smart Card manufacturing line could turn out between 5 and 10 million cards per year.

Colin Timson, of IRIS Technologies, says: "We are aiming to be a world player in the Smart Card field."

Until now, the company has concentrated mainly on the Far East and Pacific Basin markets, but is gearing up to become a global supplier of Smart Cards and solutions, including full turn key services to government and commercial sectors.

The new headquarters and the manufacturing plant is expected to be officially opened at the end of next month and become fully operational in September.

The plant will be able to take silicon in wafer form for production into modules and cards. Target markets include ID, finance and loyalty sectors.

In the contactless Smart Card sector, IRIS Technologies will be looking at transportation, passenger and baggage identification systems.

***Contact: Colin Timson**, IRIS Technologies - **Tel: +44 (0)117 907 3335. Fax: +44 (0)117 907 3339**.*

Intellect Terminal Certified by Visa

Intellect has announced that Visa International has certified the Intellect 8550 Purse Retailer terminal for use with Visa Cash, Visa's Stored Value Card.

The device is capable of supporting up to six separate electronic cash schemes at once.

Contact, Geoff Gander**, General Manager - Asia Pacific, Intellect - **Tel: +61 9333 4333. Fax: +61 9470 5002. E-mail: geoff.gander@intellect.com.au

Trans-Continental Visa Purchases

It is now possible for people in Europe to sit at a computer and shop securely over the Internet in shopping malls in Singapore - opening the way to international shopping.

The breakthrough came this month in the first use of the Secure Electronic Transaction (SET) protocol between different continents. Selected Visa cardholders with Citibank in Germany can now make purchases from two virtual shopping malls in Singapore:

Singapore Mall (http://www.small.mis.com.sg) and Welcome to BNN (http://www.bnn.com)

Initially, the service will be available to a limited number of cardholders. However, following completion of the pilot, the service will be extended to all Citibank's Visa cardholders. Citibank is the fourth participant to commence transactions in Visa's European Secure Electronic Commerce (SEC) group pilot (*see Visa SEC Pilot Growing, page 127*).

In another development, Visa USA, Bank of America and First Union Corporation will pilot the SET specification for purchases on the Internet this summer. Alaska Airlines is the initial merchant participating in Bank of America's pilot while First Union will work with Interpath Marketing, an Internet provider and sports marketing subsidiary of Capital Broadcasting Corp.

***Contact: Ian Gatherum**, Visa International Press Office - **Tel: +44 (0)171 937 8111**.*

Loose Chippings

- IBM and Gemplus have announced their intention to co-operate in the provision of Global Smart Card solutions.
- De La Rue Card Systems announces Visa Java Card Solution. Their Java Development programme is already well advanced due to close collaboration with both JavaSoft and Visa.
- Schlumberger Retail Petroleum Systems has launched a range of products to boost the company's turnkey forecourt capability for service stations. They include space-saving pumps supported by transaction terminals which open up access to Smart Cards with electronic purses, loyalty functions and co-branding capabilities.

Optical and Smart Card Reader

Drexler Technology Corporation has announced that it has entered into a customer-funded contract to develop a multi-technology card workstation for reading and writing cardholders' optical memory cards and Smart Cards with a microprocessor.

This is a major move in the merger of currently incompatible technologies, but, intriguingly, Drexler won't name the customer who is providing funding of between US $500,000 and US $800,000, depending on the options selected by their anonymous client. Completion of the project is scheduled for early 1998.

Drexler says the customer will have the right to have the card workstations manufactured by Drexler Technology or its subsidiary, LaserCard Systems Corporation, at mutually agreed pricing, delivery and technical specifications. Also Drexler and LaserCard will have the right to sell the multi-technology card workstation through their worldwide value-added reseller network.

By combining the two technologies, a single card could house multiple applications such as Internet electronic commerce, medical insurance, debit transactions, medical/health records, identification, admission tickets, airline and travel benefits programmes.

Drexler reveals that for the card workstation, the optical memory cards will contain an optical memory stripe capable of storing more than 1 megabyte of user data.

The Smart Cards for these applications will be credit card-sized with a microcontroller chip containing a microprocessor and semi-conductor memory. It will be capable of writing and reading data from a single card utilizing its microprocessor for transaction processing and its optical memory for data storage.

Based in Mountain View, California, Drexler manufactures LaserCard optical memory cards that store 1 to 4 megabytes of data.

