Spanish Banks toLaunch Electronic Purse Scheme

A Smart Card Electronic Purse is to be launched in Spain by the Spanish banking consortium, Sociedad Espanola de Medios de Pago (SEMP), who expect to distribute around four million cards nationwide.

Solaic, the Smart Card subsidiary of Groupe Sligos, France, will make and supply SX microprocessor cards and write the application software for the project.

Continued on page 183

Paying by Smart Card using a Siemens-Nixdorf terminal in Danmont's cashless shopping project in Denmark.

Smart Card News

Editor: Jack Smith

Technical Advisor: Dr David B Everett

Editorial Consultants:

Dr Donald W Davies, CBE FRS
Independent Security Consultant

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

Chris Jarman
Managing Director
Orga Card Systems (UK) Ltd

Published monthly by:

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

ISSN: 0967-196X

Next Month

Smart Card Tutorial Part 15 - Cryptography & Key Management continued

CONTENTS

Spanish Electronic Purse

Continued from page 181

Groupe Sligos subsidiary Poli-Rub, which manufactures magnetic stripe cards, enabled Solaic to win the contract from SEMP, a banking consortium representing some of the major banks in Spain and promoting the Spanish use of electronic purse cards.

Jose Maria Perez Soria, who is the Project Leader and Manager of the New Technology Department at SEMP, said they had already defined the operating system for a multi-purpose Smart Card and expected to start technology tests in the first quarter of 1994. Trials would then follow in universities like Barcelona and perhaps Madrid during the university course period from October 1994-June 1995. The universities were being considered because they were closed sites. In a second phase it was planned to launch the card in several markets with several service providers such as transport and other services like vending machines and newspaper outlets.

The card would therefore be used for banking and multi-applications purposes with the electronic purse being recharged at ATMs, Point-of-Sale terminals and self-service machines.

He said they did not expect to use more than 500,000 cards in 1994, but that depended on demand. After 1995 there would be other service providers, like transport, and the use of cards would increase. It is anticipated that the banking group will source cards from several suppliers.

Second contract in Portugal

A second contract for Solaic is to supply point-of-sale electronic purse cards to Sociedade InterBancaria de Servicos (SIBS), a private company owned by 29 Portuguese banks, which plans to launch its Smart Card electronic purse scheme nationwide next year. Gemplus Card International are supplying 500,000 cards. The Solaic card order is for merchant cards.

Customers will be able to use the card to make payments at merchants who are not equipped with electronic payment terminals connected to remote processing centres.

The Solaic contracts are their first two to supply electronic purse cards, and the company says they underscore their commitment to expand into the European microprocessor Smart Card market with an emphasis on electronic purse and health cards. The company is already a leading supplier of telephone cards.

Card details:

Type	Contact
Fabricator	Solaic
Dimensions	ISO ID-1
Contact locationFront	
Chip type	Microcontroller+memory
Chip manufacturers	Motorola and SGS-Thomson
Chip reference nos	MC68HC05SCXXX and ST16XYZ
Memory type	EEPROM
Memory capacity	
Mask ROM	6K bytes
EEPROM	3K bytes
RAM	128 bytes
Standards	ISO 7816-1/2/3
Comms protocol	T=0
Security	PIN
Cryptography	DES

Contacts: Jose Maria Perez Soria, Project Leader, New Technology Department, Sociedad Espanola de Medios de Pago, Spain -Tel: +34 1 346 5300; Charles Juster, Communication, Groupe Sligos, France -Tel: +33 1 49 00 96 33.

Nethold to Distribute VideoCrypt

News Datacom, provider of conditional access systems to BSkyB in the UK and DirecTV in the US, has announced an agreement allowing Nethold, a company controlling European pay TV operator FilmNet, to use News Datacom's analogue VideoCrypt technology to distribute channels of the Astra satellite.

The agreement covers over 20 countries in the Astra footprint, ranging from Benelux in the West, the Baltic States in the East, and Greece, Cyprus and Portugal in the South.

Contacts: Valerie Gopthal, News Datacom, England -Tel: +44 (0)628 74774.

La Poste Announce EP Plan

La Post, the French Post Office, is to develop a Smart Card Electronic Purse system with the French consortium of Bull CP8 and Philips-TRT.

The announcement was made early this month on the occasion of the celebration of the 10th anniversary of SEPT (Service d'Etudes de la Poste et des Telecommunications).

After working with SEPT on a system for securely transferring cash between Smart Cards, La Poste has now given the go-ahead for the Bull CP8/TRT-Philips consortium to develop the two operating systems required - one for the electronic purse itself, and the other for the security modules needed at every level of the system.

The security of the system is based not only on proven cryptographic techniques, but also on the development of eight new masks (one for the electronic purse, and seven for the security modules).

La Poste said the development contract will allow them to have a full industrial solution available by the end of 1994.

Bull CP8 and Philips-TRT will have the right, pending prior approval of La Poste, to offer the solution to their own customers.

Potential service providers

It was widely expected that the major French banks would join in a national electronic purse scheme. Their decision not to do so may be one that they will regret in the future.

