July 2004

Volume 13 • Number 7

Smart Card News

Smart Cards, SIM, Biometrics and RFID

www.smartcardgroup.com

17 • *Why do Payments on the Web?*

06 • *Student Management Card Project*

06 • *BZ WBK Issues 2.7m Smart Cards*

06 • *The Hong Kong Octopus Grows*

This Month's Lead Story

02 **Improved Chip Security for ID and Passports**

In This Issue

Regular Features

World News In Brief

Featured Articles

www.frost.com

Frost and Sullivan

As a fan of pastel colours this website appealed to me with its soft blues and good use of boxed information breaking the website up. To get full access to this site you have to login in, but registration is free. Frost and Sullivan are specialists in many fields including Smart Cards and have a whole host of strategic market and technical information accessible on their website. Specific Smart Card related information can be accessed from their own Smart Card portal which gives analysis and implications of market developments, trends, events and strategies. In their "Our People" section you can actually get biographies and pictures of most of their analysts and consultants. The website navigation bar uses a simple drop down menu system which allows you to move around the website fast and easily. To sum up the website is a good source for Smart Card information and the site is kept everything simple and text based.

Navigation
Content
Appearance

www.imsresearch.com

IMS Research

Another information website you need to login into to get full access is IMS Research's site. Like the F&S site, this site is also free to subscribe. However their press releases can be accessed without joining up. In the members area you can access reports and industry insights and receive free market updates with statistics and extracts from their reports. However their reports don't come for free. Members can access a full list of syndicated IMS Research reports, with prices and publication dates. The website itself has adopted the traditional top and side navigation bar and you can access information easily on fields such as Security ID and semiconductors.

Navigation
Content
Appearance

www.gdm.de

Giesecke & Devrient

Giesecke & Devrient are an international technology group. The front page of their website is nothing to write home about. The background is a bland grey, its content limited and is predominantly text based apart from two flash images. The navigational bar is easy to use, however it does take a few steps to get to any desired information. As an information base this website is very helpful and lays out the Smart Care industry into segments. It gives you simple but to-the-point information on areas such as Java Card Technology, Biometrics, Multos, National ID cards, driving licenses and Dual-Interface Cards. The websites content is kept minimal and its appearance is something to be desired, but overall the website does provide access to interesting information about the Smart Card industry.

Navigation
Content
Appearance

Improved Chip Security for ID and Passports

Global tests for improved security on electronic identity (ID) cards cards and passports are being carried out by Infineon Technologies. The chips being tested have double the storage capacity and will feature state-of-the-art security features. Infineon's SLE66CLX640P security controller is designed for tomorrow's chip card-format electronic ID cards, while the SLE66CLX641P controller is intended for integration into electronic passports. Until now, chip cards have been designed for a maximum useful lifetime of five years, whereas electronic ID cards and passports are generally valid for ten years. Featuring a storage capacity of 64 kilobytes (Kb), both the new security controllers will meet the provisions of the global Standard 9303-1, issued by the International Civil Aviation Organisation (ICAO), which has laid down framework standards for globally valid travel documents for 188 countries.

In line with the ICAO requirements for electronic travel documents, the encrypted data on both chips includes not just the details currently printed on ID papers, such as name, date of birth and period of validity, but also a number of biometric features, characteristics specific to the individual, which can be the face, the prints of one or more fingers, the image of the holder's iris or a combination of these characteristics. Unlike today, the holders of future generations of ID cards may be sure that if they should lose their card it cannot be used without authorisation. These new chips will be the only products in the world capable of supporting both of the contactless interface formats that dominate the marketplace, ISO/IEC 14443 Type A and Type B, which differ in the data transmission protocols they employ. This means that cards or passes containing the security controller can be used worldwide, regardless of the reader infrastructure already installed or being set up.

Tomorrow's electronic ID cards will be suitable for a variety of applications. A multi-application card of this kind could integrate: a personal identity card, a driver's license, an e-government card with a digital signature for using special official services, a credit card, and a monthly commuter ticket for urban transportation systems. The security chip keeps these applications and the associated data records securely separate from each other. In addition, it permits graduated access authorisations, so that only an authorised group of individuals may access or modify the data. This means that the holder need have no anxiety that the border guard examining their ID card is able to gain access to his or her tax return. The SLE66CLX640P chip is designed for use in the ID cards of the future performs the contactless transfer of data up to a distance of around ten centimeters from the reader or via electrical contacts directly to the reader. The SLE66CLX641P chip, on the other hand, which could be integrated into the laminated side of the electronic passport, along with the holder's personal details, has a purely contactless interface.

Tens of millions of examples of the forerunners to the two chips being launched now are already in use in ID projects. These include electronic ID cards in Macao, Hong Kong, Oman, Italy and the US Department of Defense, as well as the national healthcare cards in Taiwan and Italy. The security controllers are being developed in Infineon's center of excellence for contactless technology in Graz, Austria.

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

This Issue's Guest Contributors: Petr Novak • Dr David B Everett • Frost & Sullivan • Richard Crookston • Michael Nitz • Russ Davis • Alan Smith • Paul Everett

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

Axalto Leads in Smart Card Market

The 2003 edition of the annual Gartner report on the chip card market reaffirms, for the third consecutive year, Axalto's number one market share ranking in the microprocessor-based card market segment. According to Gartner's Market Share: Chip Card and Semiconductor Vendors Worldwide, 2003 report, Axalto shipped 262 million microprocessor cards last year, accounting for more than 26% of the world's total 2003 shipments of such high-end cards.

The report also underlines the 34.6% growth in shipments recorded by Axalto between 2002 and 2003. "Worldwide microprocessor-based card shipments reached 989.3 million units in 2003" stated Clare Hirst, analyst at Gartner. "GSM SIM card shipments exceeded the most-optimistic industry expectations, and demand from emerging markets is the main reason for the growth in this sector. Despite a slow start, EMV migration is also likely to have a dramatic impact on the growth of banking microprocessor card market for the next three years."

ITSO Appoints New Executives

ITSO, the Interoperable Transport Smart Card Organisation, has made three major appointments to strengthen their management team at executive level. The new General Manager of ITSO is Paul Newman. Until recently Managing Director of Bottcher UK, Mr Newman has extensive experience of the smartcard industry.

He is joined by Mike Eastham, formerly of Cubic Transportation Systems, as Head of Technology and John Verity, formerly of ATOC, as Head of Compliance and Security. Martyn Roper continues in his role as Head of Operations and the previous ITSO General Manager Peter Stoddart takes on a consulting role to assist the new executive team.

PBS is Phasing out Danmønt

The cash card Danmønt has not been adopted by the Danes as a preferred way of making small payments - mostly it has been used in closed environments like laundries, education institutions and so forth. The number of Danmønt payments has been declining over the last couple of years and since the negative development in the transaction level is not expected to turn, it has been decided to terminate the operation of Danmønt.

At the same time the debt card Dankort has taken over for Danmønt in areas, where the cash card could have been used as a form of payment.

New Biometric Token Concept

Giesecke & Devrient (G&D) are developing a new USB token, which will integrate a complete system for authentication, digital signatures, and biometrics in a single device. SuperToken combines a chip-card, fingerprint reader with picture-processor and verification software in one unit.