***Contact: J P Protsik**, Public Relations, Drexler Technology Corporation - **Tel: +1 415 969 7277. Fax: +1 415 969 6121**.*

People on the Move

The supervisory board of the Giesecke & Devrient GmbH unanimously elected **Dr Horst Köhler** as its new Chairman following the resignation of Dr Michael Endres the previous Chairman and member of the managing board of the Deutsche Bank AG in Frankfurt after nearly six years' service.

Dr Köhler has been President of the Deutscher Sparkassen-und Giroverband since August 1993 and President of the Europäische Sparkassenvereinigung in Brussels since mid-1994.

Dominique Trempont has been appointed President of Gemplus Americas with direct operating responsibility for sales, marketing, software engineering and manufacturing in North and South America. He will also be responsible, at corporate level, for mergers and acquisitions and the development of strategic alliances for the Americas.

Prior to joining Gemplus, he was a member of the Office of the President and the Chief Financial Officer of NeXT Software Inc for four years. Brigitte Baumann, President of Gemplus North America, and Bertrand Moussel, President of Gemplus South America, will retain their current responsibilities and will report to Tremont.

Mondex UK Ltd has appointed **Roger Booth** as Deputy Chief Executive. Previously a senior manager with Midland Bank, where his role was developing relationships with major retail organisations, he will be responsible for building Mondex UK's profile with existing and new card-issuing members and other key partners.

Electronic payments system company Hypercom Europe has appointed **Richard Launder** as its new Managing Director. Previously he was Chairman of BASE24 supplier Applied Communications Inc's European operation.

Hypercom Europe, based in Esher, Surrey, in the UK, is the European subsidiary of Hypercom International, headquartered in Phoenix, Arizona.

Smart Card Diary

Cards Australia '97, World Congress Centre, Melbourne, Australia, 26-28 August 1997.

The conference will cover areas such as card strategies for the future, co-branding, loyalty schemes and Smart Card applications. Future trnds will be presented by well respected experts in each field. Contact AIC Exhibitions. Tel: +61 (0) 2 9210 5700. Fax: +61 (0) 2 9223 8216.

Escat 1997, Hotel Hesperia, Helsinki, Finland, September 3 - 5 1997.

An international conference for all progressive, advanced and responsible present or future users, consumers, vendors, developers and manufacturers of Smart Cards in both the private and public sector. Contact: Congrex, tel: +358 9 752 3611. Fax: +358 9 752 0899.

Electronic Commerce and Payments on the Internet, Mandarin Oriental Hotel, Hyde Park, London, 15 - 16 September 1997.

Implementing Solutions and International Standards for Retail Financial Services. Key highlights inlcude: working with a comprehensive cross-industry IT policy; judging the feasibility of an Internet business model; discovering how to build the optimum multi-channel distribution system; analysing emerging technologies working towards a fully interactive banking area; understanding the scope and impact of new international standards.

Tel: +44 (0) 171 915 5149 (Please quote J24957 for the conference).

Scandicards '97, NackaStrand, Stockholm, Sweden, 16 - 18 September 1997.

Will cover areas such as card strategies for the future, co-branding, loyalty schemes and Smart Card applications such as electronic purse and stored value cards. Contact: Pam Chattin, AIC Exhibitions, Tel: +44 (0) 171 827 4155. Fax: +44 (0) 171 242 1508.

The Holland Chipcard Experience, Bilderberg Europa Hotel, Scheveningen (The Hague), Netherlands, 9-10 October 1997.

An International conference for those interested in Smart Card project management, business opportunities and nationwide co-operation (including the pitfalls, obstacles, successes and failures) amongst many other issues.

The conference will look at the Dutch experience with Smart Cards to see what lessons can be learnt.

Contact: Mrs Eugenie Blommestein, Euroforum. Tel: +31 40297 4835. Fax: +31 40297 4976.

Retail Automation International Conference 1997, Royal Garden Hotel, London, 14 - 15 October 1997.

Smart Card News is running a half-day workshop on Electronic Commerce in conjunction with the above conference. Subjects include the following: Doing Business on the Net, Making the Business Case, The Security Infrastructure, Trading Protocols, Electronic Payment Systems and Selling Information on the Net. Contact: Richard Jarvis, Smart Card News Ltd, RMDP, the conference organiser.

Cartes '97, Cnit, Paris, La Defense, France, 15 - 17 October 1997.