La Poste is talking to potential service providers and there is said to be considerable interest from the Paris Metro, the French capital's underground rail system, and from bus and rail operators. The Paris Council, which operates the Paris Carte pre-paid Smart Card for parking in the city, is also discussing the possibility of incorporating this service on the La Poste Card.

All the French bank cards are now Smart Cards and there are well over 20 million currently in circulation. However, La Poste has over 3,000 Post Offices which could be considered as primary outlets for electronic purse cards, as well as many other smaller offices. A particular advantage is that the card will be available to people who do not have or do not qualify for a bank card, as well as bank customers.

Contact: Laurence Grazilhon, Marketing and Communications, La Post, Paris, France - Tel: +33 1 44 10 77 80.

Sligos Half-year Results

Groupe Sligos, the French computer services company, reports FF 1.78 billion in sales for the first six months of 1993, an increase of 0.9% over the same period last year.

The Groupe says that its resilience in the current challenging economic environment has been driven by its strategy of expanding further into Europe in order to acquire recurring business activities and critical mass.

It reports that the first half-year demand for systems development services in Spain and Germany slowed down, but remained firm in Italy and France. The banking and card-processing business enjoyed strong growth in Germany while there was an increase in payment services sales orders in the United Kingdom and Ireland. The payment media, manufacturing and personalisation business reported a 24% increase in sales in France and abroad. Sligos expects to report a 4-4.5% net return on full year sales of nearly FF 4 billion in 1993.

Gemplus Deputy Manager

Gemplus has strengthened its management team with the appointment of Hubert Giraud as Deputy General Manager.

Aged 36, he is a French citizen and holds diplomas in political sciences and administration studies from the Institut d'Etudes de Sciences Politiques de Paris and Ecole Nationale d'Administration. He has held posts in several French Ministries and, prior to joining Gemplus, was the Public Sector Financial Director with the

Societe Generale.

Schlumberger/Diebold Agreement

Diebold, the USA's largest manufacturer of financial self-service transaction systems has signed an agreement to become an exclusive distributor of Schlumberger electronic funds transfer point-of-sale (EFT/POS) terminals in the US market.

Robert P Barone, Diebold Vice-Chairman, says: "We expect sales of EFT/POS debit systems to grow exponentially over the next several years as consumer acceptance continues to rise and the US Government steps up its electronic benefits transfer (EBT) programmes. By combining Schlumberger's resources in electronic transactions and Smart Card technologies with Diebold's systems integration and self-service debit card expertise, we are well-positioned to substantially influence electronic payment systems development."

The new Diebold terminal family will be among the first in the US capable of accepting both magnetic stripe and Smart Cards for authorising EBT, credit and debit transactions.

Important industry trends

The current emergence of dual technology cards and electronic terminals that accept them are important industry trends. While magnetic stripe cards are dominant in today's EFT/POS market, the use of Smart Cards, as well as cards that offer both of the technologies on one card, are increasing, said Gerard Buffiere, Vice-President and General Manager of Schlumberger's Test and Systems Division. He added: "Major banks are moving strategically to incorporate newer card technologies in order to increase POS transaction volumes even further.

"European and Asian banks are moving rapidly towards the use of Smart Cards and we anticipate that the US market will follow very soon. The agreement with Diebold enables us to take advantage of that trend".

Contacts: Bertrand Dussauge, Director of Communications, Schlumberger Technologies Smart Cards & Systems, France - Tel: +33 1 47 46 62 47. Fax: +33 1 47 46 68 66. John Kirstoff, Diebold, USA -Tel: +1 216 588 3782.

New Santal Card

Trials will start with a new card and equipment as the Santal Patient Card project enters phase two at the beginning of 1994.

The project has been tested since 1988 in the St. Nazaire area (population 250,000) in northern France, and some 36,000 cards have been issued. The scheme involves eight hospitals, 12 laboratories and 50 medical practitioners.

In this first phase, Bull 8K byte EEPROM cards were used and offered free of charge to hospital patients when they were admitted and when they consulted town practitioners.

Second phase

The second phase, which will run for the three years 1994-1996, will use Smart Cards from Solaic (card technical details on page 183). In addition to the patient card information the card will record the last three prescriptions. Doctors will be able to consult and update medical information contained on the card as well as writing prescriptions onto the card.

Initially, only 10 town practitioners and five pharmacists will be involved, but the scheme will be extended, and it is expected that at least 60,000 cards will be issued during the test period.
A similar project is to be carried out in Sweden and it is hoped that this work will lead to a European standard.

Contact: Philippe Cirre, Centre Hospitalier St. Nazaire, France - Tel: +33 40 90 60 11.

Norwegian Smart Bank Card

The Christiania Banken Kreditkassen, Norway, has ordered 44,000 Smart bank cards from Bull CP8, France. The order comprises 30,000 national cards and 14,000 VISA cards.

The card is a 1K byte EPROM card with the M4 Mask BO'. It is a hybrid card with a magnetic stripe on the back. The Norwegian EFTPOS system is based on the magnetic stripe card but terminals are capable of reading Smart Cards.

