



Smart Card & Identity News

Is published monthly by
Smart Card News Ltd

Head Office: Smart Card Group,
Suite 3, Anchor Springs, Duke Street,
Littlehampton, BN17 6BP

Telephone: +44 (0) 1903 734677

Fax: +44 (0) 1903 734318

Website: www.smartcard.co.uk

Email: info@smartcard.co.uk

Editorial

Managing Director – Patsy Everett

Technical Advisor – Dr David Everett

Production Team - John Owen,
Rebecca Kimberley, Lesley Dann.

Contributors to this Issue –
David Everett, Tom Tainton, Nigel
Beatty, Rebecca Kimberley, Peter
Tomlinson, Stephen Price-Francis.

Printers – Hastings Printing Company
Limited, UK

ISSN – 1755-1021

Disclaimer

Smart Card News Ltd shall not be liable for inaccuracies in its published text. We would like to make it clear that views expressed in the articles are those of the individual authors and in no way reflect our views on a particular issue.

All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means – including photocopying – without prior written permission from Smart Card News Ltd.

Our Comments

Dear Subscribers



Patsy Everett

It's summer and for the UK a good one at that, well so far anyway. However amongst the issues of weather, a particularly UK phenomena which is a necessary part of any meeting introduction there lies a constant barrage of depressing news. Until I got to the latest news from IMS where John Devlin author of the report, Smart Card Annual Review and Market Share Update, tells me that,

“Overall the smart card market grew by 16.7% in 2008 in terms of volumes and all manufacturers saw plenty of upside”

Call me cynical if you like but volumes don't put the meat on the table, what I'm looking for are margins and my friends in the industry tell me that's a totally different story. What this really means is looking beyond the basic cards through to the provision of services. As we have always argued here that has to be some extension of security and ID and authentication is the obvious area to look at. So in the positive light of the IMS report we believe based on our figures which don't seem to quite agree with IMS that the smart card manufacturer's league table (with our estimates of market share) looks as follows,

- Gemalto –Sales €1680 million 2008 40% market share (formed from the merger in 2006 of Gemplus and Axalto (previously Schlumberger, previously Bull CP8)
- Oberthur Technologies – Sales €882 million 2008 20% market share
- Giesecke and Devrient (G & D card division) – Sales €609 million 2008 15% market share
- Sagem Orga - Sales €250 million (SCN estimate for 2008) 5% market share

What can you say? Gemalto not only dominates the market but does appear to be hanging on even after the merger of the two lead players. We know from their annual report that they are optimising ASP (Average Sales Price) at the expense of market share and I must say I'm with them on that one.

G & D is a private company and quite difficult to follow, all my insider information suggests they are having a hard time while Oberthur is not really making enough headway on Gemalto which you would have expected after the merger since both Gemplus and Axalto shared many major clients who for obvious commercial reasons like to dual source.

Last year Oberthur bought XPonCard for \$111 million to increase its position in the Baltic region. Giesecke & Devrient bought SmartTrust in April this year for an undisclosed amount. SmartTrust specialises in server security applications in the mobile phone space and has annual revenues of \$31 million.

However not to be out done on all this Gemalto, on April 1st (isn't that ominous?) this year they completed the purchase of the NFC Trusted Services Management (TSM) team from NXP





Semiconductors. This will enable Gemalto to strengthen their NFC position in transport and payments using mobile phones. Everybody seems convinced this NFC thing is the way to go but I wonder....?

So at the end of all this do I feel cheerful? As always it's a yes and no, the major companies such as Gemalto, G & D, and Oberthur will survive although I can't help thinking that G & D is moving more in the right direction with SmartTrust rather than Gemalto's choice of TSM. But the smaller players are going to struggle from the competition coming from Asia and particularly China. The basic smart card is already a commodity, *'who moved my cheese?'*

Patsy.

Contents

Regular Features

Lead Story – UK Identity Card RIP?	1
Events Diary	3
World News in Brief	5,10,14,18

Industry Articles

An Interview with GlobalPlatform	7
Go with the Flow - Offline Transactions!	9
Crushed Contactless Olympic Dreams.	11
Service Delivery: Leading From Behind.	13
Designing a Real World Secure ID Strategy	16
Has Biometrics Finally Come of Age?	19

Events Diary

July 2009

- 30 – 1 EMV User Meeting Sheraton Arabellapark, Munich, Germany – www.emvco.com/munich
- 6 – 7 The Future of Cards and Payments, Le Méridien Piccadilly, London – www.marketforce.eu.com/cards
- 6 – 7 Information Assurance (IA) 09, QE II Centre, London – www.iauk.org.uk/en/Events/IA-09/
- 28 BiometriX 2009 Conference, South Africa – www.card-x.co.za

August 2009

- 20 – 21 Card X Conference & Exhibition, Johannesburg, South Africa – www.card-x.co.za

Source: www.smartcard.co.uk/calendar/





.... Continued from page 1

After Gordon Brown's cabinet reshuffle, the newly appointed home secretary launched an urgent review on the 15th June of the £5.4 billion identity card (ID) scheme, paving the way for a large U-turn on one of Labour's flagship policies. Was this instigated by Chris Grayling's letter and the likely demands from suppliers for the necessary 'insurance', who knows only time will tell. Alan Johnson who has replaced Jacqui Smith as Home Secretary is understood to be "sympathetic" to the critics claiming that identity cards will undermine civil liberties.