Aconite Focus's on Middle East

Aconite has signed a strategic reseller agreement with Eastern Networks, to resell its suite of EMV and Smart Card solutions in the Middle East. This tactical partnership supports Aconite's aggressive expansion in this region where there is massive growth in the cards market and combines Aconite's knowledge of EMV solutions with Eastern Networks knowledge of the markets, banks and financial institutions across the region.

Ulster Bank Test EMV

Ulster Bank have successfully tested their Chip and PIN rollout programme for their debit card customer base utilising a portfolio of EMV test tools from Aconite. Ulster Bank has deployed Aconite's EMV test tool - EMV Facilitator - a tool suite for EMV testing and operations support. The rigorous testing process in key development and certification areas will ensure that Ulster Bank will be confident that its cards meet EMV specifications well in advance of the January 2005 mandate and that customer card adoption will be smooth

Hybrid 3-way Card Reader

Secure Retail has introduced what it believes is the first hybrid and contactless motorised card reader as a single unit, creating a versatile front end for a wide range of retail, access control and security applications. The new reader also has card capture capability for chip and magnetic cards, and an electronic shutter for added security. The Sankyo ICT3K5 series card reader automatically identifies Smart Cards, magnetic stripe cards and contactless cards, and is EMV approved making it suitable for retail applications worldwide as well as government agencies and other security conscious users.

Renesas New Chinese Company

Renesas Technology Corp. has established a new affiliated company, Renesas Technology China Co., Ltd. (RCC), in Shanghai to support the strengthening and expansion of the company's business activities in China. RCC started business operations on July 1 and will be responsible for the local management of R&D, production, sales, and engineering support for China.

BART adds Another Application

The San Francisco Bay Area Rapid Transit District (BART) has extended the use of its BART OTI Smart Card for its employee security access control applications at BART offices and stations. With over 300,000 daily riders and 43 stations, BART provides Bay Area residents with a low cost, high frequency, fast and environmentally friendly alternative for their transit needs. The BART OTI is supplied by On-Track Innovations Ltd.

ITSO Piggy

The Smart Card Group has launched of PiggLET 7816-4, a Java Card applet that is designed to implement the core functionality of ISO 7816-4 for managing files and their directories. Pigglet 7816-4 enables the use of the Java Card as a multi-function card to handle a number of application areas. Typical application areas are for Citizen cards and cards used for transport applications such as those defined by the ITSO specifications for Customer Media 2 (CM2) for general microprocessor cards. In addition the applet offers electronic purse functionality.

Heidelberg Deal with ActivCard

Heidelberger Druckmaschinen AG (Heidelberg) of Germany has selected the ActivCard Secure Remote Access Solution to secure access to vital technical and sales information used by its mobile workforce. The ActivCard solution, comprised of ActivCard AAA Server, ActivCard Tokens and ActivClient for Smart Cards, secures network access for 8,500 Heidelberg mobile employees across 170 countries. The ActivCard comprehensive Secure Remote Access solution improves Heidelberg's customer service capabilities and response time by providing secure network access anywhere anytime.

Massive OTA Download for Saudi

Gemplus has carried out the largest Over-The-Air (OTA) download campaign, on behalf of ALJAWAL (Mobile Business unit of Saudi Telecom), treating 6.3 million SIM cards. ALJAWAL (Mobile business unit of Saudi Telecom) selected Gemplus to deliver an Over The Air platform and Dynamic SIM Toolkit solution in order to ease subscriber access to their new SMS-based content value added services, "Abwab". For speed of deployment, ALJAWAL deployed SIM cards to the field, embedded with a S@T1 dynamic SIM Toolkit engine, which Gemplus then "post-personalised" with 6Kb of data per card, over the air.

Infineon Expands in Portugal

Infineon Technologies is expanding its existing memory chip assembly and test (backend) facility in Portugal. The company is investing a total of 230 million euros in the second module. Work on expanding the facility kicked off in fall 2003 and full capacity will be reached by mid-2006.

Biometrics for Japanese Borders

Government Officials in Japan are considering using biometric technology in a fight to counter terrorism after claims that al Qaeda could be establishing a network in Japan. Like the United States, Japan plans to introduce a biometric border control system using fingerprints and facial features to tighten immigration.

Japan already plans to introduce Smart Card based passports which will contain biometric data on the holder, but talks are underway as to whether they will use this information as a means of screening foreign visitors. A working team of officials, including those from foreign and justice ministries, plan to start discussions on the issue later this month.

For more information visit ...

Renesas Technology Corp
www.renesas.com

On-Track Innovations Ltd
www.otiglobal.com

Smart Card Group Ltd
www.smartcardgroup.com

Fingerprint Readers for Malaysian Hospitals

Labcal's Technologies Inc has been awarded a contract by Kumpulan Perubatan Johor (KPJ), the Healthcare Division of Johor Corporation to supply SmartPrint Sentry readers (SAC-3000) to 14 specialist hospitals, located all over Malaysia. Through its Malaysian affiliate, Labcal Malaysia Sdn. Bhd., Labcal's SmartPrint Sentry wall-mounted devices and SmartPrint Tribunus software are being installed and used in KPJ-owned hospitals.

Daon Biometrics for Traveler Program

Daon will supply the core biometric technology for three of the five airports in the U.S. Registered Traveler Pilot Program. The Transportation Security Administration (TSA) awarded Unisys a contract for Los Angeles International Airport, George Bush Intercontinental Airport (Houston) and Minneapolis St. Paul International Airport. Daon will provide the core biometric and biographic management software, including fingerprint and iris recognition software, and solution development expertise to the Unisys team.

VeriFone Partner Printec

VeriFone International Partner Printec S.A. has been awarded a contract to supply 1,300 VeriFone Omni 3750 terminals to Alpha Bank, the Official Bank of the ATHENS 2004 Olympic Games. This latest deal brings the total number of VeriFone terminals used by Alpha Bank to more than 16,000. Athens-based Printec will deliver the terminals over the next two months, enhancing Alpha Bank's existing estate of 5,500 Omni 3750 countertop devices. VeriFone has sold more than 30,000 Omni 3750 terminals in the Greek market since its launch, and has more than 100,000 VeriFone terminals currently in operation in Greece today.

Sun get Leadership Award

Frost & Sullivan's recent study, World Battle of Platforms Markets, has recognised Sun Microsystems' ability to analyse market dynamics and effectively use this knowledge to improve its market position. Frost & Sullivan presented the 2004 Market Leadership Award to Sun Microsystems in acknowledgement of its market-driven strategies that have placed it in a strong position in the Smart Cards industry.

Precise Access to Fitness24Seven

Precise Biometrics AB has delivered a physical access control system to Fitness24Seven, a Swedish gym chain with facilities in Malmo and Hassleholm. So far, 2500 cards have been issued to members, who can gain access to gym facilities 24 hours a day by verifying their identity with a fingerprint and a Smart Card. Precise Biometrics will also provide support and maintenance of the system, for which Fitness24Seven will pay a fee based on the number of membership cards in circulation.

