

www.dionedirect.com

Dione

Dione has launched its own e-commerce web site this month, which provides a convenient way for its customers to support their payment terminal estates. The site provides a range of accessories, consumables and maintenance items that can be ordered for next day delivery. From this site you can buy accessories such as PIN pad cradles, terminal wet covers and holsters, plus consumables like printer paper rolls and batteries. The website itself is very easy to use and the navigational bar, positioned at the top of the page, breaks the rest of the site down into easily accessible areas. The website also provides information about Diones latest news and investor information. The site employs a pastel blue colour on a simple white background.

- Navigation
- Content
- Appearance



www.thales-ecurity.com

Thales e-Security

The first thing you notice about the Thales website is that it uses a lot of flash, but does not distract or effect the downloading of information. The site hosts a range security, banking and financial transaction processing equipment, with PDF's about their products. The website also features very useful white papers on cryptography, banking and network security. The front page contains only a navigation bar and a news window providing the latest news about Thales. The website uses very simple side navigation allowing you to access any relevant information quickly. The design is kept very simple and the content is mainly text based. Overall the site is easy to use and the information provided is kept short but relevant.

- Navigation
- Content
- Appearance



www.ingenico.com

Ingenico

The front page of Ingenico's website is a lot more busy than the other two reviewed in this issue. The site shows their latest news and has framed boxes showing the company's products, solutions and services. The site employs both text and pictures which combined give both a pleasant look to the site while portraying all relevant information about the company and its products. The site offers downloadable datasheets on all Ingenico's offerings. The site uses both French and English and has a very simple to use side navigational bar making it easy to get around. The site also has a live link to the company's share price. The pages of the site also come in printable formats, overall it has a lot of informative content and the navigation is quick and simple.

- Navigation
- Content
- Appearance



72Kbyte Chip Meets Common Criteria

Royal Philips Electronics 72Kbyte EEPROM contactless memory chip has been certified to Common Criteria EAL5+, which according to Philips is a world first for a triple interface Smart Card controller. The chip has been designed for contactless e-government applications and to meet the new security requirements being imposed by such governments as the USA, Australia, Germany and the UK for new passports.

According to Philips the 72Kbyte EEPROM memory, high security chip exceeds the specifications for smart passports set by the International Civil Aviation Organisation (ICAO) and is currently being used by Sdu Identification who specialise in the development, production and logistical management of high quality identity and financial documents such as passports, identity documents, driving licenses, memory chip cards and Smart Cards.

The SmartMX 72Kbyte EEPROM triple interface controller is the first to have contact, (ISO/IEC 7816 and USB) and contactless interfaces (ISO/IEC 14443 A) certified for use in a wide range of applications. The chips are already in volume production and offers a USB 2.0 LS interface to drive end-user acceptance enabling easy to use digital signature functions and secure physical network access. The chip can be integrated into Smart Cards or other form factors such as dongles, which can be directly connected to a PC's USB interface. The P5CT072 chip provides an additional 1Kbyte EEPROM for each implemented 8Kbyte as a standard industry practice. This ensures that the specified size of EEPROM is available for use by applications, unimpeded by the operating system, which normally requires a memory overhead. Therefore the 72Kbyte product assures at least 64Kbyte EEPROM of fully usable application memory.

Philips' SmartMX Smart Card controller family, including the 72Kbyte EEPROM triple interface Smart Card IC, uses a unique handshaking technology, which allows a significant reduction in power consumption. Philips has further increased the reliability of their technology, extending data retention time from the industry standard of 10 years to 20, and increasing the number of write cycles to 500,000. The SmartMX family also offers linear memory addressing, a dedicated instruction set and security sensors.

Common Criteria is the methodology used for evaluation of security properties of IT products and systems. The Target of Evaluation (TOE) is against defined criteria (Protection Profile) and certification is the final approval done by the Certification Body. SCN was unable to get the TOE from Philips but was pointed to www.bsi.de or www.commoncriteriaportal.org.

T-Systems in Germany did the hardware evaluation and the composite evaluation was done in France, Germany and Austria and SCN was told to note that these evaluations are application specific. Philips also point out that their solution is also suitable for implementation in bank cards for use in financial transactions. SCN was unable to find out which if any banks were interested.

Smart Card News is published monthly by Smart Card News Ltd Columbia House, Columbia Drive, Worthing, BN13 3HD England
Telephone : + 44 (0) 1903 691 779 • Fax : + 44 (0) 1903 692 616 • General Enquiries : info@smartcard.co.uk ISSN 0967 196X

Managing Director Patsy Everett ~ patsy.everett@smartcard.co.uk • Production and News Editor Jason Smith ~ jason.smith@smartcard.co.uk
Technical Advisor Dr David B Everett ~ david.everett@smartcard.co.uk • Sales Administrator Maxine Laker ~ maxine.laker@smartcard.co.uk

This Issue's Guest Contributors: • Randy Vanderhoof • Malcolm Fowler • Peter Thomlinson • Stephen Neff

Russian Agent : Alex Grizov Recon Company "Sport Hotel" 5th Floor Leninsky Prosp., 90/2 Moscow 117415 Russia

Editorial Consultants Dr Kenneth Ayer • Peter Hawkes • Simon Reed • Robin Townend

Printed by DAP (Sussex) Ltd. Telephone : +44 (0) 1273 430430

Please Note

From time to time, *Smart Card News* may include industry forecasts and forward looking statements made by the companies concerned. Readers should be advised that Smart Card News Ltd cannot be held responsible for decisions and/or actions taken by readers of our newsletter, based on the information provided including any errors therein, nor are we responsible for the opinions of the individual authors.

Don't Forget!

Our Website containing daily News On-Line, and information about the full range of SCN services, can be found at the following address: www.smartcardgroup.com

Certain images featured in this issue obtained from IMSI's MasterPhotos™ Collection 1895 Francisco Blvd. East, San Rafael, CA 94901-5506, USA





Smart Card Consortium

European Commission has named Gemplus International S.A. as leader of the largest consortium ever gathered for a cooperative research project in the Smart Card domain. Called "InspireD", the project will develop the new generation of Smart Card technology for Trusted Personal Devices (TPD). The EC has also granted funding for InspireD for a 3-year period.

The InspireD consortium comprises 16 of the leading industrial and academic stakeholders from the European Smart Card arena. This is so far the only European Commission project exclusively dedicated to Smart Cards. It will create a new standard for open platforms for the entire Smart Card and security industry. All aspects of Smart Card technology will be studied, including the silicon component platform, the cryptography and security authentication protocols for data protection, operating systems, and the software application layers.

Growth for UK Access Control

In the Access Control Market Report 2004, Research and Markets has reported that growth in the access control market was slow in 2002 and 2003. The value of the market at end-user prices was in the region of £226 million for 2002, rising to £232 million in 2003. Demand for access control has been strong in the public sector, from schools and universities, local and national government buildings and hospitals. Private Finance Initiative (PFI) contracts have changed the nature of this market sector.

This study estimates the market to show annual growth running at between 3% and 4% from 2004 to 2008, in terms of constant 2003 prices. Prospects for output of new building work in 2004 and 2005 are not favourable in the important commercial and industrial sectors, although growth is expected for public sector non-housing projects.

