News • Smart Card News • Smart Card News • Smart Card News • Smart Card News • Smart Card News
mart Card News • Smart Card News • Smart Card News • Smart Card News • Smart Card News • Smart Ca
ews • Smart Card News • Smart Card News • Smart Card News • Smart Card News • Smart Card News
mart Card News • Smart Card News • Smart Card News • Smart Card News • Smart Card News • Smart Ca
ews • Smart Card News • Smart Card News • Smart Card News • Smart Card News • Smart Card News
mart Card News • Smart Card News • Smart C
News • Smart Card News • Smart Card News • Smart C

March 2004

Volume 13 • Number 3

Smart Card News

Smart Cards and Biometrics in Government • Finance • Health • Telecoms • Entertainment

www.smartcardgroup.com

03• *DNA ID Verification on the Cards*

09 • Bolton Teamcard to Compensate Fans on Selected Matches

04 • One Billion GSM Customers: A View from the 3GSM World Congress

11 • Sun Rising

This Month's Lead Story

02 **SmartWorldAcademy Opens in Prague**

In This Issue

Regular Features

World News In Brief

Featured Articles

3GSM World Congress

The front page of this website has been kept simple and features a selection of thumbnail photos and statistics on the shows success. From this page, the site is split in the same way the show was, into the exhibition, the fashion show and the award ceremony. Moving deeper into the site, each of these sections has an additional navigational bar which provide additional information on such aspects as exhibitor lists, press releases and show map. The website itself is very simple visually, using a standard template throughout the site. The extras within the site include photos of the show itself and an additional website index for the GSM association awards which informs you of all the winners and nominees.

www.3gsmworldcongress.com

Navigation	■■■□□
Content	■■■□□
Appearance	■■□□□

Pointsec

With GSM being a big subject this month, we looked at the Pointsec site, who deal with security for mobile computing devices. The front page of their site is very informative and displays a picture of a mobile phone running their OS system. They also have two newsreels including latest press releases and news about the company. The sites navigation bar is situated at the top of the site and is easy and efficient to use. With one click you can access information on their individual products and view pictures of their key executives. An additional function is a site map, that lays out everything on the site, at a single click of the button. Visually there are very few graphics and textual content is kept short and relevant on the site.

www.pointsec.com

Navigation	■■■■□
Content	■■■□□
Appearance	■■■□□

Hive Minded

Hive Minded claim to provide the complete Smart Card platform. However their website does not really give off much of a professional image. The site features a spelling mistake of their name and the overall impression is very dull and unimaginative. Their FAQ section consists of two line answers to only 5 questions one of which is "Does Hive Minded make Smart Cards?" - reverting stuff!!! Their navigation bar is easy to use purely because it leads to very little content. One good point is their product layout that gives fairly good, if not brief, information about what they offer. To find out more about Hive and what they offer, it is probably better to just go straight to their white papers and read the PDF's about them rather then rely on any of their web pages.

www.hiveminded.com

Navigation	■■■□□
Content	■■□□□
Appearance	■□□□□

The SmartWorldAcademy Opens in Prague

A new vendor independent training and consultancy center for state-of-the-art Smart Card applications has been opened in the very centre of Europe - in Prague, Czech Republic and will start providing courses to interested system integrators and solution providers in March 2004. The center is owned and run by ACG Identification GmbH, a component and technology supplier in the Smart Card and RFID markets. The SmartWorldAcademy will specialise in software issues for high-end Smart Card technologies, address the needs of system integrators, card manufacturers and solution providers from every part of the world, who need to stay abreast of the changes in the rapidly evolving world of micro-controllers for Smart Cards.

"For a long time, the GSM SIM market has been by far the largest and fastest growing segment of the microprocessor Smart Card market. As the GSM market itself is dominated by a modest number of large telecommunications companies and these companies typically source the GSM SIM cards only from the large card manufacturers, this market segment has helped to widen the gap between the small group of large card companies with a complex portfolio and the large number of smaller independent players, who are practically unable to enter the GSM SIM market in the developed markets. In the 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 tachograph project and a few others." stated Petr Novak of ACG on what had been the driving forces behind the creaton of the SmartWorldAcademy.

The academy offers general and bespoke courses for around 250 Euros, giving an overview of available technologies, market trends and required know-how to enter the specific segments of the market. The majority of the courses concentrate on various card operating systems which are licensable independently of the large card manufacturers. The courses focus on the understanding of the relations among the different components and technologies and on practical hands-on work with real life example applications. The more specialised courses will cover specific market segments or technologies, such as the current EU Tachograph, ICAO Machine Readable Travel Documents and other complex technologies. The training centre showcases real product offerings of micro-controllers and operating systems, providing the technical infrastructure and expertise for technical platform evaluation and customer pilot projects realisation.

Oberthur Reports Fourth Quarter Results

The new sequential growth during the fourth quarter of 2003 confirms the dynamism of Oberthur Card Systems' business. Oberthur stated in their forth quarter results that they have achieved sequential sales growth of 14.6 % in the fourth quarter of 2003. It is the company's best quarterly performance in the past two years. This growth was spurred by the payment market - where Oberthur has reinforced its leadership - and the mobile communications market, with a sustained demand for high-end cards. Second half 2003 sales - 229.0 million Euros - increased by 13.9% vs. the first six months of the year. Oberthur's revenues for the fourth quarter 2003 reached 121.4 million Euros, increasing by 8.5% before parity impact on a year-on-year basis. Compared with the previous quarter, sales increased by 14.6% at constant exchange rates.

The sales growth came mainly from microprocessor cards, showing a 16% sequential growth with 37.5 million cards delivered. In the payment market, Oberthur has fully benefited from the accelerated migration to microprocessor cards in the United Kingdom. This enabled an all-time delivery record of 15.2 million cards during the quarter.

Mobile communications benefited from both the company's technological edge in high-end cards and the dynamism of the market. In this segment, Oberthur also realised its best performance in the past two years with 18.6 million cards delivered. The company remains focused on high-end segments since cards with 32k or higher capacity represented over 85% of sales. Average selling prices experienced a new sequential increase (+3%) with 64k and 128k cards accounting for more than a third of sales.

ActivCard Reports Fourth Quarter Financial Results

ActivCard Corporation released their financial results for the quarter and year ended December 31, 2003. ActivCard revenues for the fourth quarter were $6.7 million, compared to $12.1 million reported in the fourth quarter of 2002. Net loss for the quarter was $9.4 million, or $0.22 per diluted share, compared to a net loss of $9.2 million, or $0.22 per diluted share in the fourth quarter of 2002. During the fourth quarter, ActivCard also increased their ownership of ASPACE to 49% of the voting control.