Cosmos Bank Orders More Cards

Keycorp Limited has extended its relationship with Cosmos Bank for the supply of MULTOS Smart Cards. A further 500,000 MULTOS Keycorp Smart Cards have been ordered for Cosmos Bank's MasterCard International (MCI) Smart Card rollout, taking the total past the one million mark. Cosmos Bank has implemented 800,000 Keycorp MULTOS Smart Cards since 2001, making it the first bank to issue MULTOS based EMV cards in Taiwan.

New Board Director joins ACT

Applied Card Technologies Ltd (ACT) has appointed Ramanuj Banerjee as Director. Ram, will be responsible for driving new business opportunities and generating new revenue streams for ACT. He will focus on the UK, European and the US leisure, public sector and retail markets. Ram brings 24 years of experience in IT and joins ACT from ActivCard Inc in the US.

Dione announces Figures for 2003

Dione has achieved record revenues and profits for the 2003 fiscal year with a sector growth of 57%. This continued success will see Dione equipment present at over 40% of the points of sale in the UK, the first country to adopt the global EMV Chip & PIN standard.

Other highlights during 2003 for Dione included a move to a purpose built HQ, Company certification to the latest TickIT 5 global quality standard and the launch of a new payment terminal platform incorporating several technology patents.

OTI Restructures for China

On Track Innovations Ltd. (OTI) has restructured its marketing strategy to the Chinese markets by focusing on direct sales of its SmartID products in China, and by selling its 50% stake in the e-Smart System joint venture to its partner. For the year ended December 31, 2003 and the three-month period ended March 31, 2004, the e-Smart Systems joint venture accounted for approximately 1% and about 0.6% of OTI's total revenues on a consolidated basis, respectively. The sale of OTI's interest in the e-Smart System joint venture is expected to result in multiple strong marketing channels for OTI's products in the Asian market by enabling OTI to focus on directly selling its SmartID products while e-Smart continues to distribute OTI's micropayments and other products on a non-exclusive basis.

AuthenTec to Provide First Biometric Plug-In for Windows CE 5.0 OS

AuthenTec's TruePrint technology is the first fingerprint authentication technology to be included with Microsoft's Windows CE operating system with the release of the latest version 5.0. Included with the third-party development toolkit, Platform Builder 5.0, will be support for the AuthenTec's EntrePad fingerprint family of sensors which offers developers an easy method for adding fingerprint biometric support to products such as PDAs, mobile phones and multi-user computer terminals found in hospitals and in call centers.

BZ WBK Issues 2.7m Smart Cards

Polish bank, Bank Zachodni WBK (BZ WBK), has issued Austria Card (a subsidiary of the Austrian Central Bank OeNB), an Austrian provider of Smart Card Solutions, with a contract for the supply of 2.7 million Smart Cards. The cards will be used in a roll-out that aims to replace Poland's old mag-stripe cards with new Chip Cards.

Student Management Card Project

e-Smart Korea and Samsung SDS, in association with Korean Company, Kobile Co., Ltd., have entered into a "Student Management Card Project, Cooperation Agreement." Samsung SDS has projected that this Cooperation Agreement has total revenue potential during its first six years of operation alone (through 2011) of in excess of the equivalent of US$ 617,000,000 based on current exchange rates.

The first of a number of planned domestic Korean and International projects that e-Smart Korea and Samsung SDS have agreed to cooperate in doing, the "Student Management Card Project" calls for the installation and operation of the Company's proprietary Biometric Verification Security System operating platform and the issuance of the Company's, advanced Super Smart Card to students, faculty and employees of participating learning institutions throughout Korea. Specifically, the Student Management Card Project, operating on the BVS2 platform will connect mid-level schools, high schools and colleges nationwide.

The Hong Kong Octopus Grows

Financial institutions offering Octopus Automatic Add-Value Service (AAVS) has increased to 20 major banks and credit card issuing companies in Hong Kong. Citibank and Hang Seng Bank are the most recent additions to offer this service to their credit cardholders. When the remaining value on the card reaches a zero or negative balance, or when the remaining value plus the maximum negative value is insufficient to settle the full cost of the transaction, the card will be automatically reloaded with HK$250 through the extensive network of Octopus readers all over Hong Kong (each card can only be auto-reloaded once per day).

The reloaded amount will be deducted from the cardholder's designated credit card, savings, current, or integrated bank account, with every AAVS transaction clearly shown on the bank statement or passbook.

For more information visit ...

Labcal Technologies Inc
www.labcal.com

Daon
www.daon.com

VeriFone
www.verifone.com

Keycorp Ltd
www.keycorp.net

Applied Card Technologies Ltd
www.card.co.uk

An Introduction to the World of Microprocessor Smart Cards and Card Operating Systems.

By Petr Novak, SmartWorldAcademy, ACG

Petr Novak

Despite the fact that the Smart Card was invented a long time ago, the Smart Card market is still extremely fragmented. While GSM can be considered mature, other Smart Card applications such as logical access are still in their early stages. Until now, the very few key global players that exist in the market have tried to offer a complete Smart Card based solution from one source. These players buy Smart Card microprocessor chips from silicon manufacturers, package these chips into contact, contactless or dual interface modules and embed these modules into the actual card body. But the main value of these players is not the card hardware they provide - it's the software, both for the actual card and for the computer system which uses the card.

The rest of the market is organised very differently from the key global players who specialise only on one aspect of the total solution and the system integrators have the option of mixing and matching different suppliers for parts of their solution. The silicon manufacturers are the same, and they often take the responsibility of packaging their chips into chip modules. The embedding of the chip into the printed or blank white card body is becoming a commodity service offered by a very large number of independent card manufacturers around the world. So for the Smart Card hardware, the market already offers choice of different suppliers and technologies. It is the Smart Card related software where the market does not offer many options. The key component of the Smart Card software is the card operating system which manages the resources and creates an environment where applications can run. The on-card applications have either the form of data structures and a number of well-defined operations involving these data structures (such as debiting an electronic purse or digitally signing a secure hash of an e-mail message), or are applications with their own executable code performing application-specific data processing.

Due to the high security requirements and the strict control of the detailed hardware description, there are currently no open source card operating systems. For each Smart Card based solution, there has to be a matching software component within the system which uses the card as a secure token for secure information storage or processing. For desktop operating systems, the Smart Card specific interfaces are often concentrated in layers of drivers and middleware and are not directly visible to the end user. Many horizontal applications such as e-mail software or secure networking solutions are able to use standard middleware software interfaces to support Smart Cards as secure tokens. For new applications, the abstraction level of the available middleware standards is high enough to enable application developers to ignore the complex technical details of Smart Card hardware and card operating systems.

The Role of Silicon Manufacturers - There are not that many companies developing and manufacturing chips to be used in microprocessor Smart Cards. The key technological reasons are access to very low power CMOS technology (especially for the contactless and dual interface chips) and special security requirements, which prohibit the use of standard silicon macrocells to build the Smart Card chips. On the business side, as most of the market is dominated by the small number of key card manufacturers with long term contracts with existing silicon suppliers, it is not easy to find a market for a new silicon offering. Also, most customers require the chip to be evaluated to meet security requirements, which is both a long and expensive process, delaying the time to market for the newcomers. Recently, the first licensable Smart Card-related IPs have become available to silicon manufacturers, such as the SC100 and SC110 Smart Card cores by ARM. These have been licensed both by established Smart Card silicon vendors and newcomers to this market.