Massive Smart Card Rollout in SA

South Africa is set to rollout 50-million Smart Cards in 2004 and 2005. The aim is to have 100-million Smart Cards in active use in South Africa by 2009. These are the key findings contained in the Smart Card Trends and Deployment in SA 2004 report, released by World Wide Worx and Razor's Edge Business Intelligence.

Lipman Acquires Dione

Lipman Electronic Engineering Ltd has purchased 100% of the share capital of Dione from its shareholders, Tamares Capital Foundation, GE Equity and others. Under the terms of the agreement, Lipman paid \$69 million in cash for all of the outstanding shares of Dione.

EMV Definitions for Chip Migration

EMVCo, the EMV standards organisation, has released a set of common data definitions and processes, which standardises the data interface between EMV cards and issuers, resulting in simplified host processing and lower chip migration costs. The EMV Common Core Definitions (CCD) have been incorporated into the recently released EMV Version 4.1. CCD defines a common data element content and format for sending chip information between an EMV card and the issuer via the acquirer. When CCD is incorporated into a card specification, issuers of multiple branded cards can achieve benefits of a common issuer support system.

Chip and PIN Rollout Gathers Pace

The chip and PIN programme has released the latest figures on the rollout of chip and PIN cards and tills. By the end of September, 28.4 million cardholders - or two-thirds - had at least one new chip and PIN debit or credit card in their wallets. In total, 56.8 million chip and PIN cards have been issued by UK banks and building societies.

At the same time, more than 438,000 tills have switched over to chip and PIN. More key retailers including Comet, BP and Marks & Spencer have now joined Asda, Dixons, Wilkinsons, Tesco, Homebase, and PC World to have begun or completed their rollout programmes.

UK Get First Digital Tachographs

The UK is likely to be the first EU nation to implement digital tachograph equipment for commercial vehicles. Orga, which already offers highly secure Smart Card technology for the new digital tachograph system, is to supply some two million cards to the UK's Vehicle and Operator Services Agency (VOSA) in advance of the EU compulsory fitment directive for new and not-yet-in-service vehicles, which comes into effect on 5th August, 2005.





National Card for Bank of Azerbaijan

Thales's Host Security Module (HSM) has been selected by TietoEnator for use within the national Card Processing Centre of Azerbaijan. The Card Processing Center is the primary nation-wide payment card data processing service provider to commercial banks in the Republic of Azerbaijan.

ActivCard Finishes with Deloitte

Deloitte & Touche LLP (Deloitte), ActivCards independent registered accounting firm, has resigned, effective September 2, 2004. ActivCard's audit committee has begun the process of identifying and selecting a new independent registered accounting firm to audit the Company's financial statements for the fiscal year ending December 31, 2004.

Smart Cards for Windows

Alacris Inc. and Gemplus International S.A have partnered to offer a new turnkey Smart Card and certificate management solution for enterprise Windows environments. The technology partnership integrates Gemplus's GemSAFE Smart Cards with idNexus for Microsoft, Alacris' flagship product that provides integrated management of digital certificate and Smart Card technologies. The combined product offerings provide a Smart Card solution that not only brings additional security and convenience to the Windows networking environment, but also reduces the life-cycle management costs of supporting integrated Smart Card and public key infrastructure (PKI) deployments.

Orga Scores for Man U in Malaysia

Manchester United Football Club is now offering its loyal fans in Malaysia an exclusive membership program offering many exceptional benefits. The ceremony to launch the PB Manchester United MasterCard was held at Head Office, Menara Public Bank (PB) in Malaysia. ORGA Singapore, a subsidiary of Germany's ORGA Kartensysteme GmbH, is supplying the Smart Cards. Public Bank and Barclaycard developed the card program together with the financial unit of Manchester United, MU Finance, to bring fans closer to the club. Card members can look forward to exclusive privileges, such as "One United" membership, participation in the MU Points Rewards Scheme and entry into a unique points-based contest.

ORGA is supplying credit cards with a chip from the Multos 4.06 series to Public Bank, which is introducing this first ever card - the PB Manchester United MasterCard - in the Asia/pacific region in collaboration with Barclaycard International.

Free Travel Scheme in Ireland

The British and Irish Governments are considering a proposal to use Smart Cards to allow free access to public transport for senior citizens and other eligible social welfare groups across the border of the two countries. Currently in both Northern and the Republic of Ireland these groups can travel across the border for free but cannot travel within the jurisdictions. This new plan would allow senior citizens with a Senior Smart Pass to travel at no cost over the border and anywhere within Northern Ireland and the Republic of Ireland. The All-Ireland Free Travel Scheme is planned to commence within 2005.

QUICPay goes Mobile in Trial

JCB Co., Ltd will start a QUICPay contactless payment system trial project in November. The current trial will implement the system in mobile phones compatible with NTT DoCoMo's mobile wallet service. Twenty employees of the Kanachu Hire taxi company, based in Atsugi, in the suburbs of Tokyo, will receive NTT DoCoMo mobile wallet service handsets to download the QUICPay application, while about 30 of the company's cabs will be equipped with contactless readers.

Second Quarter Sales up for Oberthur

Oberthur Card Systems sales for the second quarter 2004 amounted to 108 million euros showing an 11% increase on a year-on-year basis. The sequential growth during the first three months of the year reflects mainly the sales recovery in Mobile Communications (+30.7 %) and Identity & Security (+31.8%) segments.

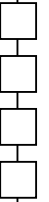
For more information visit ...



Research and Markets
www.researchandmarkets.com

Chip and PIN
www.chip-and-pin.info

Manchester United Football Club
www.manutd.com





Payment microprocessor cards deliveries have reached the level expected by the company. Sales as of the end of June 2004 have reached 210.8 million euros, a 7.3% increase compared with the previous year.

Problems with Visa/Dankort Abroad

Payment Business Services (PBS) have received a number of reports from cardholders who are experiencing problems paying for goods with the new Visa/Dankort Smart Card. So far the reports concern a few high street and airport shops in England, plus a number of websites. PBS have stated that the long 'lifetime' of the new Visa/Dankort cards may be the reason why people are experiencing difficulties in some high street shops (primarily in England) and certain Internet shops.

SBM Partner with Aconite

Saudi Business Machines (SBM), the General Marketing and Services Representative for IBM World Trade Corporation, has signed a strategic alliance with international Smart Card solutions provider, Aconite, to drive the adoption of Smart Card technology in Saudi Arabia. The agreement with the Jeddah-based SBM will see Aconite's suite of products being sold and supported throughout the Kingdom's burgeoning Smart Card sector. The launch of Smart Cards is expected in 2005, following EMV Saudi Arabia requirements issued by the Saudi Arabian Monetary Authority (SAMA) and the subsequent implementation of the necessary infrastructure.

Axalto Combats Road Safety

Axalto has announced it has been selected by the Dutch Ministry of Transport, Public Works and Water management, and Luxembourg Ministry of Transport to integrate its Smart Card technology into digital tachograph cards that will be available shortly to road transport professionals. This highly secure technological solution will not only combat road safety violations but also enable efficient fleet management by European hauling companies.