Gemplus Reports Fourth Quarter and Full Year 2003 Results

Gemplus International S.A. have released the results for their fourth quarter and full year ended December 31, 2003. The company's fourth quarter revenue shows year-on-year growth in the Americas of 54.7%, 20.6% in EMEA and 22.0% in Asia. Their Gross margin increased by 0.4% point compared with the third quarter 2003.

This was led by overall growth in Telecoms and an improved mix in wireless, which fully offset selling price decline. Improvement in the Company's underlying profitability during the fourth quarter is best seen in the gross cash flow for the quarter, which was 28.6 million euros, before restructuring, compared with 11.5 million euros for the third quarter.

Payment microprocessor card shipments rose 42% year-on-year, but declined 29% quarter-on-quarter. EMV shipments increased 50% quarter-on-quarter. Sales were mainly driven by the UK market, but were also supported by South America and Malaysia. Government ID & Corporate Security solutions revenue increased 30% quarter-on-quarter led by successful acceptance tests and shipping of the first batch of ID cards to the Royal Oman Police.

Nottingham Freedom Smart Cards Aim to Go Nationwide

The Smart Card-based travel scheme in Nottingham, UK, is planning to make their scheme nationwide throughout the UK. Nottingham county is to receive a majority share of a £1.3m funding grant by the UK Government to see if their electronic travel cards can be adapted and used on integrated transport throughout the country.

For the past two years, Nottingham Freedom cards have been issued to 100,000 school children and concessionary bus pass holders in the county. Now Nottingham, Cheshire and Southampton are to carry out a pilot project to convert their electronic card schemes to the same national standard.

The Government wants people to be able to move between different types of public transport, without having to buy separate tickets - an idea backed by the rail watchdog, Strategic Rail Authority.

World News in Brief

Bolton TeamCard to Compensate Fans on Selected Matches

Bolton Wanderers FC, a UK domestic football club, has announced that they are using their Smart Card based season ticket, TeamCard, to compensate fans who cannot attend big games. This Smart Card currently allows fans to attend matches by using their cards at the turnstiles for access to matches. The TeamCard also allows the club to monitor any ticket abuse. The club is running a scheme that provides season ticket holders with £10 worth of loyalty points which can be used for tickets, merchandise and even food at the clubs restaurant.

This offering is available to fans who give up their seat for any of the four main "Big Match" games. The plan is to later develop this scheme to cover all of Bolton's matches. The club benefits from these loyalty points for selected match seats by reselling the seats to non season ticket holders.

Hive Minded Delivers Smart Card Platform

Hive Minded, Inc. has announced the availability of version 1.1 of its Nectar Smart Card Platform, for the first time bringing ECMA certification to the Smart Card development platform. The Nectar Smart Card Platform allows developers to easily build next generation applications on the smart card platform. With support for Microsoft .NET technology on the Nectar platform, developers can write an application for a Smart Card using Microsoft Visual Studio .NET 2003, remain fully compatible with the Microsoft Windows environment, and can take full advantage of integrating smart card solutions with Web services.

Microsoft Demonstrate Gemplus Smart Cards for Network Security

Gemplus International S.A., a provider of Smart Card solutions, has announced the delivery of Smart Cards, readers, and software to Microsoft for use in the Microsoft Technology Centre's situated in 5 locations around the world. Microsoft will use Gemplus technology to demonstrate to clients the integration and implementation of Smart Cards in a Windows-based environment for network security.

The Microsoft Technology Centers will use Smart Cards, PC-link readers, and software from Gemplus's SafesITe solution. SafesITe provides customers and system integrators with all the products (cards, readers & software) and services necessary to seamlessly deploy multi-purpose employee cards as part of an organization's existing infrastructure. SafesITe supports Microsoft Windows.

IntegriHealth Introduce Smart Cards to Tackle Rising Health Costs in Africa

IntegriHealth, an African health management centre, has announced a new corporate Smart Card based product to deal with the Aids pandemic which is causing an increases in health costs for employers throughout Africa. Dr Ernest Mureithi, Managing Director of IntegriHealth, has stated in an interview with Business Week "IntegriHealth management will introduce into the market an Aids corporate product to provide education and training beyond awareness to employees and leaders, combine Aids education with on-site VCT, impact assessment on organisations, its clinical management and the monitoring and evaluation of effectiveness and adherence of clinical management,". If this electronic monitoring scheme is chosen by an organization the staff will be issued with an electronic monitoring Smart Card. This Smart Card will be held by an appointed medical care provider and all information will be held on this allocated Smart Card in the strictest confidence.

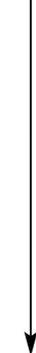## Smart Cards Renew Residence Permits in Qatar

Dr Ahmed Hamad Al-Mohannadi, Qatar's e-government director, has announced that Qatar's e-government project has made the Ministry of Interior (MoI) the Certification Authority (CA) for e-government transactions.

World News in Brief

Smart Cards will be provided to select e-government users, mainly companies in a bid to start renewing residence permits (RP). The plan is to allow companies the ability to renew the residence permits of its employees through the e-government portal using the Smart Card. The long-term plan is to provide Smart Cards to all nationals and residents of Qatar. Smart Cards will replace the identity cards issued to Qataris and expatriates now.

Target Remove Chips from Visa Smart Card Program

Target Corp., a US retail giant, has announced plans to phase out the use of the computer chips which were embedded in their Target Visa Smart Cards. The Smart chips where used to download and store discount coupons that could be cashed in at Target stores. While these type of Smart Cards have been popular in Europe, they have been slow to catch on in the United States.

The implementation of these Smart Cards cost Visa and Target around $50 million to develop and roll out. Since its launch in 2001, Target's Visa program, has been issued to 9 million accounts, and has become a large profit generator for the retailer. Through this Target aims to keep its Visa program but wish's to drop the chip facility. The company will also continue to support Smart Coupons and will aim to build them into a new loyalty program.

Mr. Aneace Haddad, president and CEO of Welcome stated "I never thought that the Target experience related much to U.S. banks. The bankers say, "I'm just a bank, not a retailer." Since Target is a retailer plus a bank, this program never resonated with a lot of U.S. banks. It was really a one-off. Initially, the banks outside the U.S. were watching and waiting, but eventually they also wrote it off as not relevant."

"This event doesn't impact onSmart Cards in the United States, because the impact has already happened. Fraud hasn't reached the same levels here as in other parts of the world. Chip won't take off in the U.S. market until fraud becomes an issue and banks are faced with the same problems as banks in Asia, Europe and Latin America. When that happens chip will be the solution - whether it's contact or contactless."

French Bank Société Générale in EMV Migration

Gemplus International S.A.,have become the first company to begin personalisation of EMV payment cards for the French financial market with the production of EMV-compliant payment cards for Société Générale, one of the largest financial services suppliers in the Euro zone. Working closely with Société Générale and GIE Cartes Bancaires, Gemplus began production of B0'-EMV cards for Société Générale on 6th January 2004. Gemplus has been a key partner of Société Générale for many years, when payment cards issued in France were based on a domestic payment application coded inside the Smart Card chip, named B0' .