A total of 15 conferences joined by the theme 'innovation, integration and new markets'. Covers the major topics current in the plastic card world today.

Topics include: Contactless Cards, Electronic Commerce, Innovations '97, Payment Terminals 2000, Cards and Security, to name but a few.

Also features the SesameS '97 - the international benchmark awards for Best Innovation and Best Application in the plastic card field.

Contact: Tel: +33 1 41 220 220 (available 7 days a week, 24 hours a day). E-mail: cartes@cepexposium.fr Website: http://www.cardshow.com

Integrated Circuit Card Standards and Specifications - Part 10 :

A Security Primer, continued...

In last months discussion we introduced the concept of digital signatures using a public key algorithm such as RSA. We carefully skipped over some of the practical problems which now need to be explored in a little more detail.

Algorithms such as RSA are computationally intensive so the signature process operating on say a large file would not only take a long time to compute but would also produce a signature of similar length to the input message or file. Remembering also that we have to transmit some level of redundancy we can see that the message length would be considerably extended. We solve this problem by the use of hash functions which are a fundamental part of the signature process. A hash functions takes a variable length message as input and generates a fixed size digest of the message typically about 128 bits. A hash function needs to achieve a number of fundamental properties:

1 Collision avoidance, we clearly require that the digit should be unique. We do not want two different messages to produce the same digest (a collision). We cannot entirely avoid collisions because in general the number of possible input messages exceeds the number of possible outputs of the hash function. So it is necessary that the probability of a collision is adequately low, in other words the output size of the hash function must be suitably large (eg 128 bits).

2 It should not be computationally feasible to find a message that hashes to the same value as that calculated for the given message. In other words it should not be possible to alter the input message without altering the output of the hash function.

A purist might not be happy with this second condition and it is common to quote a further qualification as follows:

3 It should not be possible to find any two messages that hash to the same value.

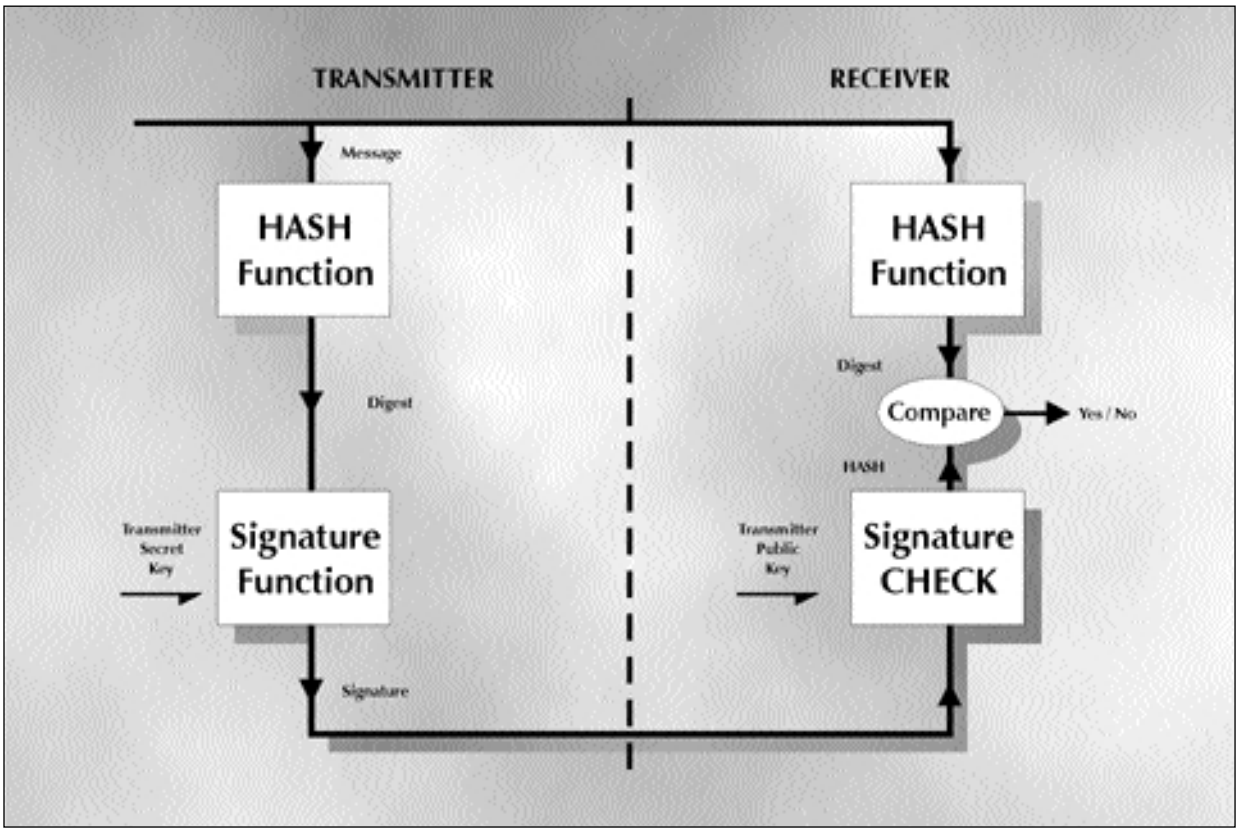
Hash functions which observe the last rule are generally referred to as strong hash functions.