RFID to Track Medical Waste

Medical waste is an increasing issue. The U.S. sends some 2 million tons of medical waste to incinerators and landfills each year. And Japan's Environment Ministry estimated last year that more than 11 million cubic meters of industrial waste had been

illegally dumped around the country. Medical waste represents only a tiny fraction of that sum, but it is of particular concern because of potential health problems. To tackle this problem Kureha Environmental Engineering Co. Ltd., a waste management company, and IBM have teamed up to track medical waste as it leaves hospitals. Testing will begin on radio frequency identification (RFID) tags to ensure that medical waste reaches its proper disposal point. IBM Japan's RFID Solution Center in Yamato, Japan, will collaborate in the test.

During the trials the cardboard or plastic containers that hold the waste will be outfitted with RFID tags. Intensive testing at the Yamato facility will examine how well these tags transmit information in a variety of situations. After those trials are completed, testing will move on to Kureha Environmental Engineering's waste processing site. Once the effectiveness of RFID tagging is confirmed, the company plans to equip Kureha General Hospital, in Fukushima, Japan, with the RFID technology to track its discarded medical waste. This is the first study in Asia Pacific of tracking medical waste and represents a new application for RFID.

Memory Card goes Contactless

Matsushita Electric Industrial Co Ltd., best known for its Panasonic brand products, has developed the industry's first SD Memory Card with contactless Smart Card capabilities. Called smartSD Card, the new SD Memory Card combines the convenience of contactless data communication capabilities with large storage capacity and high security.

The company will position the smartSD Card as key to realising the "ubiquitous network society" and will strive to create new business opportunities not only in the device sector but also in the system and solution service sectors.

Honeywell and LEGIC Team

LEGIC Identsystems Ltd has signed a global licensing agreement with Honeywell. The partnership will allow Honeywell Building Solutions to incorporate access control application solutions from LEGIC, a supplier of contactless Smart Card technology, into its portfolio of Smart Cards and readers. This will give Honeywell customers a broader range of solutions for their building security applications.





Plymouth Rolls out Smart Cards

Plymouth City Bus is going 'smart' - replacing their existing Wayfarer 3 system with the company's latest Smart-enabled TGX150 revenue collection technology. Wayfarer is working with the operator on an installation programme involving the introduction of new ticketing technology as well as a Radio LAN facility. The result will be a system that will interface with both the existing back office and Plymouth City Council's new ITSO Smart Card operation, so helping to facilitate the roll-out of the "PLYM" Smart Card across the city.

Biometric System for US DoD

Lockheed Martin has been awarded a five-year contract by the US Department of Defense to configure, build and maintain a new Automated Biometric Identification System (ABIS) that will consolidate, store, and search fingerprint data collected worldwide by the department.

This new system will be patterned after the successful Integrated Automated Fingerprint Identification System (IAFIS), which Lockheed Martin developed and now maintains for the Federal Bureau of Investigation at its Criminal Justice Information Services Division in Clarksburg, W.Va.

Biometric Trials for PACOM

Space and Naval Warfare Systems Activity Pacific has chosen Bioscrypt's V-Smart iClass biometric access control reader to augment physical access control at Pacific Command Headquarters (PACOM), and to analyze the benefits of implementing biometric contactless technologies for future generations of the Common Access Card (CAC) at Navy Region Hawaii and other Naval installations throughout the Pacific region.

Datastrip Selected Fujitsu

Datastrip Corporation has selected the Fujitsu MBF200 single-touch fingerprint sensor for use in its portable biometric Smart Card reader, the DSVII-SC. The Datastrip DSVII-SC verifies identities by reading contact and contactless chips on ID cards, passports, driver's licenses and other personal documents.

ThinkPad goes Biometric

IBM has announced that their new ThinkPad notebook line will use biometrics to increase the security on their laptop range. The new ThinkPad will have an embedded fingerprint scanner, which will replace passwords for user sign-on access to the laptop. The ThinkPad's new reader will be on a wrist rest below the arrow keys on select models of the T42. To log on to systems, software applications, databases or Web sites, users must swipe a finger across a small, horizontally oriented sensor.

ACG Wins Public Tender

ACG Identification GmbH has recently won a public tender from Bundesversicherungsanstalt für Angestellte (BfA), Germany's national provider of social security services. ACG will deliver 30,000 OMNIKEY CardMan 3121 USB Smart Card readers to various BfA subsidiaries by the end of October 2004. BfA will use the OMNIKEY CardMan 3121 readers along with hybrid cards for PC access control and electronic signature applications.

Security without a Smart Card

NDS has announced a secure content protection solution for two-way IP TV network operators. VGS, part of NDS's IP content security solution, Synamedia, is aimed at telecom and broadband operators. Built on NDS's hardware based conditional access, VideoGuard, VGS offers two-way connected networks a secure solution for the delivery of video content without the need for a Smart Card. NDS has worked closely with major chipset manufacturers to develop secure processors that can communicate with secure servers based at the network headend that provide strong content protection.

For more information visit ...



Matsushita Electric Industrial Co
www.panasonic.co.jp/maco/en/

LEGIC Identsystems Ltd
www.legic.com

Lockheed Martin
www.lockheedmartin.com

IBM
www.ibm.com

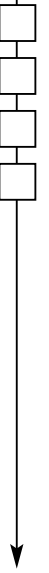
ACG Identification
www.acg.de





Treviso Launches Fares that go down as you Travel!

ascom



Treviso's new stored-value card is original - and may even be one of a kind. It encourages use of public transport by offering fares which go down depending on how many times the card is validated, calculated according to how often it is actually used over a given period. "Use public transport more often and pay less." That's the logic behind the stored-value card that will soon be in use on the 100 urban buses of Treviso.

The fortified city, located 30 km north of Venice, is proud of its many attractions. Each time the Smart Card is validated, the number of times it has been used since purchase is calculated. Beyond a certain level, the fare per bus-ride goes down. It may seem simple, but the system is as complex as it is innovative. And it's complex in several ways. To begin with, it took local councillors over a year to come up with their dream bus ticket. As well as a traditional magnetic system, with single tickets, season tickets and three fare zones, there was a contactless ticketing system, providing a dual solution. The idea of a stored-value card came up at the last moment, after months of new versions and lengthy discussions with the Ascom team. "Supporting our clients from start to finish is all part of our job", says Eliane Dejoux, the Ascom project manager who led the project and who makes no secret of how pleased she is that it has come to fruition.

The local government in Treviso wanted to give the project every chance of success by keeping control of changes in the way the system functions, and deciding how to calculate the value of each card. Only full-scale experience will prove whether a fare system which encourages passengers to use the service will actually be effective. Does it make more sense to count the number of journeys over a given period, or the total amount of money deducted from the card? Should the system take account of use of the card over consecutive days? And what are the right thresholds for each one of these different hypotheses?



Each detail was studied and discussed, each detail carefully weighed and sometimes reversed. Local councillors held long and intense meetings on every aspect of the card, including its design. Appearance is clearly an important factor in Treviso. Launched in Autumn 2004, the Treviso experience will be closely watched by public transport professionals and, of course, the politicians faced with the need to reduce urban car traffic across most of the world. But the importance of the Treviso experience is relative, as Elian Dejoux explains: "Treviso has only one urban transport operator. The project would have been totally different if we had had to develop a fare-for-use system in a multi-operator environment!" Another ambitious city may well persuade Ascom to take on that challenge somewhere else in the world. Or perhaps, somewhere else in Italy, where the company installed 85% of recent "dual" or contactless solutions.