MasterCard Reports Strong Growth in 2003

MasterCard International have stated strong performance results for the fourth quarter and full-year 2003, demonstrating continued growth across almost all regions and in key measures of success in the payments industry. Worldwide, cardholders used over 632.4 million MasterCard branded Smart Cards for almost 15 billion transactions during 2003, generating gross dollar volume (GDV) of $1.27 trillion, an increase of 5.9% on a local currency basis, and 10.4% on a U.S. dollar basis, over 2002.

In 2003, 150 million branded Smart Cards were issued worldwide, more than half of them carrying value-added applications like loyalty, digital ID, e-ticketing, e-coupons or personal data storage. A fast growing percentage of these cards are EMV compliant, demonstrating the increasing momentum for EMV compliance. At the end of 2003, MasterCard said they were working with their customers on more than 400 individual chip implementations around the world, more than double the number of active projects at the end of 2002.

DNA ID Verification on the Cards

DNA Bioscience, who provide DNA paternity and identity services , has launched the UK's first DNA Reference Card in response to demand from its clients. The current debate about National Identity Cards has raised the spectre of DNA based biometric ID cards providing a genetic fingerprint for every UK citizen.

"While the ownership and use of DNA information highlights many important civil liberties issues, this should not be allowed to overshadow the real benefits offered by DNA profiling," said Avi Lasarow, Director of DNA Bioscience.

EU Discuss Biometric Passports

During a European Parliament public hearing on biometrics in Brussels, Belgium, this month, Justice and Home Affairs Commissioner Antonio Vitorino has defended proposals to include biometric information for use in EU passports. The current issues being discussed are over the protection of personal data and the costs involved. The Commission aims to include digital facial images and possibly fingerprints on all EU passports.

They have also suggested the possibility of the creation of a register containing the fingerprints and other relevant data of EU passport applicants. However there are concerns that the technology could be used for EU-wide surveillance by security agencies, Brussels argues that the real question surrounding databases is getting the legal framework right. After October 2004 EU citizen's will require a visa to travel to the US if they do not have biometric data on their passport.

However Mr Vitorino stressed that the EU is responding to the standards set by the International Civil Aviation Organisation (ICAO), and not by the imposed deadline set by the US. Europe is not expected to introduce this technology until at least 2006.

Byometric System for Border Control at Frankfurt Airport

Byometric Systems GmbH and Oki Electric Industry Co., Ltd. are set to provide an iris recognition system for biometrics-based border checks at Frankfurt/Main Airport. This system is part of the Automated and Biometrics- based Border Checks initiative, a multinational pilot project involving 18 European nations, led by the German Federal Ministry of the Interior and Federal Border Police.

Requiring an individual only to stand in front of it, the system recognises that individual's iris pattern and confirms his/her identity, offering a simple, convenient alternative to traditional border checks.

CATSA Pilot Project for Canadian Airports.

After a competitive bid process, the Canadian Air Transport Security Authority (CATSA) has chosen ACME~Future Security Controls to develop a comprehensive solution for the operational trials of CATSA's restricted area identification card (RAIC) project to improve security at Canadian airports. ACME~Future Security Controls informed Bioscrypt Inc., a provider of identity verification technology, that it would incorporate technologies from Bioscrypt, Cross Match Technologies, HID and LG Electronics to develop a comprehensive solution for the operational trials of CATSA's restricted area identification card (RAIC) project. The RAIC will be using biometric technologies to create a secure credential card for individuals accessing restricted areas of airports. The RAIC initiative will also involve a central database to verify the validity of any card issued in Canada. The first phase of the RAIC program will be implemented as an operational trial deployed at selected airports and will involve approximately 40,000 workers. The program will eventually involve up to 150,000 workers.

SIM Chips Track al-Qaeda Terrorists

An article in "The New York Times" has shown that al-Qaeda, Osama bin Laden's network, and other terrorist groups are using pre-paid Subscriber Identity Module (SIM) cards to coordinate their activities. Investigators said that terrorist organisations favoured the SIM cards made by Swisscom of Switzerland. The SIMs carry prepaid minutes and allow a mobile phone to be used anywhere in the world.
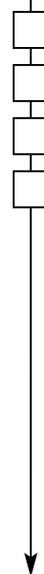
World News in Brief

This specific chip was used because terrorists could buy the chips without giving their names. Once the authorities discovered that this Swisscom chip was being used, investigators were able to track the conversations and movements of several al-Qaida leaders and dozens of operatives.

In March last year, authorities in Pakistan began to monitor specific phone numbers. This led to the arrest in Rawalpindi of Khalid Shaikh Mohammed, one of the most wanted men in the world, who is accused of masterminding the September 11 attacks in the United States. His computer and mobile phones contained 6,000 numbers that the authorities used to track suspected terrorists. In April 2003, authorities in Indonesia broke up a terror cell after investigators traced the destination of many of the calls Mohammed had placed before his arrest. Shortly after it first transpired that al-Qaeda operatives had used the cards, the Swiss parliament approved a law prohibiting the sale of SIM cards without registering personal details.

100% Flash based Smart Card IC

EM Microelectronic, a provider of RFID circuits, Smart Cards and ultra-low power microcontrollers, has announced the EMTCG256-3G, a unique flash memory-based Smart Card IC designed for use in SIM and Java cards for GSM mobile phones, as well as for banking, healthcare and loyalty card applications. The EMTCG256-3G is compatible with the ISO7816-3 Integrated Circuit Card (Smart Card) specification, and operates with power supplies from 5V down to 1.8V, making it compatible with the latest generation of ultra low power GSM cellular telephones. Memory flexibility is a key advantage of the EMTCG256-3G, which contains 256kB of pure flash memory. Most Smart Card ICs rely on a combination of ROM and EEPROM.

Barcelona FC gets ScanZone Technology

Scanbuy, Inc., a software company dedicated to developing bar code commerce solutions, has equipped Barcelona Football Club with ScanZoom technology. ScanZoom enables mobile camera phones to launch services and applications simply by taking a photo of a barcode. ScanZoom is being used as part of the ID card program for the club's 112,000 season ticket holders.

Barcelona Football Club successfully deployed Scan-Zoom for the first time at a Spanish League football match against Athletic de Bilbao on January 17, 2004.

Gemplus Launches GemConnect MySIMeditor For SIM Management

Gemplus International S.A.,has launched the Gem-Connect MySIMeditor, a SIM management solution targeted at corporate and consumer segments. Two European operators have already adopted this solution. GemConnect MySIMeditor contains software that enables the user to manage their SIM content through a computer interface.