Large System Integrators - The large global and regional system integrators and IT services companies are often required to deploy Smart Card based solutions within their customer base. With new global projects which require the breadth and depth of the large integrators, these players will be more and more frequently found in a role of general supplier of complex solutions involving Smart Cards and will soon start to invest into the Smart Card specific technologies.

Card Operating Systems - Designing the card operating system requires not only a deep knowledge of the smart card hardware, but the designer of the card operating system plays a key role in meeting the security requirements for the overall solution. As for the hardware certification, many applications mandate security evaluations and certifications also for the card operating system. Besides the large card manufacturers who have their own card operating systems there are two other types of companies who develop card operating systems. The first group encompasses some large IT companies such as IBM and T-Systems who have business units specialised in card operating systems. Besides being used for in-house projects, some of these operating systems are licensable by third parties. The second group are companies specialised in developing card operating systems as their main product offering and licensing these either through silicon manufacturers, or to card manufacturers, solution providers and system integrators. From the technical point of view, the card operating systems are either filesystem oriented (based on the ISO 7816-4 standard, which enables the storage of data on the card and to perform a predefined fixed set of operations on the data), or based on a virtual machine and programmable applications, which may add new types of data processing not included in the operating system (the typical examples of virtual machine based card operating systems are Multos and JavaCard). Today, both of these types of card operating systems have their market segments, although the market share of JavaCard based card operating systems is the one which grows fastest.

The Role of Independent Card Manufacturers - Today, the principal role of the independent card manufacturers is to embed the chip module into the card body and to initialise and personalise the card. Although there are some easily repeatable solutions which do not require the card manufacturer to be able to develop a new application or to integrate the card into the application environment, a tight integration of Smart Cards into existing applications is beyond the abilities of a typical independent Smart Card manufacturer. However, the local presence of independent Smart Card manufacturers makes them ideal partners for local system integrators and solution providers, as this partnership offers much greater flexibility than the one-size-fits-all offering of the global players and can offer much faster delivery and more competitive pricing of the fully personalised cards due to the local nature of logistics between the manufacturer and end user.

Specialised Smart Card Integrators - Most local Smart Card projects have been designed and deployed by small boutique players with specialised know-how in Smart Card technology and a vertical market segment. These companies are often VARs of the key global card manufacturers and offer their own applications and solutions using the complex product portfolio of their main supplier. These local players are also looking for more independence from their main (and often sole) supplier, greater differentiation from the direct sales channel and more flexibility by using the services of a local card manufacturer.

The New Growth Drivers - The GSM SIM market has been by far the largest and fastest growing segment of the microprocessor Smart Card market. In recent years, the increased global awareness of threats such as banking card fraud, cyber crime and global terrorism have led to new requirements of governments, financial institutions and large enterprises for solutions with higher levels of security. Often these solutions include microprocessor Smart Cards either in the traditional plastic card form, or in new forms such as chips embedded in passports or other types of documents or tokens. The most well-known global projects involving Smart Cards are the migration of Europay-MasterCard-VISA branded payment cards to chip-based technologies, machine readable travel documents (passports, visas), national ID, driving license and e-health projects, the European digital tachograph project and a few others. At the same time, Smart Card hardware offers means to protect data on the card from other applications. The virtual machine based card operating systems such as JavaCard offer transaction support and protection from different applications on the card. Finally, the costs of Smart Cards and Smart Card readers have recently dropped to the level where it is no longer the key obstacle preventing their adoption by large corporations and small business, or even in government sponsored global or national projects.

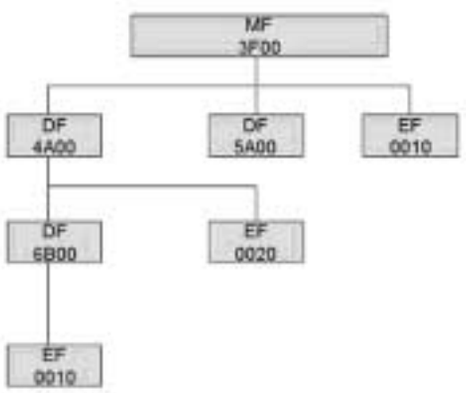
At this point the benefits of the Smart Card based solutions clearly outweigh the financial burden. This is true not only for contact cards, but also for contactless processor cards and cards with both contact and contactless interfaces (dual interface), which represent a natural stepping stone for established players in the RFID area looking for higher security solutions or innovative applications.

ISO/IEC Standard 7816 - 4 File Structures

By Dr.David Everett, CEO, Smart Card Group

David Everett

The standard describes a hierarchical file structure similar to that provided on the Personal Computer. It has a root file called the MF or Master File, directory files called DFs or Dedicated Files, and EFs or Elementary Files that actually store the data. Any hierarchy can be produced as long as you maintain the status that all files are subservient to the MF and that EFs are always subservient to an MF or DF. The figure below shows a possible hierarchy,



In practice of course these files are likely to be arranged in some structure that maps the applications being handled by the card. The DFs would represent application areas, on a Citizen's card for example there might be a DF for Education, a DF for Leisure, a DF for Libraries, and a DF for Transport. These DFs would be on a peer level below the MF. Then underneath each of these DFs would be the EFs that store the data held in as many separate files as necessary.

These files can be identified in one of 4 ways: **1)By DF name -** Any DF may be referenced by a name which can be from 1 to 16 bytes. This allows the file to be selected by means of an AID (Application Identifier) which is a registered name as defined in Part 5 of the ISO/IEC 7816 standard. **2)By File Identifier -** Any file (MF, DF, or EF) may be referenced by a 2 byte code. The value '3F00' in hexadecimal is the value reserved for the MF. The designer of the file hierarchy may choose the other identifiers as required but must avoid ambiguity and should not use the same identifier under a particular DF. The value '3FFF' is reserved. **3)By Path -** Any file may be referenced by a concatenation of File Identifiers. This is just the same as you would reference a file on the PC. For example the bottom left EF in the figure above would be referenced by, '3F00 4A00 6B00 0010'. **4)By Short EF Identifier -** Any EF may be referenced by a single byte of which 5 bits are used to value the file in the range 1 to 30. The value '0' is used to reference the currently selected EF. These Short Identifiers cannot be used in the Path referred to above nor can they be used in a Select File command.

The Data in the EF files can be arranged in one of four ways: **1)Transparent EF -** this is where the data is just stored as a continuous block In this case the data is referenced by an offset integer into the file of either 8 or 15 bits where the first element of data has an offset of '0'. The amount of data to be read or written is then defined by another parameter. The data is managed by the Read Binary, Write Binary, and Update Binary commands. The amount of data that can be read or written is 255 bytes in the short format or 65,536 bytes in the long format. The maximum offset of 15 bits allows a value of 32,767 bytes which gives a maximum file size of 98,303 bytes. **2)Linear Fixed EF -** this is where the data is stored in records of fixed length. In this structure the data is accessed by individual records using the Read Record, Write Record, and Update Record commands. The first record is number 1 and up 254 records can be individually accessed. The maximum size of the record is 254 bytes which gives a maximum file size of 64,516 bytes.