In another announcement Ascom's Division of Transport Revenue reported they had won a major order in Norway from the Norwegian State Railway. The order is for a comprehensive, networked fare collection and access control system based on advanced electronic ticketing technologies. The project volume amounts to about \$16 million. Ascom saw off some established international competitors in its bid for this project. The fare collection solution uses a contactless smart card for data storage and customers can plan and book their journey via the internet. The system includes 159 stations, where 162 automatic ticket machines have been installed, 40 service terminals and 345 validators. Ascom have been involved in the Paris public transport system RATP, the French Railways SNCF, the Milan public transport system, the Swiss Federal Railways and the Montreal Metropolitan area public transport authorities in Canada.

Spotlight



Using Contactless Technology in Secure Identification Systems



By Randy Vanderhoof, Executive Director, Smart Card Alliance



Randy Vanderhoof

Organisations are increasingly concerned with the problem of how to verify a person's identity and privileges before granting that person physical access to a building or place or logical access to information or other online resources. Solving this problem is driving both businesses and governments to implement new secure identification systems that provide increased access control security. These new systems are making fundamental changes in access control policies, processes and technologies -- within an organization, among organisations that collaborate as partners, between customers and businesses, and between citizens and governments.

Smart Card technology is increasingly accepted as the ideal platform for secure ID systems, not only because of the increased security it provides, but also because of the advantages it delivers for ease of use and multi-purpose functionality. The maturing of contactless Smart Card technology has also driven its use in a wide variety of applications requiring fast, secure access - from payment to building access to passports. This article will first look at the requirements for establishing a secure identification system and then review the trend to use contactless Smart Card technology in secure ID systems.

Secure ID System Requirements: A secure ID system is designed to address one primary requirement: verify that an individual is who the individual claims to be. When properly designed, secure ID systems implement a chain of trust, assuring everyone involved that the individual presenting an ID card or token is the person who owns the credentials on the ID and that the credentials are valid. A secure ID system can provide individuals with trusted credentials that are used for a wide range of applications, from enabling access to facilities or networks to proving entitlement for services to conducting online transactions. Critical to any secure ID system is the physical ID device. This device can take many form factors, including a plastic card, Universal Serial Bus device, or a chip-based passport. The ID device is used as a portable, trusted and verifiable representation of an individual's identity and rights and privileges within the ID system. For an ID to meet these requirements, the ID system must assure that a legitimate authority issued the ID, that the ID and the credential it carries are not counterfeit or altered, and that the person carrying the ID matches the individual who enrolled in the ID system. The figure to the right summarizes the key links in a secure ID system chain of trust during the identity authentication process when the ID is used.

Smart Card Technology and Secure ID Systems: Smart Card technology significantly strengthens security in a secure ID system, protecting both the electronic credential used to authenticate an individual and the physical device. Since the credential is permanently stored on the card, it is never available for an unauthorized user to steal. Smart Cards build protection into the physical device by supporting tamper-resistant features and active security techniques for encrypting communications and supporting mutual authentication between the card and reader. With the ability to store, protect and modify information written to the on-card electronic device (i.e., chip), Smart Cards offer unmatched flexibility and options for information sharing and transfer, while providing the unique ability to incorporate privacy-sensitive features.

Contactless Smart Card technologies offer security professionals features that can enhance systems designed to control physical or logical access. Contactless cards differ from traditional contact Smart Cards by not requiring physical connectivity to the reader. The card is simply presented in close enough proximity to the reader and uses radio frequencies (RF) to exchange information. The use of contactless Smart Card technology is particularly attractive for secure physical access, where the ID credential and reader must work in harsh operating conditions, with a high volume of use or with a high degree of user convenience.





While there are several international standards for contactless Smart Cards, ISO/IEC 14443 is the most widely used and is the contactless standard included in the United States government's Government Smart Card Interoperability Specification (GSC-IS) and in the International Civil Aviation Organization (ICAO) specification for Machine Readable Travel Documents (MRTD).

Smart cCards supporting both contact and contactless identification (e.g., for logical and physical access) are often described as either hybrid or dual-interface chip Smart Cards. A hybrid card contains two chips, one supporting a contact interface and one supporting a contactless interface. The chips are generally not connected. A dual-interface chip card contains a single chip that supports both contact and contactless interfaces. Dual-interface cards provide both contact and contactless functionality with a single chip in a single card, with current designs allowing the same information to be accessed using either contact or contactless readers. Today, smart chip manufacturers are beginning to deliver dual-interface chips with the performance and processing capabilities required to support sophisticated logical access applications. Dual-interface cards are now available that have achieved FIPS140-2, Level 3 certification (as a finished card) or Common Criteria EAL 5+ (as an integrated circuit). These security levels are as high as are available from contact-only smart cards.

Smart Cards also provide an excellent solution for secure ID systems that are using biometrics as a factor for authenticating individuals. The Smart Card can securely store the cardholder's biometric data. When the card is presented to a biometric reader, the biometric information is retrieved from the card and compared to the actual cardholder biometric captured at the access point to validate the cardholder's identity. If the application uses one of the more powerful Smart Cards with an embedded microcontroller, the biometric data can be compared and matched on the card. A "match on card" assures the greatest degree of privacy. The biometric data never leaves the card, and the card can be destroyed when the cardholder no longer needs the identity credential.

Conclusion: Governments and businesses around the world are tackling the problem of securely proving the identity of individuals attempting to gain access to physical facilities or logical resources. Smart Card technology - both contact and contactless and in a variety of form factors - is a vital link in the chain of trust for a secure ID system. It is providing the foundation for implementations of new secure access control systems worldwide.

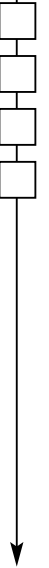
Making Life Difficult

By The Whistleblower



The news this month in the UK has been full of the IT modernization costs for the National Health Service (NHS). The program includes a patient care record scheme, a hospital booking scheme with patient choice, and new local IT infrastructures. Initially budgeted at £2.3bn in 2002 over three years the figures rose to £6.2bn over 10 years. Now we are told it could cost a minimum of £18.6bn and that officials at the Department of Health think it could even be as high as £31bn.

A spokesman for the 'National Program for IT' (NPfIT) told 'Computer Weekly' that it is generally accepted in the IT industry that implementation costs are some three to five times the cost of procurement currently standing at £6.2bn. On a quick calculation and assuming 1 million staff, that works out at £18,600 per person, is it just me or isn't that excessive? The basis of this procurement is the award to a number of large companies to develop a particular part of the project, in effect each with their own proprietary modules. Industry has long since learned that the proprietary solution to a problem not only costs more but often never appears.





Suppliers rise and fall as the development progresses. EDS earlier this year lost their contract for the secure email and directory service for the NHS to Cable and Wireless worth £164 million over 10 years. It was equally unfortunate to lose out to BT Group last year on the award of the NHS patient record system. The list is endless but the point at issue is about the best way to handle large projects funded by government. Take just the secure email, why can't the NHS use off the shelf components as would any commercial organization? Apparently they have been using 7000 different email services, but isn't the solution just a matter of specifying standards? Does anyone seriously suggest that there aren't adequate products in the market place to choose from?