Now readers may not be surprised to know that the design of suitable hash functions is a real art. There are probably more examples of flaws in hash functions than in the more fundamental cryptographic mechanisms. Such hash functions are generally computed by the use of one way functions and may be generated by the use of a block cipher or by functions based on modular arithmetic.

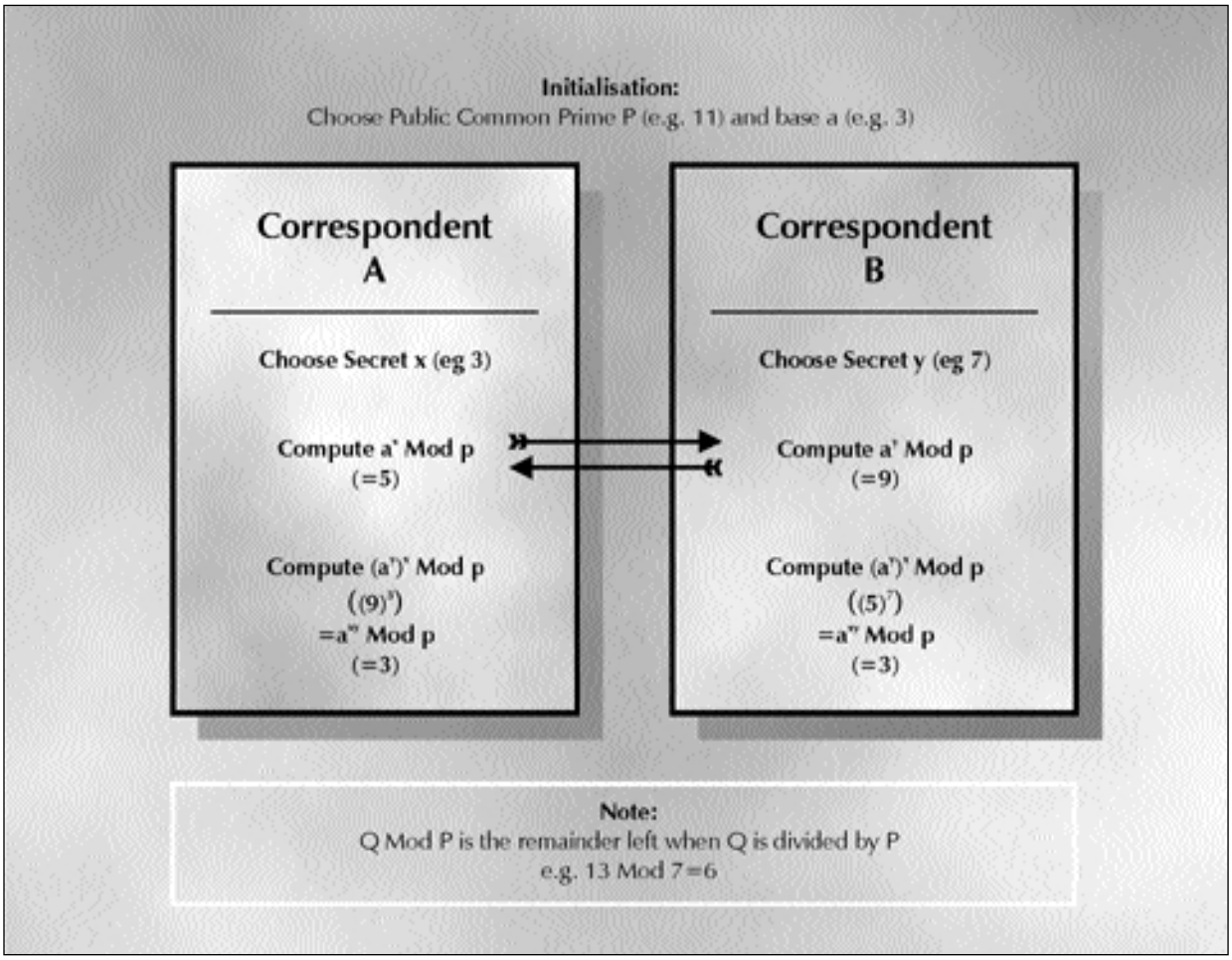
Last month we described the calculation of a message authentication code using the DES algorithm. By using a secret key we were also able to introduce the authentication property but for the purpose of a hash function we could have made the key publically known. In electronic commerce we will frequently run into MD2 and MD5. These are message digest functions designed by Ron Rivest (of the RSA trio). Another algorithm that is now widely recommended is SHA-1 (Secure Hash Algorithm) which was designed as part of the US Digital Signature Standard (DSS).