Taxi-Cab POS System in Berlin

Three thousand taxis in Berlin, Germany, are being equipped with a new Taxi-Cab Point-of-Sale system for cashless transaction processing developed by Wellcom GmbH, of Munich.

About 400 special meters have already been installed and they are designed to accept all credit cards (American Express, Diners, Eurocard, Visa, JCB), debit cards (ec cards) CabCharge Cards, and Smart Cards - specifically the Berlin Card currently under trial in the capital. (SCN December 1992).

This card is being piloted by BVG, the Berlin transport service, and was used initially to purchase tickets for local travel on selected buses and trains. Now that it is being extended to taxis it will be an added attraction for users.

The card is a multi-function card from Siemens-Nixdorf offering an electronic purse function. It can be recharged at attended terminals and at special recharging centres being installed, mainly in the U-Bahn underground stations which may start accepting the electronic purse in the future.

The System

The taxi driver has a transaction terminal called Cab-Easy into which he swipes his customer's card and enters the transaction details as requested. The device applies a set of test criterion to reject bad cards. It also prints out receipts.

In addition, the driver has a Cab-Ram, a credit card sized, removable memory device used as the transport and storage medium for all the operational parameters of Cab-Easy. This includes the card types to be accepted, hot lists of invalid accounts, and storage of all transactions. There is enough storage space for 200,000 hot card numbers or 2,000 transactions.

When the taxi driver wants to deposit his transactions into his central administration for reconciliation, he goes to a Cab-Bank and inserts his Cab-Ram card. The Cab-Bank forwards the transactions automatically with no other operator action required.

The device refreshes the operational parameters and hot lists and provides a confirmation advice of the data exchange.

If a taxi driver is unable to use a Cab-Bank for whatever reason, he can communicate with the taxi administration centre from the comfort of his own home using a Cab-Easy modem shoe.

At the taxi administration centre, a micro host computer is used to process the transactions and collate operational parameters and security data for distribution into the field.

A further element in the system is the National CabCharge Host which provides the gateway for local operators to exchange data nationally and internationally. A local micro host computer can communicate with a national host when required to clear a CabCharge account not held locally by that administration - about 20% of the traffic. (CabCharge Cards for cashless payments were developed by the taxi industry and launched in Europe in 1990.)

Taxi-Cab POS benefits

Benefits for taxi administrators are seen as: improved service profile, reduced paperwork, improved account visibility and control, integration with municipal transport systems, automatic customer account management, and improved security for employees.

Advantages for the taxi driver are: the removal of cash from the cab reducing risk from mugging, simple and secure operation, rapid and reliable payment ensured, removal of foreign currency and language problems, lucrative corporate affiliations, and increased trade due to integration with public transport.

From the customers' point of view, advantages are: no need to carry cash to use a taxi, removal of foreign currency and language problems, detailed activity reporting on monthly statements, and security for children and special concern groups.

Contacts: Jurgen Platt, Wellcom GmbH, Germany -Tel: +49 89 782046. Fax: +49 89 782040; Manfred Reichherzer, Siemens-Nixdorf, Germany - Tel: +49 89 636 2471.

Patient Data Cards in Europe

In a move to harmonise the development of Patient Data Cards (PDCs) in the European Community, AIM, Advanced Informatics in Medicine, has launched a concerted action known as "Eurocards." The objective is to extend the use of PDCs in Europe by achieving coherence among local initiatives.

Dr Niels Rossing, Director of the AIM Programme, DG XIII, Commission to the European Communities, and Antonio Pernice, explained the Eurocards initiative at the "Health Care Card Systems: Facts and the Future," conference in Marseilles, France, last month.

In their paper the authors identified critical strategic directions as follows:

* the expansion, co-ordination and assessment of experiments in the area of the so-called clinical applications (vertical applications referring to a specific type of disease, for instance, chronical diseases, diabetes, dialysis, etc) and integration of these experiments on the basis of a common platform and of an interoperable interface.

* the support to the identification of horizontal application areas linking administrative and clinical aspects, where the same infrastructure could be shared (emergency, prescriptions).

* the extension of the use of the professional card, which identifies the holder as a (para-) medical professional, entitled to have access to specific classes of information related to an individual patient in a local or in a distributed database, or to receive specific professional information and/or services.

* actions directed to the national authorities and to service providers, promoting the awareness on the possibilities and the impact of the PDC and the benefits for the users. For this purpose the concerted action is also linked with CEN (TC 251 Working Party 7) and with other related activities of AIM.

The report of the AIM working group for PDCs (1989-90) outlined the kind of data and the data structure for cards within the Community and recommended a "template" structure for accessing information stored in the card, as it meets the need of cardholders and health care professionals without compromise to security or confidentiality. The "template" tailors the access to medical data and controls the ability to write on the card according to the needs of the different types of health care personnel.

If PDCs are to facilitate the transfer of medical data across European boundaries, then data must be written on the card using a common code as several different codes in health care are in use within individual European countries. The development and use of minimum data sets accepted throughout Europe will maximize information exchange.