So how does the Smart Card industry compare? In the mobile telecommunications industry we can see a big success story with the GSM SIM card which really launched the future of microprocessor smart cards from the early 90s. ETSI at the time specified the standards for the GSM service (using existing standards where relevant and appropriate) which were duly published and open to all vendors. Each of the Network Operators is free to choose its products from any vendors who can meet the specifications. Market forces prevail! The EMV (Eurocard, Mastercard, and Visa) Smart Card to replace the existing magnetic stripe is looking to be an equally successful project. Again the specifications have been openly published and banks and retailers alike are free to choose the supplier of their components subject to them meeting the specifications. This leads to competitive pricing for cards and terminals and although margins may be reduced at least it's open to any that are competent to play both small and large.

What about other Smart Card projects? Well in the US the DoD is well ahead in its published specifications for the Conditional Access Card (CAC), The International Civil Aviation Organisation (ICAO) is also plowing ahead with its specifications for ePassports, and while we might argue the approach which leads to large E2 memory chips at least the industry is able to respond in a competitive manner. ICAO is not paying for the development of 64 kbyte Contactless memory chips.

In the UK we have seen the National Smart Card Project (NSCP) looking for interoperability at the Local Government area and ITSO working on the interoperable transport scheme. The NSCP has not yet published its specifications but ITSO produced the latest version 2.1 in March 2004. ITSO used to stand for the Integrated Transport Standards Organisation but now has lost the meaning and retained the letters to allow it to move further a field than just transport. The Department for Transport (DfT) has actively promoted the scheme with financial incentives and there can be no doubt that the project is well known. ITSO's General Manager of 4 months, Paul Newman has just suddenly left, apparently to take up other consulting contracts, this must be a new way of describing 'pursuing other interests'

However well known this project is not being supported with the same enthusiasm by either service providers or major vendors - why? In the first instance the largest single Smart Card transport scheme, TfL (Transport for London) already has its own proprietary 'Oyster' scheme issued to more than 2 million customers (as at June 2004). The developers of the ITSO specifications had a problem, do you start with a green field or do you incorporate existing products? They chose the later, the Oyster and Calypso Contactless cards for example are included in the ITSO specifications. Whilst a pragmatic choice perhaps, you are faced with two problems (at least).

The overall architecture particularly the security management becomes overly complex to handle all the options and in addition the solution is not attractive to the existing players. If you are a regulator you can use a stick otherwise it has to be a juicy carrot and who will pay for this inducement? If the DfT feels unable to continue its sponsorship it might just all fizzle out because nobody else can apply the necessary influence. Simplification might be another way to solve the problem!





Off with the Old, on with the New



By Peter Tomlinson, Independent Consultant, Iosis Associates



Peter Tomlinson

The Office of the e-Envoy has become the e-Government Unit of the Cabinet Office - eGU. I couldn't help bringing to mind the Flanders and Swan song:

*I'm a Gnu, I'm a Gnu
The g-nicest work of g-nature in the zoo
I'm a Gnu, How do you do
You really ought to k-know w-bo's w-bo's
I'm a Gnu, Spelt G-N-U
I'm g-not a Camel or a Kangaroo
So let me introduce,
I'm g-neither man nor moose
Oh g-no g-no g-no I'm a Gnu!*



So here we are, with eGU rather than Gnu, run by the new man Ian Watmore. What a lot we expect of him (perhaps). Does another couplet from Flanders and Swan apply to him?

*A year ago last Thursday I was strolling in the zoo
when I met a man who thought he knew the lot.*

And it goes on:

*So I asked him: 'What's that creature there?'
He answered: 'Oh, H'it's a H'elk'
I might of gone on thinking that was true,
If the animal in question hadn't put that chap to shame
And remarked: 'I b'aint a H'elk. I'm a Gnu!'*

So what is eGU? Does it have a character of its own? eGU must be here to implement government policy in Information and Communications Technologies, which is to bring into the public sector best practice from all quarters, and to promulgate information assurance. Its all there in Cabinet Office papers on their web sites - the policy, but not the method. eGU needs the funding to bring in the best practice and promulgate it throughout the public sector, bringing relief to those stalwarts in public bodies who have boldly gone ahead alone; the industry must match that commitment with its best troops.

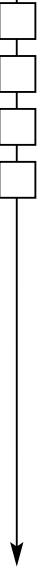
Flanders and Swan carried on to recall another encounter:

*Among the hunting trophies on the wall above my bed
Stuffed and mounted, was a face I thought I knew;
A Bison? No, it's not a Bison. An Okapi? Unlikely, Really. A Hartebeest?
When I thought I heard a voice: 'I'm a Gnu!'*

The opportunity for industry partners to participate in eGU deliberations is at the regular meetings of their Smart Card Working Group. That group currently considers function only. There are those of us from the industry who have consistently said that, in the use of secure tokens (often implemented as Smart Cards), security methods must from the beginning be considered together with functional methods. They are not separate animals - they are both parts of the same concept. Yet the previous Cabinet Office model of separate treatment of the two parts (in OeE and CSIA) continued unchanged at the summer meeting.

*Oh, g-no, g-no, g-no,
G-no g-no g-no I'm a Gnu
G-no g-no g-no I'm a Gnu*

It's very G-nice of you (to be here, I presume F&S meant).





When It Comes To Targeting Customers & Keeping Them Loyal, It's All About Relevance

By Malcolm Fowler, Vice President & General Manager, Ernex



Malcolm Fowler

Much analysis has gone into the debate about which type of loyalty instrument is most effective in helping businesses dynamically interact with customers in order to build and maintain more profitable relationships. The debate, focused on Smart Cards versus magnetic stripe cards, is irrelevant.

The type of card consumers carry in their wallet will not help an organization's loyalty program succeed - the reward relevance and the program delivery method will. Smart Card adoption has been high in Europe and Asia, driven by challenging credit card verification capabilities in a telecom infrastructure that is not as robust as that of North America. The Smart Card, which stores data directly on the card, has helped to reduce fraud at considerable cost savings for card issuers. In North America, the robust telecom infrastructure allows real-time verification of magnetic stripe cards for banking and loyalty reward programs without the need for additional infrastructure. Loyalty programs based on Smart Card technology attempt to offset higher card costs with reduced telecommunication costs by storing loyalty data on the card and enabling program rules at the point-of-sale (rather than at a centralized host). These speed and efficiency gains are offset by two factors: (a) the desire of many loyalty operators to analyze data in a central location, necessitating its periodic collection; and (b) the challenges in updating program rules at each point-of-sale when changes are required.

Most retailers in North America currently have the magnetic stripe technology and telecom infrastructure in place to cost-effectively enable host-based, real-time loyalty programs. This structure allows businesses to update program rules once, in a central location, without the extra effort of "touching" all their individual points-of-sale. Since more information can be stored in these types of real-time databases, organizations have the ability to take advantage of the added depth and richness of customer information. The popularity of customer loyalty programs is at an all-time high. According to an analyst report by industry research firm Gartner Inc., more than 60 million Americans belong to at least one of more than 200 U.S. based loyalty programs, making these programs so widespread that customers have increasingly come to expect them.