The SIM is inserted into a cardholder that connects to a PC via the USB portal. Data can then be uploaded and downloaded at the convenience of the end-user. In a recent survey conducted by TNS Sofres, 200 end-users in three European countries (UK, Germany and Sweden) were asked if they considered the managing of their SIM card contents via their PC interface a useful service. The results were extremely positive with an average of 67% finding this solution useful.

Iranians Queue up for Mobile Phone SIM Cards

The mobile phone market in Iran is very big business. Hundreds of thousands of Iranians have been laying siege to post offices and banks to sign up for the latest issue of mobile telephone SIM cards -- even at the sky high price of $530 apiece. Even though the SIM cards on offer will not be released for a year and cost a small fortune and customers will still have to pay for the telephone and existing lines bought on the open market cost more than double.

With the present rate for a SIM card currently hovering around the $1,200 mark, any new lines are highly sought after. Just three million mobile phone lines are currently in service. According to figures from the Post and Telecommunications Ministry, a quarter of a million new lines were sold in the first 48 hours after sales opened -- the equivalent of $390 million. In addition, on average each customer appeared to be buying up between 10 and 15 lines each -- a sign that the mobile phone market, like the car and property sector, has become a key form of investment.

7

One Billion GSM Customers: A View of the 3GSM World Congress

By Patsy Everett, Managing Director, Smart Card News Ltd

The 3GSM World Congress was held in Cannes last month and attracted over 29,000 people with 560 exhibitors from around the world. For me the two major events were the fashion show (see page 18) and the awards evening. The GSM Association is responsible for the awards, which are in their 9th. year and aim's to honour people, organisations and companies that deliver new ideas, methods or new technology which will improve customer relationships.

Patsy Everett

There are six categories, Technology Innovation, which was awarded to Sony Ericsson for their T610, and the Argogroup for their Monitor Master User Experience Optimisation Platform. The Applications and Services award was won by the Vodafone Group for their Mobile Connect Card and Smart Communications for their Smart Load and Valista. The Marketing and Promotion award was won by Telecom Personal S.A for the "CUBE" and T-Mobile International for re-branding VoiceStream to T-Mobile. The Mobiles in the Community award went to O2 and "Milly's Fund" for Teach UR Mum 2 TXT personal safety campaign and WideRay Corp. for the Uganda Health Information Network. The GSM Association Chairman's award and the Best-in-Show award.

Craig Ehrlich, the GSM Association Chairman awarded China Mobile Communications Corp. his award commenting that China Mobile had played and continues to play a leading role as a driver of GSM growth. The EMC World Cellular Database reckons that China Mobile has 69% of China's GSM customer base of 240.4 million and 64% of China's total mobile market. The Congress also celebrated the fact that there are now one billion GSM customers world-wide, this exceeds the number of fixed telephone lines globally.

It would appear from the number of conversations SCN had at the congress that there is an increasing concern about security. The mobile operators do not want the industry to go the same way as the Internet. The mobile commerce market has been valued at $20 billion and in a white paper, Deutsche Bank valued global revenues of GSM at $277 billion for 2003 and forecasts revenues of $500 billion by 2005.

Consequently a number of companies are working on secure biometric signatures and securing sensitive data. It would appear that some companies are not happy with the "fit for purpose" scenario any longer although they may yet discover it's the only economical solution. Another area of great interest was the use of the phone as a tracking device with the safety of children very much in mind. Anti-spam and pre-screening of content and images was very much in evidence but one of the busiest small stands was live streaming sex shows, as well as ways to pay with the phone.

The exhibition was well run and planned with exciting stands, large crowds of people and the yachts were busy with drinks parties. I will go again.

Event Special

Sun Rising

By Jason Smith, Production Editor, Smart Card News Ltd

Sun Microsystems was incorporated in February 1982, with just four employees and by 1988 they had achieved $1 billion in revenue, which was the fastest rise ever for a computer company. In 1993 Sun made its debut on the Fortune 500 and in the same year reached the incredible milestone of one million systems shipped. In 1995 Sun proceeded to introduce the first universal software platform, designed from the ground up for the Internet and corporate intranets. This new piece of technology was branded "Java technology" and it enabled developers to write applications once to run on any computer.

Jason Smith

By 1997 this Java technology was being used by NASA engineers to develop an interactive application allowing anyone on the Internet to be a "virtual participant" in the space administration's groundbreaking mission to Mars. A year later Sun produced the next generation of Java technology - "Java 2 s". This new software delivered more speed, more flexibility, and a complete set of foundation classes. By 2001 more than 2.5 million programmers were developing innovative Java applications. Nowadays Java technology appears to be everywhere. Sun currently estimates that 1.5 billion devices around the world are powered by their Java technology.

Java technology to-date powers everything from secure identity cards to mobile phones, printers, Web cams, automobile telematics, desktops, medical equipment, servers, jet engines and more. Sun estimates more than 470 million Java Cards have been deployed globally. Besides mobile phones, the technology is commonly used in multi-purpose citizen identification cards such as the 22 million healthcare IDs issued by the Taiwanese authorities.

"The costs and risks of viruses and identity theft have become everyday issues for CIOs and individual consumers. As a result, the community has increasingly turned to Java technology because of its ubiquity and security to protect both data and services," said Jonathan Schwartz, executive vice president of software, Sun Microsystems. "This installed base presents a huge revenue opportunity for developers, service providers, device manufacturers, and operators and its continued growth keeps the community healthy and creative." Current Java technology-based digital identity Smart Card deployments include;

Jonathan Schwartz

❑   National Aeronautic and Science Administration: NASA is planning to issue a Java technoogy-based "One NASA" Smart Card to increase agency security and simplify security management. The Smart Card helps ensure advanced levels of identity assurance and enables consolidation of all employee and contractor access cards into a single card for entry to NASA centers, facilities or computer systems. Beginning with trials at the Marshall Space Flight Center in Huntsville, Alabama, NASA expects to ultimately deploy more than 100,000 Smart Cards by the end of 2005.
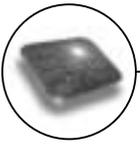
❑ Government of Thailand: Simplifying access to government services and protecting against identity theft, the Thai government will begin issuing the first of 62 million Java technology-based Smart Cards to its citizens and government representatives during April 2004. The multi-function ID cards are designed to contain personal ID, fingerprints, tax, social welfare and social security numbers, agricultural data and healthcare data. Using the ID cards, citizens will be able to access government services at e-government kiosks nationwide and by Smart Card readers integrated into desktop computers.

These new wins for Sun have allowed them to build on the Java technology handset momentum, currently deployed by 77 operators worldwide including AT&T Wireless, China Mobile, China Unicom, Cingular Wireless, NTT DoCoMo, Orange, T-Mobile, Vodafone, and many others.

In the mobile data services market, compelling new content has brought 2.5 and 3G networks to life worldwide, operators have standardised on Java technologies in handsets to power mobile data services and GSM SIM Cards to authenticate network access and SIM-based applications.