3) Linear Variable EF - this where the records can be of variable size. As before there can be up to 254 records but each of these records can be of variable length with a maximum size of 254 bytes. In this case the record effectively contains data that defines the size of the particular record. The same commands, Read Record, Write Record, and Update Record are used as previously. **4) Cyclic EF -** in this case the records of fixed length can be imagined to be in a circle where the most recently created record is the first logical position in the file, with the previously written record number 2 and so on. This is typically used as the form for a log file where the older records get overwritten and you are always maintaining the most recent records as the size of the file. This file which uses the same record commands as above is also limited to 254 records of 254 bytes. As with the previous record structures the individual records can be accessed as the first, next, previous, or last records in the file.

Differentiation is Key in the Smart Card IC Market

FROST & SULLIVAN

By Frost & Sullivan, World Smart Card IC Market Analysis

Manufacturers of Smart Card ICs are focusing on offering increasingly advanced ICs and to differentiate themselves from competitors, Smart Card IC manufacturers will have to focus on vital competitive parameters of price, technology performance, and time-to-market. Research and development investment toward improved chips is also needed, which proves to be difficult in a shrinking profit margin environment. New analysis from the Frost & Sullivan, World Smart Card IC Market, reveals that this market generated revenue totaling $1.40 billion in 2003 with the total market revenue expected to reach $2.38 billion in 2007.

The global system for mobile communications (GSM) penetration of the less saturated markets of Asia and the Americas is increasing, and telecom operators are promoting higher-memory SIM cards to provide value-added services. Increasing demand for high-memory 64k and 128k SIM cards as well as for Java cards in particular are improving the GSM product mix."The arrival of 3G and 2.5G services is boosting high-end Smart Card IC chip sales since they require larger memory capacity to store new features and bigger files," says Industry Analyst Anoop Ubhey.

The use of contactless technology by retailers and in various transit projects worldwide is also spurring high uptake of Smart Cards. In addition, the retail and payment application have shown tremendous potential for contactless Smart Cards. "Migration to the EMV standard in the banking sector is also creating substantial opportunities for Smart Card IC chips," states Industry Analyst Jafizwaty Haji Ishahaq. Government's interest in ID security applications post 9/11 brings further potential to the chip-based market and with the launch of high volume national ID projects such as the China national ID project all help to generate enormous opportunities for the industry.

"Using Smart Cards not only provides easy identification and decrease in instances of fraudulent activities, but also benefits governments through the integration of multiple applications such as retirement benefits, e-purse, and so on," says Programme Manager Prianka Chopra. Nonetheless, major Smart Card projects that require expensive infrastructure upgrades can create cost issues for the implementer and lead to delayed projects.

www.frost.com

Why WiFi will go the Distance in the Wireless Payment Race

By Richard Crookston, Head of Marketing, VeriFone EMEA

Richard Crookston

Although Bluetooth has been touted as the future for wireless EFTPoS applications, issues with range and security hold it back and deem it an impractical payment solution. Wireless Fidelity (WiFi), on the other hand, opens new doors for payment industry applications: it is robust and effective and offers significant benefits to retailers. Put simply, Bluetooth is a Personal Area Network (PAN) solution. According to the IEEE 802.15.1 standard, this is what Bluetooth was designed for. Like WiFi, Bluetooth is a cable replacement technology, but its short range makes it useful only for connecting devices to peripherals, for example, synchronising information stored on a mobile phone and a Personal Digital Assistant (PDA).

In this respect, Bluetooth is a useful tool around the house, but its basic design makes it unsuitable for EFTPoS applications. Its biggest drawback is its short range. Because Bluetooth is a low power technology, its range is limited to a maximum of ten metres. A greater range is needed in most retail environments. Added to this, it is no simple feat to coordinate an armada of disparate Bluetooth-enabled devices within one combined EFTPoS system - short range makes this a complicated prospect, when the whole point of wireless payment is to make things easier. The suitability of Bluetooth as an EFTPoS option is further reduced by a number of security issues that remain unresolved. As stated earlier, Bluetooth is designed for Personal Area Networks only: that is, specifically for one-to-one short-range communication, and not for EFTPoS applications. In the comfort of your home, there are few PANs that urgently require robust security - the information being exchanged is unlikely to be of interest to hackers and fraudsters, who, in turn, are unlikely to be within a range of ten metres, ready and waiting with a Bluetooth-enabled device on the off-chance that you are using one next door.

Bluetooth's security problems remain unaddressed because the applications for which Bluetooth was intended do not generate a pressing need for security. If it is used in home entertainment applications, there is little to worry about. In the context of electronic payment, however, Bluetooth's security problems should be taken very seriously. 'Bluejacking', where mobile phones are used to send unsolicited messages to other devices within range, and 'Bluesnarfing', where users connect to and access data held on other people's devices, are two issues that the payment industry must quickly acknowledge. Neither setting Bluetooth-enabled devices to 'undiscoverable' mode nor upgrading them to the latest 1.2 version of Bluetooth will necessarily protect against the threat of Bluesnarfing. These attacks are relatively harmless if the victim is sending, say, travel information, but this vulnerability has serious implications if the victim is sending payment information.For wireless EFTPoS applications, retailers must turn to WiFi to ensure the integrity of their customers' sensitive payment data. Due to its many advantages over Bluetooth, WiFi is emerging as a worthy victor in this field. It is ideal for running robust commercial applications over local area wireless connections - indeed, as a wireless Ethernet technology, it was designed to replace LANs, and in this capacity its increasing popularity shows no sign of abating. Market research companies reported WiFi hardware shipments in 2003 valued between $1.7 billion and $2.5 billion, and WiFi hotspots are surfacing everywhere from airports to Quick Service Restaurants (QSRs).

Corporate enterprises everywhere are already familiar with WiFi, so any challenges that remain in adapting it for widespread deployment in retail environments should be well understood, and can be identified and surmounted easily. With range in mind, few will accept the task of planning a shop floor for Bluetooth, but this solution area is exactly what the WiFi standard was designed for. Many retailers already use a wired Ethernet system, so extending their infrastructure through WiFi is a simple installation with numerous benefits. With greater bandwidth and faster processing, using WiFi to implement IP to the EFTPoS terminal results in faster transactions and versatile handling of data intensive applications such as cheque conversion with imaging.

Using WiFi for running IP applications also provides end-to-end SSL security to encrypt the data that will be routed over the network. With its 128-bit encryption, SSL is widely supported by the financial industry as the security standard of choice wherever electronic payments are concerned. SSL is a standard that offers interoperability and scalability, as well as fast automated certification that is appropriate for all EFTPoS transactions, regardless of transaction volume or value.

This summer brings the release of the 802.11i standard and the industrial-strength encryption used in the new WiFi Protected Access (WPA) protocol, providing security protection equal to, or even superseding, that of transactions currently conducted over wireline technology. WiFi technology is developing rapidly to stay on top. Recent breakthroughs have tackled the issue of power consumption, making handheld WiFi devices an extremely viable - and attractive - option. The benefits of WiFi for Voice-over Internet Protocol (VoIP) suggest that mobile phone users may soon be offered interoperability of WiFi and 3G transmissions such as CDMA 1x and GSM/GPRS. The use of WiFi for wireless payment applications offers speed, security, versatility, accessibility and cost-effectiveness - retailers are already responding to these clear advantages.