For organizations that are looking to loyalty programs as a way to recognise and retain their best customers, the benefits of real-time are clear. By pushing the rewards redemption processes to the front line in real-time, an organization can reduce or eliminate resources spent on call centers and fulfillment warehouses, while customers can avoid the long delivery times often associated with reward fulfillment. Real-time loyalty makes sense, especially since instant gratification strikes at the core of making a program relevant to a consumer, not to mention successful to the bottom-line.

But the benefits don't stop there. It is widely accepted that 20% of customers produce 80% of profits, and some industry analysts will even claim that more than 100% of profits are driven by the top customer segments. Think this isn't important to your business? Think again, as the bottom segments of a business' customers can actually contribute negatively to profits. Real-time loyalty programs can help an organization identify its best customers, reward them for their patronage, and weed out the rest. While many industry pundits closely followed the progress of retail giant Target and its foray into the Smart Card loyalty market, most failed to realize that it was not the Smart Card technology itself that failed. With a reported investment of \$50 million in infrastructure, Target was able to attract a purported 9 million customers to its loyalty-enabled card, proving that the interest and opportunity in loyalty benefits existed.





The problem was that consumers ignored the high-tech Smart Card loyalty features because the perks and benefits were not delivered in a relevant manner. Target's program required consumers to go to a special kiosk in order to access the loyalty coupons for redemption at the point-of-sale. In the end, the debate that focuses on Smart Cards versus magnetic stripe cards is irrelevant. Magnetic stripe cards, Smart Cards, finger print devices or retinal scans are simply the identifier for a host-based loyalty solution. There is good reason to believe that Smart Card technology may yet emerge as the technology of choice to reduce credit card fraud in North America.

However, an effective customer loyalty program is not about the type of customer interface, but rather the benefits associated with it. Businesses wanting to adopt their own rewards program should consider a solution that is real-time in nature, which allows customers to be rewarded and/or recognised right at the point-of-sale. Most importantly, businesses should specifically focus on the relevance of their rewards. Ultimately, acknowledging consumer preferences and delivering rewards in real-time for their patronage is what will make your loyalty program successful - not to mention smart.

On the Move

Paul Newman Resigns from ITSO

Paul Newman has asked to leave ITSO to take up a consultancy opportunity and that ITSO, with some regret as to timescales since this has arisen at short notice, has agreed to release Paul with immediate effect. Paul will be handing over to Mike Eastham, as Interim General Manager, with immediate effect.

Change at the Head of G&D

Chairman of the Board and CEO of Giesecke & Devrient, Willi Berchtold has left the company in a harmonious mutual agreement. Until Mr. Berchtold's successor has been appointed, board members Dr. Walter Schlebusch and Dr. Peter Zattler will manage the company on an acting basis.

Cubic Announces New CEO

Cubic Transportation Systems has named Dave Lapczynski as the new Chief Operating Officer, overseeing all program management, engineering, and manufacturing functions for the Company.

New Head of Unit for LEGIC

LEGIC Identysystems Ltd has appointed Robert M Fee as the new General Manager of its North American Business Unit. The continued growth of interest in the use of the LEGIC 13.56 MHz contactless Smart Card technology in North America has led to the decision to establish a dedicated new business unit to continue growing the brand in the US, with

a main office headquartered in Miami Lakes, Florida and a field sales office located in Naperville, Illinois, USA.

New President for Gemplus

Gemplus International S.A has appointment of Michel Canitrot as President of Gemplus, Latin America, reporting to Philippe Vallée, Executive Vice President. This appointment is part of Gemplus' strategy to maximize the geographical opportunities for Smart Card development and enhance its regional presence. Michel, 58, brings many years of experience in Sales and Marketing management.

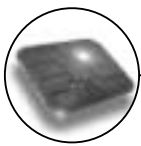
New Director of Quality at VCT

Versatile Card Technology Inc. (VCT) has promoted Joseph Cruz to Corporate Director of Quality & Statistics. Cruz, who has been with the company since 1999, has held several positions in the company and will now serve as a Corporate Director managing the VCT Qualteq Division in South Plainfield, New Jersey, USA.

STS Appoint Jon Cairns

Smart Technology Solutions (STS) have appointed Jon Cairns as business development director. With extensive experience in the software and electronic payments sector, Jon Cairns will be a key contributor to STS' continued development at a key phase in the company's growth.





The End of Cash as We Know it?

By Patsy Everett, Managing Director, Smart Card News Ltd



Patsy Everett

At a recent mobile industry round table hosted by the CEO of Valista Raomal Perera, leading lights in the industry discussed their thoughts on where they think the industry and the technology is going and whether this is what the consumer wants, particularly the youth market.



Jean Benoit van Bunnem of the Orange group thought that simplicity of use was the main requirement, and the service being offered should be perceived as a trusted brand with no complex registration processes, and a fully integrated payment system.

Susie Lonie, senior product manager at Vodafone agreed and used the analogy of purchasing shoes on a Saturday in the high street. The consumer is not interested in the payment mechanism the retailer is going to use, just the shoes. Consumers do not want an interesting experience with an interactive payment product, they want it to be quick, easy and secure. Mike Short VP at O2 said that their evidence showed that some consumers would prefer anonymity for certain types of content and that some devices presented barriers and this was an issue for handset manufacturers as well as carriers.

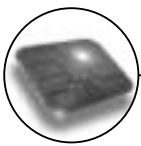


Andrew Bud of mBLOX made the very interesting observation that SMS was an old technology initially developed for service engineers and mobile personnel as a replacement for paging, and said "Consumers have picked up this technology, quite without permission because it was very cheap, absolutely ubiquitous and simple to use. Based on these rather unscientific, un-technical justifications they turned this into the biggest media channel that has ever existed".

"There is an intangible fun factor in SMS and you see people texting for no good reason other than it is a fun thing to do. That's why, I think, the use of SMS as a paying mechanism took everyone by surprise, a billing mechanism based on SMS which, in the UK was invented by Vodafone by accident, has turned into a paying mechanism which has completely disrupted the entire content value chain because it is fun, easy, ubiquitous, simple and familiar, it was physiologically appealing. That is a much stronger argument than any technological virtue." Bud said.

David Birch of Hyperion made the point that we would all love to pay for our parking ticket, for example, with our mobile phone but if you have to go to a website, login, punch in your password then send your message and then the phone rings you back with your PIN, it's just too complicated. He then went on to point out that Mondex offered a good secure anonymous payment system and that if operators had put that in the system in the first place then the current discussion would not be taking place.

It is now 7 years since the first ring-tone was launched and Musiwave are seeing a 15% growth month on month in music and video downloads. Gilles Babinet of Musiwave thinks one of the key reasons why mobile is so successful for voice is because it's easy not because it is technically viable. Oliver Steely of MasterCard pointed out that there is one main question asked by retailers and that is how many people can pay with this technology and the customer wants to know where they can spend using the technology.



Banks do not want to process the small payments but are keen to process the larger amounts such as those used to top-up a pre-pay phone card, so there is no competition between the banks and mobile industry when it comes to micro-payments.

Tim Jones, CEO at Simpay made the point that the mobile industry is not competing with credit cards but enabling, that there is a role for a payment scheme structured to support low value payments. Tim also can't wait for the mobile phone to look like a miniature PC as the PC industry has a good file format for music, still images and video.