We can now put together our complete signature process on as show in *figure 1* opposite: The transmitter first calculates the hash or message digest. It is this digest that is then processed by the signature function using the secret key. The message and signature are transmitted to the receiver where the receiver then computes the digest of the message using the same hash function which is usually a publically known function. The receiver then recovers the message digest from the provided signature by using the transmitter's public key. The two digests are then computed to determine the validity of the signature process.

It is at this stage that we need to consider the black art of key management. In the early days of message security it was this area that caused all the problems. This was the particular disadvantage of symmetric cryptography where it was necessary to establish the same secret key at both ends of the communication channel. In many ways it was the capability of public key systems to handle this problem in a manageable way that led to their widespread use in message security systems. The use of digital signatures in practical applications came somewhat later.

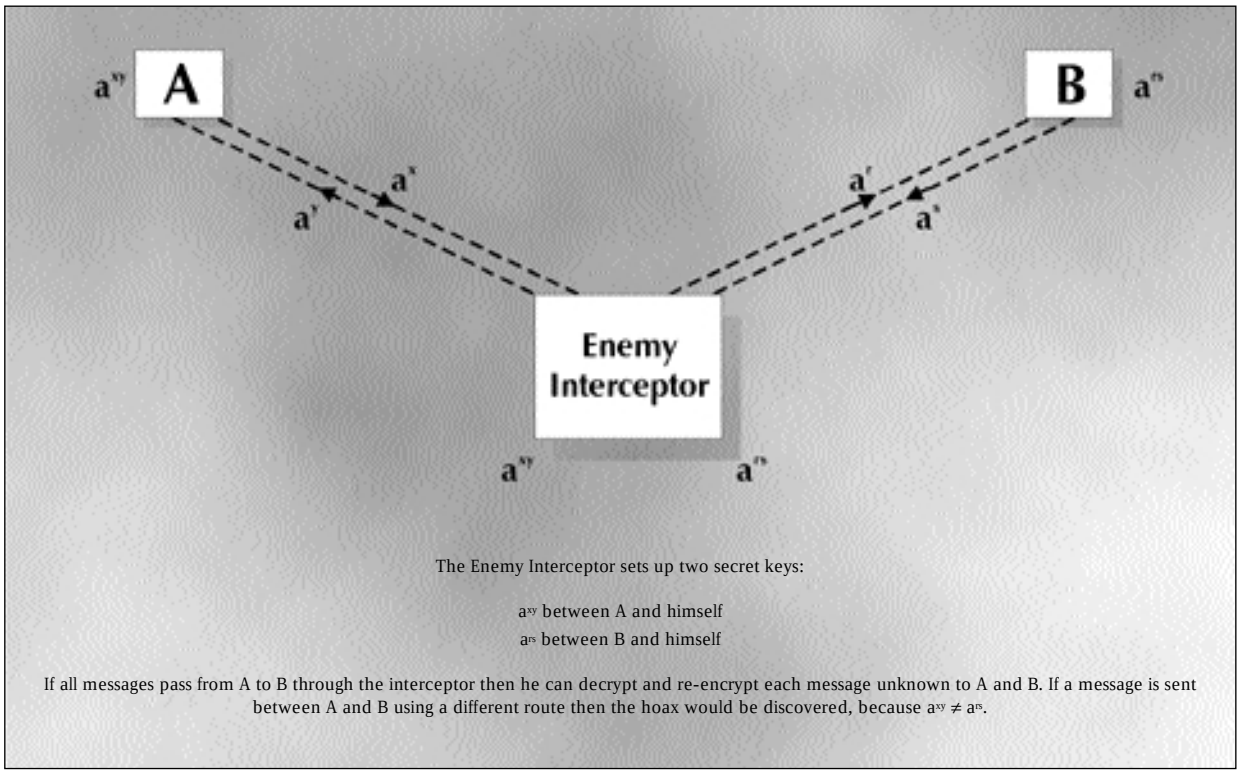


Left:
Figure 1



Left:
Figure 2
Diffie-Hellman Key Exchange

Right:
Figure 3
Diffie-Hellman Key
Exchange Vulnerability



The Enemy Interceptor sets up two secret keys:

a^{xy} between A and himself
a^{rs} between B and himself

If all messages pass from A to B through the interceptor then he can decrypt and re-encrypt each message unknown to A and B. If a message is sent between A and B using a different route then the hoax would be discovered, because $a^{xy} \neq a^{rs}$.

So how do you distribute secret keys amongst a number of participants? In truth with great difficulty. The general process was to install a common master key in the correspondent nodes using secure processes. A common technique is to generate this master key in parts (say 3 components) where each part is generated and managed by a trusted party. These three individuals come together at the correspondent nodes where they separately enter their key into the trusted cryptographic equipment. For a small number of nodes co-located this was a manageable process but today the geographical displacement and sheer scale of the operation makes this approach impractical. If we consider for example an EFTPOS (Electronic Funds Transfer at the Point Of Sale) scheme it is clear that you can't send a team of people around to every terminal and it was this problem that taxed the thinking of the designers. Of course once you have established this initial key relationship you can lever off it to generate session keys, it was just the initial process that caused the problem.