Smart Care for Patients

Giesecke & Devrient

By Michael Nitz, Giesecke & Devrient

Health officials all over the world are faced with the same problem-namely, that the costs of their national health care systems are rising dramatically year after year, while the quality of patient care does not seem to improve at the same rate. For that reason, intelligent healthcare concepts and technical solutions that will both reduce costs and also increase the quality of medical care are sought after. Germany's healthcare reform, which went into effect on January 1, 2004, was designed by lawmakers trying to control the exploding cost of treatments.

An important component of this reform is the planned introduction of cards for medical insurance policyholders by January 1, 2006. In addition to containing its owner's personal information, the chip card also features the option of including medical data, previous drug documentation and electronic prescriptions. When changing physicians or being admitted to a hospital, the treating physicians will always have access to updated patient information. They will prevent the time-consuming requests for treatment documentation and expensive duplicate examinations. This stored, sensitive information requires special protection from unauthorized access.

The Health Professional Card (HPC), also known as a physician's card, is equipped with a passport photo of the owner and ensures this type of protection. Currently, five Saxony-based hospitals are conducting a field trial named 'SaxTeleMed' using the HPC. The Giesecke & Devrient technology group supplied a total of 620 electronic physician badges. G&D developed these special Smart Cards in accordance with specifications given by the KBV, a national association of medical insurance providers, and the German Medical Association. The principle behind the HPC is simple. By inserting the electronic physician's card into a card reader and providing a PIN, physicians can identify themselves as being authorized to examine and make changes to a patient's electronic file. Yet the HPC is more than a medium for authentication; it is also a prerequisite for digitally signing and encoding medical findings, images and patient data.

For the first time, the HPC meets all legal electronic signature requirements and it accomplishes secure communications between treating physicians over open networks. The electronic physician IDs become especially meaningful when it comes to accelerating diagnoses and shortening a patient's non-treatment intervals. Thus, it is conceivable that a specialist, who is either at another specialised clinic or on call at home, can analyze a diagnosis if required. Instead of having to wait for the specialist to make a personal visit, it is now possible, for example, to send an X-ray via the Internet to the specialist's computer who can immediately provide an expert opinion.

Biometric Myths: Six of the Best

By Russ Davis - CEO of ISL Biometrics

Russ Davis

It is probably the hottest sector in the security field today. Yet the biometrics industry, which produces human-based identification systems, is weighed down with claims and counterclaims, fallacies and myths. While some of the myths are no doubt based on an element of historical or scientific truth, some are now so out of date or inaccurate that they are almost laughable.

Myth Number One - The first myth that needs to be dispelled is that biometrics is a modern-day idea. Despite its high-tech glitzy image, the principles behind the technology can actually be traced right back to Egyptian times, when workers building the great pyramids were not only identified by their name, but also their physical size, face shape, complexion and other noticeable features, such as scars. It may have taken the next four-and-a-half thousand years to really get going (*see "A Brief History of Biometrics"*), but the technology is now experiencing a "hockey stick" adoption curve with governments, hospitals, schools, airports, retail outlets and modern offices all successfully using this remarkably straightforward empowering technology.

Technology Truths - The problem with such a rapidly emerging industry is that many people are elevated to the position of "expert", almost overnight. This can be a particularly dangerous situation - especially when the expert used to be the company salesman or marketing executive. This scenario has led to some of the industry's best technological fallacies, which can either be put down to pure ignorance, or worse, the stirring up of malicious rumours in order to gain competitive advantage. Take for instance myth number two - iris recognition devices use lasers to scan your eyes. This damaging rumour is completely without substance, although the confusion is understandable given that the first company to produce such a system called itself IrisScan (now renamed as Iridian Technologies). In fact an iris recognition camera takes a black and white picture from up to 24 inches away and uses non-invasive, near-infrared illumination (similar to a TV remote control) that is barely visible and very safe.

Myth Number Three - stolen body parts - is also a classic, and has been seized upon by many a Hollywood director, who are not known for letting the true facts cloud a good storyline. With most biometric devices there is an element of liveness detection, which can measure many variables, from a finger pulse to a pupil response. This would normally be enough to prevent the system from working once the body part had been removed. However, other factors quickly come into play. For example, an extracted (or enucleated) eyeball quickly begins to decompose, with the cornea clouding over and obscuring the iris. A severed finger also dies rapidly - typically becoming useless after around 10 minutes.

New Myths - Fingerprint technology also gives us number four on the list of myths. This relates to the inability of the technology to enrol or verify the identity of children, or women of Asian descent. This myth is relatively new, because until a few years ago it was a reasonable criticism of the technology, given the challenge of acquiring small fingers with "faint" fingerprints. However, recent advances in imaging have led to far greater resolutions being achieved by fingerprint sensors, so boosting a biometric system's ability to extract the pertinent information required to create a biometric template of that person. Children, in particular, seem to hold no fear of the technology, believing it to be "cool". It may be surprising to learn that at least 1,300 primary schools in the UK are using fingerprint technology to replace old-fashioned password-based systems in their libraries. The interesting spin off benefit here is that so many children want to use the technology that the number of books taken out increases dramatically.

Police Protection - Number five on the list relates to the belief that fingerprint information captured by a commercial fingerprint system could somehow be used in a criminal investigation. This myth stems from a misunderstanding of how a biometric system typically works in a commercial environment. Almost none of the available commercial fingerprint-based systems store the entire image of a fingerprint. Rather they extract information from that fingerprint to create a mathematical representation or template.

This template, which is often encrypted, is designed so that it cannot be reverse engineered to reconstruct the original fingerprint image, and so is useless information to the police, or indeed a hacker. (The feeding of identical template data to a fingerprint system's matching engine by a hacker will normally fail, as this is almost a sure indication that the data has been stolen and that a replay attack is underway.) In a non-commercial biometric system, such as the recently announced US-VISIT system, which is being installed to monitor the comings and goings of foreign nationals in the USA, the situation is different, with full fingerprint and facial images being acquired and stored. This information can and has led to the arrest of more than 500 people since January 2004.

The silver bullet? The final myth number six- is perhaps the most important. So often biometrics are touted as the silver bullet that will rid the world of evil. Again this is to over-estimate and misunderstand the abilities of biometric technology. For instance, contrary to common belief, biometric systems are not able to confirm with any level of certainty the true identity of a person. Rather, they are able to confirm whether this is the same person that initially enrolled into the system. The person's true identity is irrelevant to the biometric system. Confirming a person's true identity is far more a question of checking the validity of an individual's official identification documents, such as birth certificates or driving licences. Biometric technologies are also unable to perform miracles. If a government doesn't have a quality photograph of a known terrorist suspect, then the chances of stopping that person at a checkpoint using facial recognition are slim. All that said, biometrics can play a valuable assisting role in the fight against organised crime and terrorism, but it must be part of a holistic approach, which uses many different strands of information.