Issues of confidentiality and security of patients records is a major concern, but the broad principles outlined in the various Data Protection Acts within Europe can form a substantial basis on which the use of PDCs can be implemented. For example it is now widely accepted that the decision to use a card containing personal medical information must remain with the individual citizen on a voluntary basis.

Comprehensive framework

The objective of the AIM actions on PDCs is to provide a comprehensive framework for research and development activities run on a European basis. Coherence among local initiatives is required if the PDCs are to be used across national borders and the key message is if any trials are going to be set up in the EC it is recommended that Eurocards be contacted and that work be planned together with its representatives.

The involved group will function as a clearing house for all PDC experience in Europe and much money can be saved by avoiding redundancies and overlapping and by exploiting the existing experiences.

The CEC-AIM Office is at Avenue de Beaulieu 29 3/37, B-1049 Brussels, Belgium - Tel: +32 2 296 3508. Fax: +32 2 296 0181.

Overview of Health Care

Twenty-seven countries were represented at the international conference on "Health Care Card Systems: Facts and the Future," held in Marseilles, France, last month. There were 430 attendees, including 60 speakers and 20 session chairpersons, demonstrating the high level of interest in health care Smart Card applications.

A key session centred on the presentation of national policies and strategies by Ministries of Health and Social Services involved in the introduction of this technology. While France and Germany are setting the pace in Europe it was interesting to hear of the developments in other countries, and delegates had the rare opportunity of hearing about health card progress in Japan.

Japan

Koji Miura, Director, Office of Medical Technology Development, Ministry of Health and Welfare, Japan, said the personal health card system has been developed by the Ministry of Health and Welfare since 1987 using an 8K byte IC card. The first field trial was introduced at the relatively small and remote town of Goshiki (population 10,000). In the first three years, 500 cards were provided free to volunteers who were 65 years old or over. At the end of that period 80% of the cardholders said they would have applied for the card even if they had been charged. After six years, about half of the population now hold cards.

A second trial has been going on in the city of Himeji (population 500,000) since 1990 to investigate the system's applicability in an urban area. Here the health card is issued from a health centre where all basic non-medical data and some medical data are input. Participating physicians input their patients' medical data at the point of service. Some 104 medical facilities are participating and the number of cards to be issued is 7,000.

In addition more than 20 projects have been conducted by cities or hospitals in Japan, mostly on a relatively small scale compared with the projects sponsored by MHW. Some of them do not use IC cards, but optical cards.

France

Pierre Antonmattei, Director of the French Ministry of Health and Social Affairs, reported that there had been about 20 different card projects since the first trial of a French health care card, the Carte Sante, in Blois in 1985.

He told delegates about the work going on in three important areas:

* the development of a Health Professional Card, unique to each health professional, and constituting an access key to all medical and medico-administrative hospital data systems while respecting the privacy of individuals.

* the Carte Vitale health insurance Smart Card project to streamline insurance administration and payments and reduce the mountain of paperwork involved (over 800 million reimbursement claim forms a year).

* the Santal application to improve communications within the hospital environment and with doctors' surgeries.

Germany

Georg Baum, Federal Ministry for Health, Germany, said that in a comprehensive reform of the public health care system, it was decided to replace the health insurance certificate with a health care card and by 1 January, 1995, at the latest, this card would serve as a treatment pass for some 70 million insured persons in the Federal Republic of Germany.

The Netherlands

Bert Brunninkhuis, Ministry of Welfare, Health and Cultural Affairs, The Netherlands, said there were 24 initiatives in the development of a care card, varying from an initial study to the exploitation phase. These involved 15 insurers and seven providers of care. Together insurers and providers of care had started six projects.

It appeared from a study that the large-scale introduction of the card could be expected between 1995 and 1997.

An initial development was the establishment of a national chip card platform in which government and industry would combine forces in order to create such conditions that large-scale introduction of the chip card would become possible.

Portugal

Anibal Rodrigues, of the Portuguese Ministry of Health, said the project to provide a Patient Data Card was considered a priority but there were problems of an ethical and legal nature. The creation of automated files containing personal data, and in the event, the data processing of a national patient record, created some major constitutional problems with the human rights issue. There were also some difficulties in the funding of the project due to the high costs attached to any of the forwarded solutions and to the present context that forced cuts in spending.

Owing to these restraints and the forecast that 8 million Patient Data Cards would be issued in the next two years, magnetic stripe cards were favoured.

Sweden

Mrs Leni Bjorklund, Director of the Swedish Institute for the Development of Health Care (SPRI), said that in 1989 a Smart Card trial was started in Tjorn, a small island on the west coast near Gothenburg to test the possibility of using the patient card to hold prescriptions. Recently, Apoteksbolaget, the National Pharmacy Corporation which runs all pharmacies in Sweden, decided to promote the general introduction of the technology.

SPRI and Apoteksbolaget were now planning a trial with around 50,000 patients in one region where the effects of prescriptions on cards and other medical and administrative date would be studied. There had been another trial in southern Sweden restricted to laboratory results on a Smart Card, and a trial had just started restricted to maternity care.