Java technology-based Smart Cards are also being adopted by many corporations and governments for identity solutions. In the traditional computing market, the growth of alternative desktops and the user requirements for Java technology have led to many new desktop licensing agreements, while the expansion of Java Web services is driving the adoption of the Java platform from server infrastructure to the edge of the network.

"Java technology is making mobile data services happen, it's everywhere. From the data center to the device to the latest mobile Java Web services, it is clear that the Java platform is the platform of choice for open and secure mobile services," said Alan Brenner, vice president of consumer and mobile systems group, Sun Microsystems, Inc., at the 3GSM World Congress 2004, Cannes, France.

"Sun is providing solutions for the entire mobile ecosystem - infrastructure products, handset implementations, development platform, and go-to-market solutions - enabling operators, device manufacturers and developers to securely connect everything and everyone on the planet to the network." Sun's new products, programs and partnerships deliver new mobile data revenue generation opportunities to all members of the wireless industry. With 250 million Java technology-enabled mobile phones from 31 manufacturers deployed in 77 operator networks and a half-billion Java Card secure digital identity deployments in Smart Card and mobile phone environments.

Java technology appears to continue to grow as the number-one content platform for mobile data services. The available technologies provide content vendors and carriers with a rich and secure mobile data services platform to realize increased average revenue per unit (ARPU) through compelling applications and services. The market has seen a recent explosion of innovative new wireless services and applications built using Java technologies for 2.5G and 3G mobile phones. Enterprises are also beginning to extend their infrastructure to mobile employees and customers to realise operational efficiency and increased revenue opportunities.

The future continues to be bright for Sun.

www.sun.com

An IT Manager's Insight into Mobile Security

By Magnus Ahlberg, Managing Director, Pointsec Mobile Technologies

Mobile security is a hot issue, but who is listening? Who really cares? The mere word of security sends most people running. Investing in preventative IT security has never been a very popular topic. Most board directors clam-up and switch off at the words "Your company could be at risk if you don't invest in XXX technology". It's a hard sell for IT managers and it often takes a competitor or themselves to become a victim of crime before they sit up and listen. Users too are very lazy and complacent when it comes to IT security - they don't value the information they carry around with them and most are just too busy to worry about anything further to complicate their lives.

Magnus Ahlberg

This was made very clear in the Mobile Usage Survey conducted by Infosecurity and Pointsec which found that a third of users don't bother protecting their mobile device with a password even though they store highly confidential company and personal information on them including all their other passwords, PIN numbers and bank details.

Surprised by these figures? I doubt it! If you're an IT manager you'd have been there. In-fact you're users have probably lost more laptops than you can remember? Surveys show that any large organisation lose's between 3-5% of their laptops every year. Relaying laptop theft stories in the local pub is almost as common-place as people boasting how much their houses have shot-up in price over the last two years. However, with an increasingly mobile workforce, often using privately bought mobile devices, the board and IT departments have to take greater notice of who is carrying what around with them and take a rain check of the damage that could be caused if this information was lost and broadcast to the outside world. It is often fine when company information just resides on PCs and servers in an office as the IT departments have far greater control over the information and what is being sent out. Now the same information is being carried out of the office, left in bars or restaurants, at the back of taxis or trains and most commonly forgotten in airports, the IT manager has a nightmare job on his/her hands.

Insuring against hardware theft is rapidly becoming pointless and expensive and few companies bother to take out policies because the premiums are now so high. Plus, companies are now realising that the true cost of a stolen item of hardware is not the device itself, but the information it contains. No companies are without laptops, PDAs or smartphones these days, so if you want to make sure your company does not become another statistic or victim of data theft here are a few golden rules you may want to follow.

Golden Rule Number One: You must have a mobile Use policy or ensure that your corporate IT security policy has specific provision for mobile devices and you update it whenever you adopt new hardware categories such as combined PDA/phones. The information that needs to be protected is the same, it is just a different way of storage.

Golden Rule Number Two: Take the responsibility of IT security away from the end-user and centrally manage and deploy it. Work on the premise that no-one can be trusted to safeguard their device. Wake up to the fact that they are just not interested in security.

Golden Rule Number Three: Invest in a solution which is usable and flexible. Easy access and transparent encryption that does not slow down a user's device is now available on the market- user's will go to whatever measures to disable the device or buy their own if security gets in their way.

Golden Rule Number Four: Have a blanket approach to security by owning every mobile device that leaves your office and make access control and encryption mandatory. DO NOT allow users to use their own mobile device to store company information. Don't be fooled into believing that they are already protecting their devices with the "factory" password settings or encryption. Nine times out of 10 they won't be. Record the serial numbers of all PDAs and similar devices including memory cards.

Golden Rule Number Five: Be realistic with passwords - Users hate them! An enforced, long and difficult password will result in them writing it down or forgetting it. If they can choose themselves, they will pick the easiest passwords they can such as their pet or child's name, anniversaries or birthdays. You bet after a long Christmas holiday or annual leave they'll make a call to the helpdesk to ask for a reset. One way around this is to dispense with the idea of passwords altogether. Pointsec has, for example, presented a new idea with their PicturePIN access control which consists of a series of pictures chosen by the user from a randomly displayed, larger gallery. Instead of having to remember a password in order to access his encrypted information, the user simply points out the pictures corresponding to "his" story. Not only is this system just as secure as traditional passwords, but there are other advantages too. Its novel, so there's more chance that people will want to use it. Plus, visual images are much harder to forget than faces. There is even a possibility to add your own pictures for your organisation. And just in case the user is tempted to write down his "password", he'll find it very difficult to do so. So the thief who steals a machine and expects to find the password for the encrypted drive written on the base of the device is going to be sadly disappointed.

Golden Rule Number Six: Become a realist - but still endeavour to educate your users! Accept the fact that users won't take a blind bit of notice of security, however, don't give up - send them a mobile security user policy - make them sign and return it by getting HR to work this policy into their appraisals. Try and make them streetwise but accept that they will still leave their mobile devices in the car, in airports and have them pick-pocketed in crowded places. Nothing can be guaranteed, but by following these rules, you can show that you have taken adequate steps to protect your organisations information and hopefully rest at night, safe in the knowledge that when thousands of mobile devices get lost or stolen this year, yours won't be the one hitting the papers with embarrassing and expensive consequences.

www.pointsec.com

Events Diary 2004

March

30 - April 1	ISC West Conference - *Las Vegas, USA*
30 - April 1	ASIS Emerging Trends in Security Conference - *Renaissance Hotel, Chicago, USA*

April

5 - 6	Vouchers & Smart Cards in the Modernisation of Public Transport - *London - www.symposium-events.co.uk*
6 - 8	Card-Ex 2004 - *Cairo, Egypt*
21 - 23	Cards Asia 2004 - *Singapore*
26 - 29	CTST 2004 - *Washington, DC - www.ctst.com*
27 - 29	Infosecurity Europe 2004 - *London - www.infosec.co.uk*
27-28	The 17th Lafferty Cards and Payments Conference & Expo - *Barcelona, Spain.*

May

5 - 7	Thomson Media 16th Annual Card Forum & Expo - *Renassance Orlando Resort, Orlando - www.tmconferences.com*
11 - 12	Ticketing for Transport 2004 - *London - www.iqpc-transport.com*
12 - 14	6th Smart Cards + Smart Label China - *Shanghai - wwwscfc.org.cn*
17 - 19	Cards Middles East 2004 - *Dubai - www.worldofcards.biz/2004/cards_AE*

12
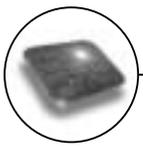
Why Should Card Issuers Care About Changes in Manufacturing?