From Myth to Reality - While there are many other myths plaguing the biometric industry, the good news is that the technology has been able to rise above them to claim its place at the security top table. The benefits of the technology have just been too attractive to let unfounded myths get in the way. Some of today's best biometric systems are saving organisations time and money, while helping to raise the security bar to new heights. For example, "door-to-desktop" systems are now appearing, which merge an organisation's physical access control system at the front desk with its network of computer terminals around the building. This enables an employee to replace cumbersome tokens and passwords with their fingerprint, turning the premises into a truly smart environment. In the past, pundits have talked about mainstream biometric adoption being years away. Today, with smart passports just around the corner, and adoption rapidly increasing in places such as hospitals, schools and airports, new estimates are being measured in months. The myth that biometrics will never become a mainstream technology is truly being smashed.

A Brief History of Biometrics - Biometrics go back a lot further than their futuristic image might suggest. Even the architects of the Great Pyramids in Egypt recognized the benefits of identifying their labourers using previously noted bodily characteristics. The Egyptians were clearly ahead of their time, as very little development in the field of biometrics occurred for around four thousand years. It was only in the late 1800s that people started to develop systems that used the fingerprint and other bodily characteristics in order to identify individuals. In 1880, for example, Henry Faulds, a Scottish doctor living in Japan, published his thoughts on the variety and uniqueness of fingerprints, suggesting that they could be used for the identification of criminals. Meanwhile, in 1900, the important Galton-Henry system of classifying fingerprints was published. Other than a few isolated pieces of research into the uniqueness of the retina (which was finally turned into a workable product in 1985), the biometric industry remained fairly static until the 1960s, when the Miller brothers in New Jersey, USA, launched a device that automatically measured the length of people's fingers. Speaker verification and signature verification were also developed in the 1960s and 70s. Interest from the US armed forces and intelligence agencies then emerged, but it wasn't until the turn of the century, and in particular until after 9/11, that the awareness of biometrics broke out of specialised industry circles to reach the fever pitch levels seen today.

"Phishing" - Defrauding Online Retailers

By Alan Smith, Buisness Development Director, ClearCommerce Europe

Alan Smith

Defrauding e-commerce merchants is now a sophisticated and lucrative criminal business. Criminals are using methods such as 'phishing' to steal proprietary financial information, or perhaps even your identity, to enable them to attack e-retailers and providers of Mail Order Telephone Order services (MOTO) and steal millions of pounds worth of goods like televisions, PCs, digital cameras – anything that can be quickly turned into money.

Phishing scams, such as email campaigns disguised with logos of banks or your internet service provider, require you to enter sensitive and useful data such as your card number, mothers maiden name, or even pin number. The information then goes to organised crime rings in West Africa, Malaysia, Eastern Europe, or some other unlikely safe haven where laws protecting against cyber crime may be poorly enforced or nonexistent.

This information is used by criminals to rob retailers in large scale strikes. When a storefront with desired goods is found, fraudsters work in teams to make multiple purchases, taking an unsuspecting retailer for potentially millions of pounds. While consumers are almost fully indemnified against fraud-related losses by their card issuers, merchants' exposure to loss through fraud is virtually limitless. Costs begin with the loss of the value of goods sold and shipped – generally, at the fraudster's request, by an expensive overnight courier. Add to this the processing charges associated with the reversal of a bad transaction, plus the costs of investigating the chargeback.

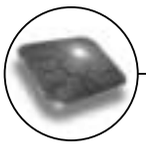
Once a merchant has exceeded the threshold established by the credit card issuing associate, additional fees and penalties pile up. But this is just the beginning. Yet inspite of these overwhelming costs, less than one third of online merchants use some sort of protection from card-not-present fraud, perhaps encouraged by apparent low industry loss averages.

For online merchants the lesson is clear: Don't get hung up on industry averages; fraud attacks can take a company down. Once fraudsters have attacked its too late to mount a defence. The best defence requires a dynamic and comprehensive infrastructure, supported by a reputable vendor with an up-to-the-minute understanding of what the fraudsters are doing and a large client database from which countermeasures can be configured to address emerging schemes.

According to Gartner, the dollar value lost to fraudulent transactions last year was 1.7% of total sales. All industry experts agree that the problem will continue to grow through the rest of this decade, mirroring the growth of the online channel. With Forrester Research predicting that online business volume will increase to at least eight per cent of total retail by 2007, online fraud could quickly develop into a financial crisis of epidemic proportion.

On average retailers stop around 6% of transactions through 'fear of fraud' so there is significant business to be gained if retailers used more accurate tools to prevent online fraud and allow good customers to continue to purchase online." It is interesting that in the fast moving and dynamic world of fraud prevention: whenever you find a fix, the crooks will find a way around it. Preventing e-commerce fraud while maximising sales is an ongoing battle in which merchants must remain vigilant.

www.clearcommerce.com



Manufacturers Must Articulate Business Case

By Frost & Sullivan, Battle of Platforms Analysis FROST & SULLIVAN

Smart Card manufacturers and open platform consortiums need to establish a viable business case for multi-application cards. Misgivings among card issuers about the returns on investment made on multi-application Smart Cards is one of the primary barriers to their greater deployment. New analysis from the Frost & Sullivan report, "Battle of Platforms", reveals that this market has generated unit shipments of 220 million for JavaCard and 8.3 million for MULTOS during 2003 and that the total market unit shipment by 2008 is expected to reach 867 million and 46.8 million for JavaCard and MULTOS, respectively. The relative high costs of open platform applications over native platform products continues to be a major deterrent to their acceptance. While open platforms are ideal for Smart Card applications that feature dynamic downloadable capability, they are at the wrong end of the price spectrum for end users who prefer less expensive, low-functionality solutions.

"With the introduction of the 'JavaCard S' program and MULTOS 'step/one,' the cost restraint of application development in open platforms has been alleviated to some extent," says Frost & Sullivan Research Analyst Karthik Nagarajan. "End users can now use JavaCard and MULTOS platforms for single/fixed function card applications, which will also be interoperable with multi-application cards that an organisation might launch later." In the banking segment, the uptake of JavaCards and MULTOS cards has been steady, but the market share rankings are expected to remain static in the short and medium terms. This is because most multi-application projects in banking have only dual applications (payment and loyalty or e-purse and debit). Once the prices of open platform products come down, they should be able to increase their shares in the banking segment. While the tremendous popularity of Java as a computing language is boosting the JavaCard's appeal to users, MULTOS has had to carry ahead on its own steam. The extra impetus is expected to come from the introduction of the MULTOS' 'step/one' program, which is expected to be a success, especially among issuers in the banking market who are looking at limited functionality. "Platform developers are optimistic about MULTOS' chances due to its ability to reduce cost of acquisition for the issuer by having a low platform payload that can run on smaller silicon chips," notes Nagarajan.

Apart from the banking segment, MULTOS is expected to take off in a big way in the national ID application segment. Hong Kong's national ID project that involved seven million cards is one of the biggest success stories for MULTOS, and with Japan recently announcing the launch of voluntary ID cards, the market is likely to enter a new phase of development. "In a unique move, the Japanese Government approved a variety of card platforms and conducted interoperability tests between them," comments Nagarajan. "The mix is most likely to contain two MULTOS, three JavaCards, and three native card products." This is a very healthy sign for the card industry, as these projects can be expected to evolve in future to accommodate more and better applications.