The introduction of public key systems caused a paradigm shift in thinking for which the Diffie Hellman algorithm was fundamental. Here was a way of establishing a common secret in two end points using a public connection medium. The process which is widely used today is worthy of further consideration. It is based on the use of a one way function using modular arithmetic. The crux of this system is the difficulty or work function of inverting the one way function. The operation of this process is shown in *figure 2* (previous page):

To help the explanation we have used some simple numbers as an example. As can be seen we end up with the common secret number 3 at both A and B. The security relies on the fact that we cannot invert the discrete log function (eg given a^x mod p we cannot feasibly determine x). This is the classical logarithm problem. Now given the number in the example such an inversion would be trivial but it is left as an example for the reader to try such an inversion using numbers of say 512 bits long. It is important to note that the Diffie Hellman key exchange relies on authentic communication. If you were communicating remotely with a third party then an enemy could interpose himself in the middle and set up a relay attack as shown in *figure 3,* above. An additional process must be applied to ensure that the true end points receive an authentic set of values. For instance one might use two communication paths either to communicate the values or to check their authenticity.

David Everett

Next month: Certification Authorities

Mondex in Israel

Discount Investment Corporation (DIC), part of the IDB Holding Group and Paz Oil Co., recently announced that they have purchased the Mondex electronic cash franchise rights for Israel.

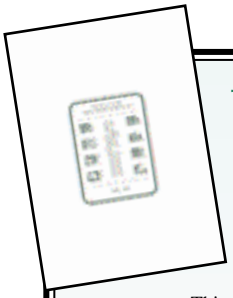
The franchise gives DIC and Paz the exclusive rights to commercially develop Mondex electronic cash for Israeli residents.

DIC is one of Israel's largest investment companies with total assets approaching US$ 1 billion. Paz Oil Company Ltd. is Israel's largest supplier of refined petroleum products. In 1996 Paz activities resulted in sales before tax of US$ 1.361 million.

DIC and Paz have taken the decision to develop Mondex with a coalition of partners from banking, industry and the merchant community to try and ensure widespread acceptance.

The group plans to introduce Mondex in the first quarter of 1998 utilising the new MULTOS operating system for Smart Cards (see *SCN* May 1997).

Contact: Idith Yaaron**, Mondex Israel. **Tel: +972 (0) 3 693 9393.** **Robin O'Kelly**, Mondex International, **Tel: +44 (0) 171 557 5016 / 5036.