Canada

In Canada, public (government and non-government) agencies used plastic identification cards in the day-to-day administration of health care insured benefits/service programs primarily for identification for entitlement, said Richard Alvarez, Assistant Deputy Minister, Corporate Services and Management Support Division, Alberta Health, Canada. Existing cards generally did not carry payment, medical or utilisation data and the highest level of card technology used was the magnetic stripe. The Canadian Red Cross, for example, issued a magnetic stripe card to blood donors, carrying blood group and type.

In the private sector, Green Shield was most active with Smart Cards in experiments in North Bay and Essex County for its drug benefit plan. Activities involving advanced cards in Canada could be characterised as essentially experimental or investigative. There was a role for IC cards for small, special purpose applications, but its role in large-scale payment and transaction processing for health care/services or in health records management remained uncertain.

USA

In the USA, where President Clinton has made health care reform a priority, Smart Cards have been seriously considered in a proposal that everyone will receive a standard card, often called the Health Security Card, which will uniquely identify the individual, said Daniel L Maloney, a member of the White House National Health Task Force Work Group on Patient Information Systems.

While the Smart Card was not widely used in the United States at present, the situation was changing as regional pilots introduced the advantages of Smart Card technology to more and more people. Examples of regional health care field tests included the Western Governors' Association Health Passport Project which proposes to use Smart Cards to deliver public and private health services for mothers and children in Western states; and the Department of Defense proposing the Multi-Technology Automated Reader Card (MARC) in a medical setting in the state of Hawaii.

He concluded that in the health care reform there would probably be a standards-based health care card, but its exact characteristics had not been finalised.

Gemplus Personalisation Centre

Gemplus has opened a European Smart Card personalisation centre at Sarcelles (Val d'Oise) near the international airport at Roissy, Paris. It will have an installed production capacity at end December 1993 of 1-1.5 million cards per month, and the flexibility for further expansion.

Gemplus PSI has been created in response to the Group's rapid growth in banking and GSM mobile telephone markets in France, Europe and elsewhere.

The centre will also meet the demands of Smart Card markets such as pay-TV, healthcare, database management, logical access control for micro-computer databases and telematic servers, etc. It can also cater for markets using plastic cards without microchips such as private cards, customer loyalty cards, and credit cards.

Security

Security at the premises comply with the recommendations of the french Bank Card Syndicate and the equipment used ensures confidential data processing and card management for all services from database reception by packet switching network to direct mailing of Smart Cards and secret codes to the issuer or end user by separate mailing.

Photographs on this page show some of the card personalisation machinery used in the new centre. For security reasons, photography is not allowed inside the premises.

Gemplus PSI will employ approximately 40 people in 1994 and forecasts the creation of 100 jobs by 1995.

Formed five years ago in Gemenos in the South of France, the Gemplus Group has a Smart Card production capacity of 14 million cards per month.

Gemplus PSI is at 1 Place de Navarre, 95200 Sarcelles, France. Jean-Pierre Caunac has been appointed General Manager, and Benoit Mellerio, Marketing and Sales Manager.

Contact:Lucien Dugachard,Pesonalisation Services - Tel: +33 1 39 33 08 00.

Cambridge Road Pricing Trials

Road pricing trials began in Cambridge, England, early this month as part of the European Commission-funded ADEPT (Automated Debiting and Electronic Payment for Transport) project (SCN July 1992).

The trials will run for about three weeks and involve three County Council vehicles which are equipped with computerised meters which deduct cost units from Smart Cards supplied by McCorquodale Card Technology, England.

The meters are activated by microwave beacons on the roadside which facilitate three types of road pricing:

* single entry toll

* distance-based charging

* congestion only charging

Other trial sites in the ADEPT project are in Gothenborg, Sweden; Lisbon, Portugal; Thessaloniki, Greece; and Trondheim, Norway.

Mike Sharp, County Council Director of Transportation, says: "This is a very important development which we are pleased to be involved in. Opportunities must be taken to explore the use of advanced technology in transport systems.

"The results of these trials will be collated with those from other European experiments in order to develop a standardised approach throughout Europe."

Contacts: Philip Blythe, Senior Research Associate, Transport Operations Research Group, University of Newcastle-upon-Tyne, England - Tel: +44 (0)91 222 8352; Rodney Woodhatch, McCorquodale Card Technology, England - Tel: +44 (0)737 223373.