Events Diary 2004

August

5 - 6	Cards Australia - *Australia - www.worldofcards.biz/2004/cards_au*
4 - 6	Prepaid Markets Expo 2004 - *New York City, USA - www.prepaidmarketsexpo.com*
17 - 19	Banking Technology Africa 2004 - *South Africa - www.terrapinn.com*
25 - 26	EMV Thailand 2004 — *Bangkok - vribeiro@apsca.org*
31-September 1	Innovative Solutions for Plastic Card Production - *Seoul, South Korea - www.icma.com*

September

2 - 4	SmartCards Expo 2004/e-Security 2004. - *New Delhi, India -www.electronicstoday.org*
15 - 16	3rd Asian High Security Printing Conference - *Jakarta, Indonesia - www.cross-conferences.com*
21 - 23	EFMA Cards and Payments Conference & Expo - *Paris, France - www.efma.com/cards*
22 - 23	e-Smart 2004 - *Sophia Antipolis French Riviera - www.worldofcards.biz/2004/cards_AU*

October

5 - 9	Advanced Technology Exhibition and Conference - *Japan - info@tradefair.co.uk*
17 - 19	Banking Technology Africa 2004 Conference - *Africa*

Why do Payments on the Web?

By Patsy Everett, Managing Director, Smart Card News

Patsy Everett

Why have micro-payments on the web not progressed in the last 10 years? I remember when Mondex was launched we all thought this was the answer to enabling e-commerce over the Internet but 10 years on we are still using our credit/debit cards or setting up subscriptions to make payments. Back in 1992, when we were all enthusiastic about electronic money, a major concern for the central banks was the financial integrity of the currency whilst the retail banks were worried they would be dis-intermediated (left out) so they were not as excited about the technology as the Smart Card industry, some might even think the banks actively discouraged the technology.

Back in 1992, when we were all enthusiastic about electronic money, a major concern for the central banks was the financial integrity of the currency whilst the retail banks were worried they would be dis-intermediated (left out) so they were not as excited about the technology as the Smart Card industry, some might even think the banks actively discouraged the technology. One of the advantages of electronic money, from the banks point of view, is the float and of course the merchant would love to get rid of cash, its expensive to bank and suffers from shrinkage, but the consumer loves cash, it's a really good product. The main convenience of an electronic purse to the man in the street is in the machine environment such as vending and ticket machines but this area was not tackled in the 90's.which was mad as the electronic purse is really good for remote payments, but the concept was too early. Now that we are all Internet savvy electronic money takes on a new perspective.

We want to make remote payments but just how easy is it. We have had credit cards since the '70's, we understand the technology and up to now the card issuer and retailer has taken responsibility for any fraud, but if you want to buy something remotely under $10 it's not easy, the overheads on a credit/debit card are to high. Visa Cash with CEPS (Common Electronic Purse Specification) could be the answer, there are over 8 million world-wide, I've never seen or used one but understand that it does not require on-line authorisation or PIN and can be a pre-paid disposable card. Paypal is probably the best known payment enabler on the Internet, it works but there is a site at www.paypalsucks.com which points out that when using Paypal you have no consumer rights, there are no charge backs if your card is used by an unauthorised party and they do not publish their telephone number, making it exceedingly difficult to contact them. Apparently it takes 180 days to get your money back if you are lucky as any investigation into a fraud is investigated and judged by Paypal and they freeze your funds in the process. It also takes 180 days for them to reply to your email. Damming comments I should think. How about Gift Cards, they are a big thing in the states so it won't be long before they hit us.

The business case for these is that they can be used at any Visa/MasterCard acceptor site but again the overheads are too high for small payments because they are really just a pre-authorised debit card. How about all the innovative purse schemes of the 90's, what ever happened to them? Such names as DigiCash who filed for Chapter 11 in 1998, Beenz and Flooz collapsed in August 2001, Proton was purchased by ERG in January 2002 for A$150 million then later sold to STMicroelectronic for A$60 million, and Danmont which will come to an end next year. There are still many micropayment systems being developed and its not surprising when the Federal Reserve estimate that there are over $2 trillion cash based micro-payments made per year in the USA alone. Millicent is one based on an electronic ticket called a script which supports payments of less than a cent, Peppercoin is a small payment solution for digital and physical merchants comprised of a Small Payment Gateway which functions like a traditional payment gateway, an online customer self-care module and the Peppercoin Payment Service, which interfaces with the Small Payment Gateway to enable Universal Aggregation and of course Mondex now owned and operated by MasterCard. The big success story for small payments must be ring-tones, how come it's so easy to buy an awful, small piece of music for a few pounds but extremely difficult to buy useful information. It has to be the SIM and the infrastructure of the mobile phone operator which bills the customer account.

The big success story for small payments must be ring-tones, how come it's so easy to buy an awful, small piece of music for a few pounds but extremely difficult to buy useful information. It has to be the SIM and the infrastructure of the mobile phone operator which bills the customer account. The only problem here is the cost of the funds if pre-paid, as the retailer takes 20% of the top-up fee. Another area where small payments will be possible is through satellite TV.

In the UK SKY is the market leader with over 7 million subscribers. They have a good billing relationship with their subscribers (as do the mobile phone operators) and as David Birch of Consult Hyperion pointed out recently, SKY will be opening up their spare Smart Card slot in the set top box, to third parties. So for couch potatoes there is no need to move from in front of the TV to do their shopping or banking. With the use of a handheld remote the shopper can be identified by a unique number and their purchases can be paid for through their subscription or by using their Smart Card with an electronic purse but which purse? Will there ever be a global purse? For micropayments to be a success on the Internet there has to be a critical mass of places to use the product and a critical mass of ways to obtain it.

Smart Cards Breath new Life into Access Control Industry

By Paul Everett, Research Analyst, IMS Reasearch

Paul Everett

IMS Research predicts the transition to Smart Cards will boost demand for access controls. In recent years, the access control industry has been struggling, with capital investment in security equipment having been slashed due to the flagging European economy. However, with the European economy in a stage of recovery, and the trend to Smart Cards gaining momentum, the European access control industry is set for a return to strong growth

IMS Research predicts the European market for electronic physical access control equipment will reach 390.8 million euros in 2009, with a forecast compound annual growth rate (CAGR) of 7.6%. Recently there has been much hype about biometrics technologies but their impact on the access control industry has to date been minimal. With Smart Cards there is less speculation. 13.56 MHz proximity technology offers a number of capabilities above what the traditional 125 kHz technology offers. For example, companies can combine access control and payment systems on one card, enabling employees to use the same card to get into a building or to pay for their lunch".

In Europe much debate surrounds which technology will become the preferred Smart Card format, with Legic, ISO 14443A + B (including Mifare) and iClass vying for the number one position. IMS Research predicts that ISO 14443A + B will become the de facto Smart Card standard for access control applications in Europe. The product mix varies considerably from country to country with Legic being the preferred technology in Germany and ISO 14443A + B dominant in the Benelux region through its strong links to Philips. ISO 14443A + B boasts the largest installed base in Europe and rival technologies will find it hard to compete as unlike its competitors it is an open standard. IMS Research forecasts that by 2009 ISO 14443A + B readers will account for the largest proportion of Smart Card reader shipments within the access control industry, with 48.3% of the market. IMS cites Smart Card proximity readers (13.56 MHz) as the best growth opportunity in the electronic physical access control Market.

www.imsresearch.com