Oliver Steely agreed "I think Tim's point about turning phones into the mini PC is absolutely crucial. And the reason I say that, from our perspective, it is more about the browsing and the Internet experience than about file formats and proprietary technology. In the card industry, we have a solution for securing remote credit card payments. It is an agreement that we came to between ourselves and VISA and American Express, and our UK banks are deploying it right now." he said

It works on the remote channel and I'm probably in the wrong room to say this guys but you know mobile is just one of five or six different remote channels that our bank customers are going to use, so let's build something that allows payments to happen across all of those remote channels simultaneously. Let's not try and build something that only works in one sub-setting because the losers will be the consumers and the merchants." mr Steely said.

At the end of the day consumers are happy with their credit cards, they have been around for 30 years or more and are part of a \$4trillion global industry, they may even one day be found in the mobile phone but not for micro-payments, the overheads are too high. As Susie Lonie pointed out if you lose your credit card it takes about 80 hours before you realise it, if you lose your phone it's about 8 minutes. There is obviously a place for both technologies and perhaps the mobile phone will see the end of cash as we know it.

Events Diary

November 2004

- 2 - 4 Cartes 2004 & IT Security 2004 - *Paris, France* - www.cartes.com - www.itsecurityexpo.com
- 15 - 17 Inside ID Conference & Expo 2004 - *Washington DC, USA* - www.jupiterevents.com
- 16 Smart Card Club - *London, UK* - www.smartex.com
- 17 Infosecurity Manchester - *Manchester, UK* - www.infosecroadshow.co.uk
- 17 - 19 ID World International Congress 2004 - *Barcelona, Spain* - www.idworldonline.com
- 18 - 19 EFMA Loyalty Conference Programme - *Prague* - www.efma.com/loyalty
- 22 - 24 Middle East Financial Technology Exhibition & Conference - *Bahrain* - www.meftec.com

December 2004

- 7 - 8 RFID for Contactless Payment Systems - *Atlanta, Georgia, USA* - www.iqpc.com/technologyiq
- 14 Smart Card Club - *London, UK* - www.smartex.com
- 9-10 The 9th eESC Open Conference - *Prague*

January 2005

- 26 - 27 Security Printing & Alternative Solutions in Russia - *Moscow, Russia*

February 2005

- 14 - 16 GSM World Congress - *Cannes, France* - <http://www.3gsmworldcongress.com>





Continued US Investment In Smart Cards

By Jason Smith, Production Editor, Smart Card News Ltd

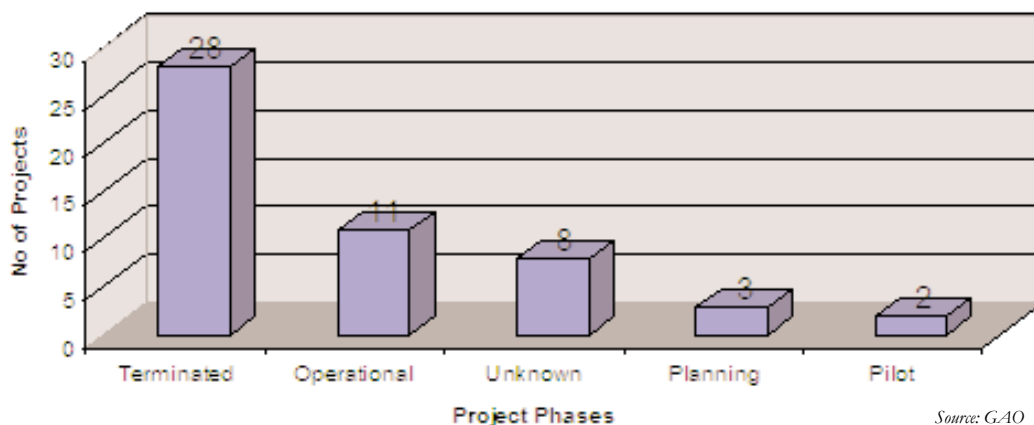


Jason Smith

Smart Card Technology is becoming a key factor in helping the federal government provide security for its many physical and information assets. Smart Cards offer the federal government a secure verification process for identifying employees and other personnel who need access to buildings and logical access to computer systems. They also offer to support other business-related functions in areas such as tracking immunisation records or storing cash value for electronic purchases.

Since the 1990s, the federal government has considered the use of Smart Card technology and in 1996, the General Services Administration (GSA) was tasked with taking the lead in facilitating a coordinated inter agency management approach for the adoption of multi-application Smart Cards across government. To make it easier for federal agencies to acquire commercial Smart Card products, the GSA developed the government wide Smart Card Access Common ID contract, which allows federal agencies, those covered by the Chief Financial Officers Act as well as the Department of Homeland Security (DHS), to procure Smart Card products and services. By using this contract, federal agencies can help reduce the cost of Smart Cards and ensure that vendors incorporate interoperability specifications, according to the director of GSA's Center for Smart Card Solutions.

In a report by the US Government Accountability Office (GAO) entitled "Federal Agencies Continue to Invest in Smart Card Technology" they documented the progress made by the federal government in promoting Smart Card technology. The survey involved 24 major federal agencies regarding the status of their Smart Card projects. The report was originally carried out in January 2003, and since that time 28 out of the 52 Smart Card projects that were reported as ongoing have since discontinued, as of June 2004, because they were absorbed into other Smart Card projects or were deemed no longer feasible. Of the remaining 24 projects, 16 are in planning, pilot, or operational phases and are intended to support a variety of uses (the agencies did not provide current information on the remaining 8).



Twelve of the 16 projects are large-scale projects intended to provide identity credentials to an entire agency's employees or other large groups of individuals. Examples include the Department of Defense's (DOD) Common Access Card (CAC), which is to be issued to an estimated 3.5 million DOD-related personnel, and the Transportation Security Administration's Transportation Worker Identification Credential, which is to be used by an estimated 6 million transportation industry workers. Based on this survey of federal agencies, 10 additional Smart Card projects have been initiated since their last review was completed.





Included are small-scale projects, involving cards issued to as few as 126 cardholders (such as a project in the Department of Labour's Employment and Training Administration), and large-scale agency wide initiatives, such as, the Department of Veterans Affairs (VA) Authentication and Authorization Infrastructure card, which is to be issued to an estimated 500,000 employees and contractors.

Four of these agencies reported purchases under the GSA's Smart Card Access Common ID contracting vehicle, and others likewise have plans to use this contract. Between December 2004 and December 2008, five agencies including NASA and the Departments of Defense, Homeland Security, the Interior, and Veterans Affairs-are planning to make an aggregated purchase of up to 40 million cards through the GSA contract. As part of this purchase, these agencies are scheduled to begin making quarterly procurements beginning in December 2004 of approximately 1.2 million cards. In response to the survey, the majority of the agencies (4 out of 7) that reported new initiatives said that they purchased Smart Cards under the GSA contract. The remaining agencies cited reasons for not acquiring Smart Cards under the GSA contract, such as purchase arrangements with another agency or purchases under other types of contracts.