Smart Card Microcontrollers Part 2

Manufacturer	Philips	SGS-Thomson	SGS-Thomson
Type number	83C852	ST16301	ST16612
Microcontroller core	80C51	ST16XYZ	ST16XYZ
Architecture	8 bits	8 bits	8 bits
ROM	6K bytes	3K bytes	6K bytes
EEPROM	2K bytes	1K bytes	2K bytes
ECC	Yes		
Page write		1-32 bytes	1-32 bytes
EPROM	-	-	-
Write cycles endurance	10K	100K	100K
RAM	256 bytes	128 bytes	160 bytes
OTP memory	No	No	No
Voltage	5V	5V	5V
Max clock speed	6MHz	5MHz (Internal)	5MHz (Internal)
Max current	15mA	15mA	15mA
Sleep mode	Yes (100uA)	No	No
Special functions	Coprocessor (modular arithmetic)	Random Number Generator	Random Number Generator
Die size	3.8mm X 5.9mm	N/A	N/A
I/O ports	2	2	2
Availability	On request	Now	Now

SGS-Thomson	SGS-Thomson	SGS-Thomson	SGS-Thomson
ST16B22	ST16623	ST16V623	ST16F48
ST16XYZ	ST16XYZ	ST16XYZ	
8 bits	8 bits	8 bits	
11K bytes	6K bytes	6K bytes	16K bytes
2K bytes	3K bytes	3K bytes	8K bytes
1-32 bytes	1-32 bytes	1-32 bytes	1-32 bytes
-	-	-	-
100K	100K	100K	100K
224 bytes	224 bytes	224 bytes	288 bytes
No	No	No	No
5V	5V	5V	5V
5MHz(Internal)	5MHz (Internal)	2MHz (Internal)	5MHz(Internal)
15mA	15mA	15mA	15mA
No	No	No	Yes
Random Number Generator	Random Number Generator	Random Number Generator	Random Number Generator
N/A	N/A	N/A	N/A
2	2	2	2
Now	Now	Now	Now

Manufacturer	SGS-Thomson	Siemens	Siemens
Type number	ST16C853	SLE44C10	SLE44C40
Microcontroller core	ST16XYZ	Sieco (8051 Op code Compatable)	Sieco
Architecture	8 bits	8 bits	8 bits
ROM	8K bytes	8K bytes	8K bytes
EEPROM	2.5K bytes	1K bytes	4K bytes
ECC		Yes	Yes
Page write	1-32 bytes	4 bytes	4 bytes
EPROM	-	-	-
Write cycles endurance	100K	10K (70^0C, 5V)	10K (70^0C, 5V)
RAM	352 bytes	256 bytes	256 bytes
OTP memory	No	32 bytes (256 byte pages write protect)	32 bytes (256 byte pages write protect)
Voltage	5V	5V	5V
Max clock speed	5MHz (Internal)	7.5MHz (Ext)	7.5MHz (Ext)
Max current	15mA	10mA (5MHz)	10mA (5MHz)
Sleep mode	No	Yes (100uA) (10uA no clock)	Yes (100uA) (10uA no clock)
Special functions	Coprocessor (modular arithmetic)	None	None
Die size	N/A	N/A	3.6mm x 5.1mm
I/O ports	2	1	1
Availability	Q1 1994	On request	Now

Siemens	Siemens	Texas Instruments	Texas Instruments
SLE44C80	SLE44C200	TMS373C005	TMS373C007
Sieco	Sieco	TMS370	TMS370
8 bits	8 bits	8 bits	8 bits
16Kbytes	10K bytes	4K bytes	4K bytes
2.5K bytes	8K bytes	256 bytes	-
Yes	Yes		
4 bytes	4 bytes		
-	-	-	8K bytes
10K (70^0C, 5V)	10K (70^0C, 5V)		
256 bytes	256 bytes main processor, 350 bytes crypto processor	256 bytes	256 bytes
32 bytes (256 byte pages write protect)	32 bytes (256 byte pages write protect)		
3-5V	5V	5V	5V
7.5MHz (Ext)	7.5MHz (Ext)	10MHz	10MHz
10mA (5MHz)	15mA (5MHz)		
Yes (100uA) (10uA no clock)	Yes (100uA) (10uA no clock)		
None	140 byte Crypto coprocessor		
N/A	3.65mm x 6.71 mm	N/A	N\A
1	1		
Q2 1994	Now		

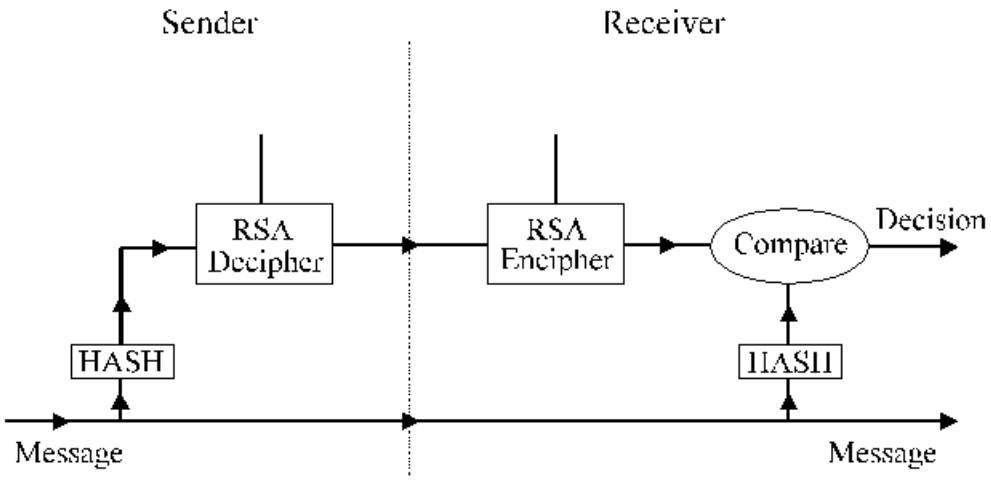


Fig. 1. A RSA Digital Signature

Smart Card Tutorial - Part 14

Cryptography and key management (continued)