The International Smart Card Industry Guide 1997/98

The third edition of the International Smart Card Industry Guide is due for publication in September.

This year's edition will be even more comprehensive, covering current Smart Card projects and providing a Directory of Companies with descriptions of their products, services, and contact names and addresses.

In addition there will be feature articles on the *Java Electronic Commerce Framework*, *Java Card or MULTOS - What Do I Choose?* and *Electronic Money and Government* written by industry experts.

Retailing at just **£125** plus postage, this Guide is an essential reference book to keep abreast of the fast-moving technology and its players.

Subscribers to SCN can purchase the Guide for **£70** plus postage. To order or for more information please contact the Marketing Manager **Albert Andoh** on +44 (0) 1273 236677.

Multi-Function Cards in Holland

Right:
Giropas: a multi-function chip card for Postbank
See cover story
[Chipper Nederland]

Far Right:
The Peanut Marketing Card
[USDA]

Electronic Purse Trial for Japan

Nippon Telegraph and Telephone Corporation is planning a major electronic purse trial starting next year in the Shinjuku district of Tokyo involving city banks and major department stores.

Some 100,000 customers are expected to take part. They will be able to reload the cards at the banks to make telephone calls, purchases at retail outlets and to shop on the Internet by inserting the card into a reading device connected to their home computers.

Smart Card Computer Keyboard

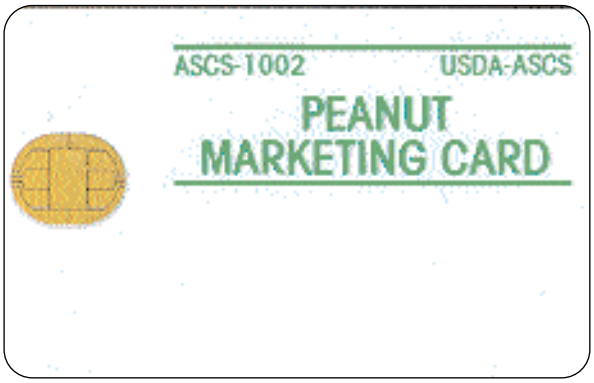
Hewlett-Packard rolled out a Smart Card computer keyboard at the PC Expo in New York last month. The keyboard has an integrated Smart Card reader, drivers and resource managers for Microsoft Windows 95 and NT.

It incorporates PIN processing technology from H-P for security so that the Smart Card PIN never resides on the PC itself, but stays encrypted on the keyboard, eliminating the risk of hackers accessing the PC and discovering the PIN.

The keyboard, developed by Key Tronic Corp and H-P-acquired VeriFone, is based on the PC/SC Workgroup standard developed by leading international companies to ensure that Smart Cards, readers and Personal Computers made by different manufacturers will interoperate.

Contact: Mark McMurtrie**, VeriFone - **Tel: +44 (0)1895 824031. E-mail: Mark_ml@verifone.com

US Smart Peanut Project



As Smart Card projects become ever more advanced and sophisticated it is interesting to look at the US Peanut project which has been on-going since the late 1980s. The US Department of Agriculture (USDA) has been using a Smart Card system to keep track of peanut marketing since 1986.

Price support legislation means a quota of peanuts is set that farmers may grow to be exchanged for a guaranteed price. With between 60,000 and 70,000 peanut producers, 540 peanut buying points and 25 peanut shellers, the potential for mistakes in a paper-based system was high.

In 1985 a feasibility study was conducted to explore the possible use of Smart Card technology. The following year a pilot began involving six states and 19 counties. Full implimentation began in 1987 and ten years later is still in use today.

Smart Cards supplied by Bull/MicroCard Technologies have been issued to each peanut farmer and card reader terminals are installed at each peanut buying location. When a peanut load is brought to the buying location the holder's card is inserted into the reader. The quota is validated and the information is then updated.

A cost/benefit study revealed that: for every US Dollar spent on the automation process a resulting benefit of US $2.27 was realised. The cost and benefit to the Government from the Peanut Buying Project were quantified and compared from 1985 - 1996. The net present value of the project is estimated to be US $15,206,010 (in 1985 dollars).

Contact: Tonye Gross**, USDA - **Tel: +1 202 720 4319. Fax: +1 202 690 1536. E-mail: tgross@wdc.fsa.usda.gov