By Bill Knotts, President, Spartanics

Most card issuers probably aren't aware that the equipment card manufacturers use affects them. However recent developments in card manufacturing technology now make it possible to reduce costs and to get a faster turnaround time on orders. Due to the growing differences in how card manufacturers are equipped, it is important for card issuers to be aware of new developments in the marketplace and how they can affect the costs and delivery times of their orders. One of the most recent developments is a new 10-up card punching system that can more than double card output by punching a larger number of cards in one press stroke than ever before possible. Older systems can hold dies that punch from 1 to 5 cards at once. At their best, these systems could produce up to 35,000 CR80 cards an hour. With the newer card punching systems, they can accommodate dies that punch from 6-10 cards at once and can produce up to 70,000 CR80 cards an hour - twice the output of older systems. However this doesn't mean that the newest 6-8-10-up systems automatically cost twice as much. pIn terms of cost vs. output, these systems provide the best value. A 3-4-5-up card punching system that can produce up to 35,000 cards per hour costs anywhere from $130,000-$230,000. On the other hand, 10-up systems that can produce up to 70,000 cards an hour costs $260,000-$300,000.

For card manufacturers who have sufficient customer demand this means faster turnaround time and decreased costs, savings that can then be passed on to card issuers. Basic design considerations are important when it comes to card punching equipment, because this has an effect on throughput, especially when breakdowns occur. Only top of the line card punching systems have a modular design that allows the malfunctioning part of the equipment to be removed and replaced with a loaner module from the manufacturer when breakdowns occur. While the broken part is shipped to the manufacturer, repaired and returned, the equipment keeps operating throughout, using the replacement part. The modular design of these card punching systems ensures continuous uptime even in the event of a breakdown for card manufacturers, and on time delivery to issuers. For card issuers, this also means that it takes less time for new products to go from concept to finished piece. New cards in different shapes and sizes are being offered to consumers by card issuers every day in an attempt to gain market share. By shortening production time, the 10-up card punching systems help new cards get on the market as quickly as possible. Some card issuers may think that with increased throughput comes a decrease in quality and precision. However this is not the case with the top of the line card punching systems. In fact, the only systems that can achieve the 70,000 cards per hour throughput use optical registration to correct in 3 axes (X, Y and Theta) with every press stroke within +/-0.1mm or better. As an added benefit of the precise registration, fewer defect products are produced due to punching errors, and material wastage is reduced.

Card issuers that demand the highest quality cards should also be aware of other card manufacturing equipment that can help achieve the highest quality possible when added to a manufacturing operation. For example, the best automated inspection equipment not only guarantees unfailing card integrity but it is faster and more reliable than human inspectors. These systems can fully inspect up to 36,000 cards per hour and requires only one run to guarantee 100% inspection. While mistakes are inevitable and standards can be somewhat subjective where manual inspectors are concerned, top of the line automated card inspection systems apply the same standards to each and every card. They use a sample set of approved, defect-free cards and set them as the example for all other cards going through the system to be judged by. The system then catches all the cards that fall outside the acceptable range. The best automated inspection systems can not only monitor color and defects from edge-to-edge, but can also check for missing holograms, signature panels and magnetic stripes. Card manufacturers that use systems such as these can guarantee card issuers that they are getting 100% accuracy on all orders. No amount of careful human inspection can match the level of accuracy provided by fully automated inspection systems.

opinion

14

Over time, the cost of employing human inspectors is actually more expensive than using automated inspection equipment. Card manufacturers can cut inspection costs by a minimum of 75-80% by transitioning to automated inspection systems. As with the 10-up card punching systems, these savings can then be passed on to the card issuer. Card issuers in-the-know are aware of how these new developments equal lower prices and faster turnaround times. Advances in manufacturing equipment do not just affect card manufacturers, but have an impact on costs and delivery times for card issuers as well.

Who's Accessing your Information?

By Jason Smith, Production Editor, Smart Cards News Ltd

One in five of the UK's larger companies suffered security breaches of their information systems in the last year because of weaknesses in their approach to identity management. This information is one of the key, initial findings from the 2004 Department of Trade and Industry's biennial Information Security Breaches Survey, conducted by a consortium led by PricewaterhouseCoopers.

Jason Smith

The survey covered 1,000 companies and discovered that roughly one in ten large companies, within the UK, had faced a significant fraud or breach in their level of confidentiality. More than half of all companies affected said that this problem was their worst incident of the year, even outweighing virus infections. Confidentiality breaches cause significant business disruption (for more than a month in 15% of the cases) and took significant staff time to investigate, on average 10-20 man-days. These breaches also incurred the biggest direct cash cost of any security incident - more than £100,000 in legal fees, investigation costs and fines in 15% of cases. The report lays out that it is the access controls of the Companies that are failing to prevent these incidents.

The first root cause of this is that often the sheer number of users and systems puts user administration processes under strain. To counter this, companies are increasingly automating their processes for granting access to systems. 16% of all companies and 31% of large ones do this. Automating user provisioning appears to work. None of the respondents that had done this had suffered financial frauds or systems penetration from outside in the last year The second root cause is over-reliance on passwords to check users' identity. Some 87% of all companies rely solely on user ID and password, while worryingly 7% have no controls at all. Businesses that adopt single sign-on without strong authentication had a higher than average incidence of unauthorised access. Tokens, Smart Cards and biometrics are only used in 6% of companies. This rises to roughly a quarter of the large businesses. The latter seem to be reaping the benefit with just 3% suffering from an unauthorised access breach compared to 20% for those that haven't adopted these levels of authentication. These root causes are identified in a fact sheet entitled 'Identity Management' sponsored by Entrust who are a provider of identity and access management solutions.
]
Chris Potter, the PricewaterhouseCoopers partner leading the survey, said "Companies have traditionally been poor at setting up new users and deleting leavers from their systems. We are increasingly seeing businesses automate these processes. While most businesses over-rely on passwords, large organisations are also starting to adopt strong authentication methods such as Smart Cards and tokens to check users' identity. A comprehensive approach to identity management includes strong authentication, access control and provisioning. The results of this survey clearly demonstrate the benefits early adopters have gained in terms of reduced security incidents." Philip Richardson, vice president, Northern Europe, Middle East and Africa, Entrust, added "It is amazing that one in five businesses experienced a security breach in the past year as a result of weaknesses in their approach to identity management when the technology needed to reduce this risk is now so readily available. However, the message seems to be resonating with senior executives and Board-level directors. Decision-makers are not only becoming more aware of the potential disruption and damage that security breaches can cause to business, but also that there are new information security governance concerns presented by the changing regulatory landscape."