Digital Signatures

The availability of public key cryptography algorithms has led to the adoption of a range of digital signature mechanisms. These signatures not only produce the properties of data integrity and source authentication but also effectively meet the requirements for non - repudiation. A digital signature may be generated by means of the RSA algorithm as shown in fig.1.

The message is reduced to a digest by means of an appropriate hashing algorithm. The resultant digest is calculated to be smaller than the block size of the RSA algorithm (typically 512 bits). This digest is then processed by the RSA algorithm as shown below using the secret key of the sender. The receiver takes the signature and applies the algorithm using the public key of the sender. The receiver also processes the message to calculate the message digest and compares the result. This form of signature is sometimes referred to as a signature with appendix because the message needs to be sent along with the signature. If the message is smaller than the block size of the algorithm then the hash function could be omitted to produce an impressed signature. In this case it would not be necessary to send the message since this data would be recovered by the RSA encipherment process. It should however be noted that there is a fundamental requirement for any signature process to incorporate adequate redundancy (say 128 bits). This means that a necessary amount of deterministic data must be included in the input to the signature creation process.

Signature generation

$S = M^d \text{ Mod } N$ (equivalent to the decipherment operation)

Signature checking

$M = S^e \text{ Mod } N$ (equivalent to the encipherment operation)

Where M = Message block (or digest)
S = Signature
e = Public key (of sender)
d = Secret key (of sender)
N = Modulus

The particular points to be noticed about the use of the RSA algorithm are that the block size is set by the choice of modulus (product of two primes) and that the encipherment key may be chosen to be very small (often e = 3). The modulus N is common to both the signature generation and checking process and the size of the secret key d will be the same size as N. It is now readily apparent that the signature creation process is much slower than the signature check operation being the ratio of 576 : 2 modular multiplications on average.

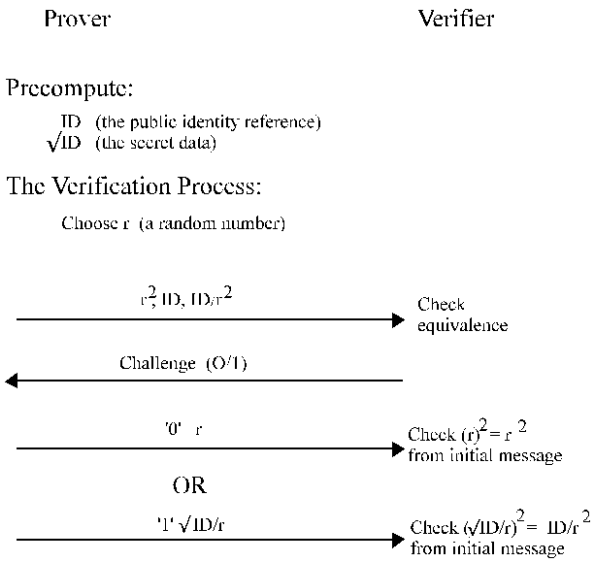
There are two obvious vulnerabilities with digital signature algorithms that must be addressed in the design of a secure system. In the first instance it is clear that it is very easy to generate an apparently authentic copy of a digital signature since it has none of the properties necessary for forensic evidence that may be applied to a written signature. The second problem relates to the authenticity of the keys. Here we have shown a process where the sender supplies both the keys for signature generation and checking. It is clearly essential to use some additional process to be assured of the authenticity of the senders public key. We will look at this in more detail when we discuss key management. Without this proof of authenticity neither of the properties of source authentication or non - repudiation can be substantiated.

The digital signature algorithm (DSA)

This relatively new algorithm was first proposed by NIST (U.S. National Institute of Standards and Technology) in 1991. It is different from RSA in that it is designed only for the creation and generation of digital signatures and not for the encipherment and decipherment of data as may be achieved by the RSA algorithm. The DSA algorithm is defined as follows:

Global constants

p = a 512 bit prime number
q = a 160 bit divisor of p - 1
g is chosen such that $g^q = 1 \text{ mod } p$



$$(g = a^{p-1/q} \bmod p)$$

where $0 < a < p$

For each entity

Choose a secret key x $0 < x < q$

Compute a public key $y = g^x \bmod p$

Signature generation

apply a secure hash function to the message to calculate H.

Compute:

k = A random number $0 < k < q$

$r = (g^k \bmod p) \bmod q$

$s = (K^{-1} (H + x r)) \bmod q$

Signature verification

Compute:

$t = s^{-1} \bmod q$

Check:

$r = ((g^{Ht} y^{rt}) \bmod p) \bmod q$

One cannot resist wondering which is the better signature algorithm? Before we can show some comparisons it is appropriate to look just a little further at an identity verification algorithm invented by Fiat and Shamir.