Federal Agency	Project Name	Status	Estimated Completion
Defense	Common Access Card	Operational	Apr. 2004
Homeland Security	Identification & Credentialing Program	Pilot	
General Services Administration	Nationwide Identification	Operational	Dec. 2004
Interior	E-Authentication	Operational	Jan. 2006
Labour	E-Authentication	Planning	Apr. 2005
NASA	One NASA Smart Card Badge	Planning/Pilot	Sept. 2004
State	Global Look ID	Operational	Sept. 2006
Treasury	Electronic Treasury Enterprise Card	Operational	Sept. 2004
Veterans Affairs	Authentication and Authorisation Infrastructure Project	Pilot	Sept. 2007

Source: GAO analysis of data reported by Federal Agencies

In 2003, the Office of Management and Budget (OMB), in accordance with the President's vision of creating a more responsive and cost-effective government, issued a memorandum to federal chief information officers outlining details of the E-Authentication E-Government initiative on authentication and identity management. OMB also created the Federal Identity Credentialing Committee (FICC) to make policy recommendations and develop the Federal Identity Credentialing component of the Federal Enterprise Architecture, to include services such as identity proofing and credential management for the federal government. In February 2004, FICC issued policy guidance on the use of Smart Card-based systems in badge, identification, and credentialing systems with the objective of helping agencies plan, budget, establish, and implement credential and identification systems for government employees and their agents.

For example, the Washington Metropolitan Area Transit Authority has deployed an automated fare collection system using contactless Smart Cards as a way of speeding patrons access to the Washington D.C., subway system. Smart Cards can be configured to include both contact and contactless capabilities, but two separate interfaces are needed because standards for the technologies are very different.

From this we can see that agencies across the US Government continue to actively invest in Smart Card Projects with plans to issue millions of new cards for both physical and logical access for employees and other personnel in the near future and the investment will grow. We can also establish that US agencies are also moving towards integrated agencywide credential projects, with several agencies planning to consolidate their Smart Card purchases through GSA's Smart Card Access Common ID contract





For High Security: Contactless Smart Cards are the Answer



By Stephen Neff, Vice President Sales and Marketing, LEGIC Identsystems Ltd



Stephen Neff

Photo IDs, first generation technology swipe cards and second generation low frequency proximity cards have long been around in the corporate security environment for the purposes of identification and access control. But while such systems have proven reliable and effective for many years, they no longer meet today's requirements in terms of security and the demand for tamperproof systems. Third generation 13.56 MHz contactless Smart Card technology provides a comprehensive solution for high security single and multi applications.

Photo ID cards provide for ease of identification and increased security levels. However, they provide no reliable vehicle for identity verification. Forgers can recreate ID photos easily using digital cameras and high speed printing facilities. While safeguards against forgery are available and are applied in, for instance, government ID cards, these safeguards tend not to be applied in less sensitive environments in which a quick manual inspection of the photo ID card is the most convenient method of verification.

First-generation technologies provide a higher level of security than photo-only IDs. Swipe cards, for example, contain ID data, usually stored in the form of a magnetic stripe, which is presented to the reader at the protected door. These cards take little time to use. Each card can be individually programmed to permit access to only those areas a holder is authorised to enter. Other criteria such as time and date controls can also be easily introduced, meaning those who are authorised to enter particular areas will be able to do so during work hours, but can be prevented from entering at other times. If a card is lost or stolen, or if a member of staff to whom it was issued leaves without returning it, security personnel can delete that card from the reader's database or from the central computer.

The main drawback associated with first-generation systems is that the readers are prone to wear, and the card data can be copied or altered. In addition, if no second level of verification takes place such as the use of a PIN - intruders can gain access by using lost or stolen cards without anyone noticing.

Second-generation technology cards, exemplified by low-frequency (125/134 kHz) proximity systems, have over the years established themselves as a higher-security alternative to first generation technologies. They allow the convenience of contactless operation, and they also offer the option of incorporating a PIN for verification. Proximity systems are not prone to wear and have a unique ID (UID) number that can be allocated to an employee and a site, which theoretically cannot be copied. These systems as a rule have only a very small read only memory. Hence they offer no possibility to write information back to the card and are unsuitable for use with 'Template-on-Card' biometrics systems and 'Network-on-card' applications. More critical, especially for high security applications, is the fact that the UID number is not encrypted. This has now become, among experts, the biggest drawback where tamperproof requirements and high security is an issue.

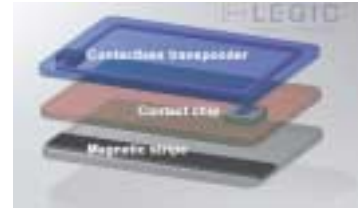


Technology has again moved on, and a new third generation of Smart Cards is looking to supersede these older technologies. Since the introduction of 13.56 MHz contactless Smart Card technology systems, access control systems have now merged into highly practical multifunctional systems that can be centrally and efficiently managed.





Up to 127 independent applications (for example, cashless payments, access, time & attendance, etc.) can be implemented on a single transponder. Dynamic multi-application management accommodates applications of varying memory size and in any sequence. This is particularly beneficial if additional applications have to be added to a transponder that is already in use.



These read/write-capable systems can store significant personal data as well as access control information. Their larger memory allows them to offer more high-security features than less advanced cards making them best suited for many of the security applications that have recently opened up. Third generation 13.56 MHz contactless Smart Card technology offers optimal security for data and applications, from host communication to data memory on the transponder. The high-security encryption level (based on the industrial standard algorithm DES/3DES) can be individually configured for any application and any data path section.

The Link to Biometrics: Like their predecessors, contactless Smart Cards can be exploited by unauthorised users if safeguards are not in place, that is if a card is lost or stolen. However, loading biometrics information onto the memory of a contactless Smart Card (template on card) can solve this problem. This ensures that no one but the rightful owner can use the card. It also addresses privacy issues, since the biometric information is stored on the card and not in the biometric reader system.

There is a wide variety of biometric systems available that are suited to commercial use. It is possible to incorporate the use of retina, iris, hand, palm, fingerprint, vein, face or voice recognition data, or a combination of any of these, onto a single card. Each facility's unique security needs should determine the right type of reader for that facility. In choosing a biometric method, users may consider the needed level of convenience, speed and ease of use, level of security, cost, scalability, size and portability.

To implement a contactless Smart Card/biometric system, the security department uses a biometric reader in a special mode to scan or enroll the biometric of each person authorised to be on the site. This data is then translated into a template using a special algorithm within the reader. The template is encrypted and written onto the Smart Card that is held up to the biometric reader being used for enrolment.



The enrolment process is usually done under the supervision of a site security officer to ensure that the cardholder being enrolled is indeed certified as the correct person. When a cardholder then attempts to enter a site, he or she presents the card to a biometric reader and subsequently presents his or her live biometric—finger, hand, voice or eye, for instance. The reader will evaluate the live biometric and translate it into a number, which it compares with the template stored on the card. If the two match, access is granted.

A whole host of other applications can be added to contactless Smart Cards initially or at a later date. These include cashless payment for vending and employee restaurant use, time and attendance, IT-Access, and parking lot access.

Contactless Smart Card systems, with their benefits for operators and cardholders, are not a thing of the future. They are already in use extensively. And in today's world, with its need for ever more vigilant security, the benefits of such technology cannot be ignored.