Market in Figures

14

Biometrics and Identity Verification in Payment Environments - Ready for Prime Time?

By Nick Holland, Director of Emerging Technologies Advisory Service, Mercator Advisory Group - www.mercatoradvisorygroup.com

Nick Holland

The rapid evolution of electronic payments has driven the demand for increasingly complex keys and locks. Traditionally, access has been controlled by 'something you have'; keys that unlock doors to controlled physical spaces. As the emphasis has shifted from protecting physical spaces to logical ones, the keys have also morphed into many shapes and forms, including magnetic stripe cards, RFID key fobs and SIM cards. These can be grouped under the collective heading of 'tokens'. However, tokens can be lost, stolen or duplicated. Another age-old system of entry is to provide 'something you know' to someone on the other side of a door; such as a word or a phrase.

Electronic equivalents have become a core method of entry to systems, so much so that we are required to remember, on average, twenty one separate passwords to access our networks, email and bank accounts. Herein lies the problem; 'something you know' can be and often is forgotten, or for convenience the same password is used on multiple occasions. Compounding the problem is that passwords are often written down, making them available for interception and unauthorized usage. In short, they have the same vulnerabilities as tokens; they can be lost, stolen or duplicated. Biometrics provide alternatives for ID authentication; 'something you are' and 'something you do'. You become the key to the lock via a physiological or behavioral characteristic. Theoretically this would be fantastic - a system would be able to identify you as yourself from the entire global population. If only this were the case.

Biometrics don't provide a binary accept / reject response like a token or password, but instead provide a level of correlation between a biometric provided at the time of enrollment and the biometric being submitted for entry to the system. If the correlation is above a predefined threshold, the user gains access. If it is below the threshold, the user is shut out. In 'One to One' systems, where a user is verifying their identity, this can be relatively accurate since the comparison is just against your own biometric template. But in 'One to Many' systems, the biometric is compared with hundreds, thousands or possibly millions of templates. The technology to provide matching to a high degree of confidence just isn't there yet. In fact, in the most accurate commercial systems, you are likely to see a false match every 1 in 100 cases. Clearly this makes the deployment of biometrics as the sole means of identification unfeasible for large scale systems. As a result, most implementations involve biometrics as an additional layer of security; a fraudster might have a stolen card and manage to intercept the PIN, but the chance that he / she has a fingerprint similar to that of the criminal as well as the card and PIN is unlikely. Statistically possible, but unlikely. Other implementations use biometrics as a substitute to a token or a password. This may not enhance security in any way, but may make the transaction faster, cheaper, or more convenient for the merchant and consumer.

Cheque Cashing: Safeguarding the cheque cashing process in the US has been the biggest market for biometric suppliers to date in the retail sector. This is due to the high rate of fraud, thought to be growing at 2.5% annually. The use of biometrics in cheque cashing environments has been demonstrated to not only significantly reduce fraud, but also makes the cheque cashing process simpler for both customers and merchants since after the initial enrollment the user doesn't have to re-present the various forms of ID required for cheque cashing, they just have to provide a biometric and a password. This has the benefit of 'locking-in' a customer to a specific cheque cashing store or chain. Such is the popularity of these convenient biometric systems that where they have been implemented, significant uplift in cheque transaction volume has occurred. A good example is Cardenas Supermarkets in Ontario, California. They process around 10,000 cheques per week totaling an average of $5 million. After introducing a biometric system, cheque cashing increased as much as 25%. IDentecheck offers a similar system which can process up to 20,000 matches per second and authenticate a cheque writer's identity in less than one second.

15

The company claims to be able to move customers through 30 to 50% faster using biometrics instead of traditional cheque processing. The entire system costs under $7,000 for merchants, presenting a significant return on investment for cheque cashing establishments.

Let you fingers do the shopping: Cheque cashing has been instrumental in demonstrating the potential of biometrics and the possibilities for other forms of payment have not been overlooked. There are many initiatives in the air at the moment designed to increase throughput at the checkout and to replace such arcane payment methods as cash with faster, easier and safer technological alternatives. Vendors of POS terminals in the US are currently producing devices that incorporate fingerprint scanners, or offer the ability to attach a standalone scanner at a later date. These mainstream devices use a card for identification of the individual and the biometric for verification that the individual is who they say they are. A fingerprint scan might only be fractionally faster than entering a PIN, but in the world of high volume low value transactions, this might equate to a significant increase in throughput and therefore revenue. Higher profile offerings are the ones that do away with tokens entirely - there are a handful of companies offering POS solutions with biometrics at the center of the transaction process, notably Pay By Touch, BioPay and Biometric Access Corporation (BAC). A good representative of these types of systems is offered by Pay By Touch.

The user must first complete the enrollment process by providing contact information (name, mailing address, phone number and e-mail address), their written signature, an easily memorable numerical search code (such as a social security number or phone number) and financial account data including account numbers, expiration dates, routing and bank numbers. Users then provide a fingerprint biometric which is converted into a template and stored on a local server. When using the system for payment, the user places their finger on the scanner and enters their memorable search code. This retrieves their corresponding template on file. A real-time template is created which is compared to the enrollment template and a level of correlation is provided as a score. If the correlation score is above the predefined threshold, the user can enter the system and then choose which mode of payment they want to use. One of the key selling points for Pay By Touch is that the interface can be customized so that a specific payment choice is first on the menu. For the sake of speed and convenience, the customer is likely to take the first option offered. This has substantial benefits for merchants; by steering the customer towards an electronic cheque payment, transaction fees are much lower than those required for processing through card association networks, as much as 75% less. Other merchants might prefer to guide custom towards their own brand store card, effectively locking in the customer to further transactions in the store.