The Fiat - Shamir Identity Algorithm

This algorithm represents a class of zero knowledge proofs where it is possible to show that you know a secret without actually revealing the secret. The trick to this method relies on the difficulty of computing a square root mod m without knowledge of the constituent primes. A reference number ID is chosen by the central key authority as a quadratic residue so that it can calculate √ID mod m as a pre computation. This ID represents the secret.

The algorithm uses a global modulus m which is the product of two primes (known to the central key authority) as was shown for the RSA algorithm. The process takes place as shown below where all computations are assumed to be mod m.

It is readily apparent that if the prover supplies both responses for a particular r then the secret would be revealed since,

$$r. \sqrt{ID}/r = \sqrt{ID}$$

Just one invocation of the challenge process is

not sufficient since the prover may be lucky to get away with just proving the square root of the random number r^2. However if the process is repeated twenty times then the probability of a masquerade is 2^{-20} or about one in a million.

This identity algorithm has been extended by Fiat and Shamir to act as a digital signature algorithm. The challenge is based on the message to be signed and vectors are used for ID and $\sqrt{}$ ID to develop a sufficient signature size.

It is now possible to make some comparison between the different signature algorithms in terms of the size of the data elements and the number of modular multiplications as shown in the table. These are of course the important parameters when operating with Smart Card microcontrollers.

	RSA	Fiat - Shamir	DSA
Public key size (bytes)	64	576[1]	212[2]
Secret key size (bytes)	64	576	20
Signature generation: No of squares	511	8	159
Signature generation: No of multiplications	255	36	79
Signature checking: No of squares	1[3]	8	159
Signature checking: No of multiplications	1	36	119
Signature size (bytes)	64	521[4]	40

Notes:

1) Can be reduced by using an algorithm for computing from a public ID
2) Includes the common data p, q and g
3) This assumes an encipherment key e = 3
4) $\sum y_i = 512$; $\sum e_{ij} = 9$ (Fiat Shamir typical signature parameters)

David Everett

Next month. Part 15 - to be continued.

Smart Card Diary

1993 Plastic Cards Conference, Karos Indaba Hotel, Johannesburg, S Africa, 8/9 November.

A chance to hear about Smart Card developments in South Africa where, for example, the banks have agreed a common standard for financial applications. Contact: Babette van Gessel, AIC Conferences - Tel: +27 11 803 9680.

European Payments '93 (EFTPoS & Home Services), Sheraton Hotel, Edinburgh, Scotland, 16-18 November.

Contact: Paula Biagioni, Conference Secretariat - Tel: +44 (0)41 553 1930.

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

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

Smart Card '94 Conference and Exhibition, Wembley Conference Centre, London, 15-17 February, 1994, with a Smart Card tutorial on 14 February.

Conference Secretariat - +44 (0)733 394304.

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

☐ UK £375

☐ International £395

☐ Please invoice my Company

☐ Cheque enclosed

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

Name_____

Position_____

Company_____

Address_____

_____

Tel._____

Fax._____

Name_____

Address_____

_____

Card
No._____

Expiry
date_____

Signature_____
_____

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

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

Smart Cards for Korean Bank

The Kwangju Bank has become the first Korean bank to order Smart Cards with an order for 25,000 cards from Bull CP8, France. Half of the card order is for VISA Silver and Gold cards.

The order is a result of Bull CP8 representing Smart Card technology in the French pavilion at the international exhibition in Taejon, some 250 kilometres south of Seoul.

McCorquodale Appointment

Bill Waller, former General Manger of Cashcard Systems, leisure industry Smart Card specialists, has joined McCorquodale Card Technology to strengthen their Smart Card team.

McCorquodale say they are increasing their investment in their Smart Card activity in both equipment and people. Already providing cards for the retail, parking and access control markets, they are planning to expand their product offering to include pay-TV, telephones, transportation and leisure products. McCorquodale is part of the Bowater Group of Companies.

ACA To Be Formed

An Advanced Card Association is to be set up in the UK to act as a trade association for the industry, it was decided at a meeting of interested parties in London last month.

Association membership will represent all sections of the card industry including semiconductor and card manufacturers, system developers, and possibly others like consultants. A committee was elected to formally set up the Association to be launched by mid-December.

Contact: Simon Reed or Chris Stanford, c/o Charta Associates, England - Tel: +44 (0)442 231844.

Brewers Trial Cashcards

The cards pictured above are being used in trials by two major brewers, Allied Lyons and Scottish & Newcastle, to test cashless payment in selected managed houses.

Allied Lyons subsidiary, Taylor Walker, is using the cards in two of its Mr Q's specialist pool pubs in London. Scottish & Newcastle are using them in three pubs in North East England.

The cards, from Schlumberger, France, can be purchased at the bar and loaded with the customer's choice of value. They can then be used to operate games and non-payout amusement machines, or to buy food and drink on the premises.

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