A competitor to Pay By Touch, BioPay has evolved their bCheck system from a cheque cashing product. Unlike Pay By Touch which offers a range of payment options, bCheck is cheque only, ensuring that all payments using the system go through as ACH transactions. So far bCheck hasn't spread much outside of BioPay's home state of Virginia, but the company has achieved some large scale implementations, notably with the BI-LO chain of supermarkets offering bCheck in all 176 stores. Outlay for the system is between $10,000 and $12,000 per installation. Not cheap, but the company reports a very quick return on investment can be achieved with some merchants reporting savings of $2,000 per month on cheque loss. Both Pay by Touch and BioPay are in their infancy in terms of customer and merchant acceptance and it will be interesting to see how optical and silicon scanners perform over time in high traffic consumer payment environments. POS devices receive a considerable level of abuse and are expected to perform day-in-day-out for between five and ten years. How resilient optical and silicon scanners are remains to be seen. A better alternative long term could be ultrasound scanners which can read fingerprints through dirt, grease and grime. However, merchants may be tempted to purchase lower priced alternatives if they do not consider carefully the level of abuse their scanner is likely to receive. This may well be a false economy; as the system degrades over time and becomes increasingly inaccurate at verifying a user, customers will likely revert to traditional payment vehicles.

Beyond Fingerprints: Biometric Exotica: The almost exclusive use of fingerprints as THE biometric for the consumer payments industry is understandable. They are a stable, cheap and tried-and-tested identifier, and despite the association with forensics, the fear of identity fraud and convenience of use are winning people over. With the market so clearly polarized towards a specific form of biometrics, one could be for-

16

given for thinking that there are no other forms out there. However, there are a handful (excuse the pun) of other biometrics being used in ATM and POS applications. A fairly new biometric showing considerable promise is the scanning of blood vessel structure in fingers and hands. These have been shown to be not just unique and very difficult to duplicate, but also stable throughout adult life. The Japanese payment card organization, JCB, has recently announced plans to introduce the world's first fingerprint / blood vessel pattern authentication that combines payment systems with access control. The rollout is somewhat conceptual - it allows tenants of a 156 unit condominium complex in Osaka to open doors and pay for purchases at the complex center by placing a finger on an infrared reader. ATM manufacturers have also been dabbling in biometrics. Canton, OH based Diebold has implemented hand geometry scanners for securing access to both logical and physical systems. Their PassVault self service safe deposit box is one such system and has been implemented at the East Memphis branch of the First Tennessee Bank. PassVault is located on the wall outside the day gate to the vault. Customers gain access by entering a PIN and placing their hand on the scanner which measures length, width, thickness and surface area and compares this with an enrollment template.

The replacement of physical keys with human ones makes the system far more user friendly and meant that any employees could be freed up for other tasks. Although Diebold is not currently applying this technology to their ATM's, their willingness to experiment with biometrics could well spill over into other divisions. Both Wincor Nixdorf and NCR have explored the potential of iris scanning technology. Wincor Nixdorf ran a trial over 2003 in the headquarters of Dresdner Bank in Frankfurt to test public acceptance of iris recognition systems. The results of this pilot have yet to be published. An iris scanning trial by NCR in the UK was tested on 1,500 customers of the Nationwide Building Society in Swindon. The trial was originally scheduled to last 6 months but the bank was so pleased they extended it a further 18 months, by which time a number of customers had managed to forget their PINs. Taking iris recognition a stage further, NCR Advanced Solutions Concepts in Dundee, Scotland have developed two concept ATM's; 'Bud' and 'Stella'. Both use an iris recognition system to identify the customer. This is important to note; both terminals are one factor identification systems and not verification systems; no other identifying attribute such as a card or a PIN is provided by the user. Both machines are in the realm of science fiction at this point in time, but as high precision biometric readers such as iris scanners reduce in cost and increase in accuracy, we may see ATM's related to these in the not-too-distant future.

Reality Cheque: The key element holding back biometrics can be summed up in a single word; 'imprecision'. Biometrics can be made more precise, but the closer the match is required to be to enter a system, the more likely it will be that your biometric would be rejected. In consumer payment scenarios, the main criteria by which a system will be judged are speed and convenience. Security is important, but not so much so that a customer would be prepared to repeatedly attempt to have their fingerprint verified as their own at a busy checkout. There are also competing technologies that could throw a proverbial spanner in the works for biometric payment solutions. The Exxon Mobil Speedpass has recently expanded its scope to allow for RFID payments at supermarkets. Registration involves providing chequeing account information, so all transactions go through ACH networks. For biometrics, if the key selling point for merchant buy-in is that customers can be steered towards electronic cheque payments, then this system can perform the same task just as well and has a wide degree of public acceptance already. It means we have to carry our keys with us when we shop, but I'm unsure how great a hardship this is. Another serious alternative to biometric systems will go public in July with the mass rollout of MasterCard's PayPass contactless smartcard in the US. MasterCard has the recognition and marketing firepower to make many converts and it's unlikely that biometrics can compete on speed, convenience and ubiquity in the face of such high profile competition. On a more positive note, biometric technology is quickly evolving, boosted significantly by the need for tighter security of physical and logical systems in a post September 11 world. The public are clearly ready to adapt to new payment paradigms and moreover, the climate of fear stemming from high profile cases of identity theft and consequent paranoia means that the public is prepared to overcome their skepticism of 'Big Brother' privacy invasion in return for decreased risk of having their identities stolen. In a society that requires more locks and keys than at any other time in history, biometrics are a relatively simple and cost effective method of adding additional security to existing transaction processes. It's a technology that's going to be too compelling to ignore.

Sexy Technology

By Patsy Everett, Managing Director. Smart Card News Ltd

Smart Card News decided to visit the 18th. 3GSM World Congress held in Cannes last month for the first time. Your author was particularly interested in the wearable technology fashion show which was a first at the congress. Forgetting the beautiful people, which was difficult, the technology was fascinating. The fashion show was not a gimmick or attention grabber but a serious look into the future and how fashion will enable us to get around wearing our technology without it hindering our life style.

Patsy Everett

The fashion show moved at a very fast pace and featured funky jewellery type mobiles to serious business and lifestyle phones which incorporated everything a smartphone can do . There were virtual keyboards, a Bluetooth stethoscope, a Bluetooth pill dispenser, a child safety system, a wearable GSM base station as well as a watch phone, a medallion phone radio, a neck-leash headset and a light-glove virtual control system.

One interesting technology was body type armour designed for the emergency services, in which the wearer could store and recharge all their technologies hands free and glasses of which one lens is used to display information such as data from a service manual. Another interesting technology was the use of bar codes which when photographed, using a Smartphone, would enable the holder to purchase goods, through the phone or exchange information.

Some of the companies that contributed to the show were, IXI Mobile, Seiko Instruments Inc., HIT Inc., Splashpower Ltd., Connexion2, IBM, Bang & Olufson, IQ Systems, PDD Design, Nike, Philips, Motorola, ORGA, Hutchinson, NEC, Orange, Bango.net, Nextlink, LightGlove and Microvision.

The organisers of the 3GSM Wearable technology fashion show are looking for companies with futuristic mobile products to be included in next years show, if your company has cutting edge devices that can be incorporated into a lifestyle fashion show. To find out more visit the website below:

www.3gsmworldcongress.com/fashion