Mr Johnson is widely seen as the most credible rival to Gordon Brown and has told officials that he wanted a rethink of the ID card scheme, which was launched by Tony Blair following the 9/11 attacks in 2001 and which has since been championed by Brown as a new way of fighting terrorism.

The government says it wants "to give people a sure-fire way of proving they are who they say they are" and argues ID cards will boost national security, tackling identity fraud, prevent illegal working and improve border controls. From what we've seen of this fiasco already, it just looks more like an attempt to have every single person in the UK on a national biometrics database, not quite the same thing as an ID card.

The Home Office plans have changed because according to BBC News, "the Home Office is under pressure to cut costs. Public support for the scheme has also been hit by a series of data loss scandals, although the government claims the majority of the population are still in favour."

The likely scenarios surrounding the introduction of the ID card depends on who wins the next election. If Labour wins, then the ID card will be put to a vote, with MPs deciding whether to make the ID Cards compulsory for UK Citizens over the age of 16. This will depend on the success of the pilot projects to be implemented by Thales. Both the Conservatives and the Liberal Democrats said that they would scrap the scheme if they were to win the elections. Most other political parties, such as the Scottish National Party (SNP), Plaid Cymru, the Green Party and UKIP, are also against ID Cards. This is in addition to the grassroots campaign against them, through groups such as NO2ID.

Now, the fact that the majority of the parties are against the ID cards suggests that this is a battle that the labour party doesn't need to fight and given their financial situation dropping it into the bin will keep everybody happy would seem a good idea. It's probably only the fact that it was in the Labour Party Manifesto that they are taking care to lose it gently.

The scheme, if it is to be implemented will cost the taxpayers, according to the Home Office, £5bn. The London School of Economics, however, have said that this figure is completely underestimated, with the true figure likely to be between £10bn and £20bn. All these figures are to some extent misleading depending on how they are drawn up because a large part of the cost is associated with the biometric passport and associated database.

So, as I am sure all of you are wondering, what exactly is to be included and excluded from the data to be stored by the national database and what information will be on the cards themselves?

The details of each card holder were originally to be placed on a single database holding the personal information of all those issued with a card. This has now been scrapped due to the costs involved and the data security concerns brought to light by specialists in the field. Instead the information will be held on three existing, separate government databases, with the whole scheme being overseen by a new independent watchdog.

The government has sought to put some fears about the ID card scheme to sleep by announcing they will not store details about someone's race, religion, sexuality, health criminal record or political beliefs. The information that they will be storing, however, includes 49 types of information which the Identity Card Bill says may be on the national register. These 49 items will include:

- **Personal information** – Full name, aliases, date and place of birth, gender, addresses
- **Identifying information** – Passport type photo (including shoulders), signature, fingerprints
- **Residential status** – Nationality, entitlement to remain in UK, e.g. grants, terms, etc
- **Personal Reference Numbers** – Registration, Issue, Passport, and Driver Numbers, Work Permits
- **Registration and ID card History** – Dates applied, omission reason, lost, stolen and damaged ID cards
- **Security information** – Personal ID number, password or other code, questions and answers.

Mr Grayling told BBC Radio 4's Today programme that he was concerned about "a number of signals" recently suggesting "quite big penalty costs" were being built into contracts, which will leave a "substantial bill" for the taxpayer. "I want companies to be cautious and recognise that if they invest large amounts of money preparing for business, it may not happen," he said. Grayling continued by adding, "There's a danger the government will build more poisoned pills into contracts that will simply make it more difficult to scrap."

Based on this month's events it seems ever more likely that the ID card will disappear but we should not overlook the national data base that is not likely to stop.

David Everett, Smartcard & Identity News





World News In Brief

French Government Buys Gemalto Stakes

Reports this month have emerged that TPG Capital have sold 8% of their 12.5% stake in smart card makers, Gemalto. The French government's fund, FSI (translates into Strategic Investment Fund), bought the 8% of Gemalto for approximately 160 million Euros (\$224 million), also demanding that it wants one representative on the management board of Gemalto to help back the group's profitable growth strategy.

Gemalto "plays a key role for the competitiveness of the French economy, and is ideally placed in the digital world to grow in coming years," says Gilles Michel, Chief Executive Officer of the Paris-based fund. "In principle, if Gemalto at some point has an opportunity which requires an increase in capital, we'll be ready to support it," Michel added.

The FSI was created last year by the French President, Nicolas Sarkozy, to protect companies considered "strategic" by the government from "foreign predators" and helping them survive the global financial crisis. The FSI, earlier on this year is 51% owned by state lender Caisse des Depots et Consignations and 49% by the French government.

Despite the sale of 8% of the 12.5% stake owned by TPG Capital, TPG intends to retain the remaining 4.5% stake at this present time.

Halifax Ghostbust after Trial Closed

After over a month of eagerly awaiting and nail biting, the case brought to Nottingham Crown Court on the 30th April earlier this year has finally come to a close.

Alain Job, football coach for Basildon Town Ladies Football Club, brought forward a lawsuit with Halifax Building Society challenging Chip & PIN security after claiming that £2,100 disappeared from his account.

The hearing, held at Nottingham Crown Court on the 30th April, lasted a day, with the Halifax building society claiming that Mr Job had used his real card at an ATM machine and inferred that Job was either trying to defraud the bank, or he was grossly negligent in handling his card and PIN. However, due to the complexity of the case heard by the judge, the verdict took over a month for the judge of the one-day trial to deliver.

Even after Halifax destroying two critical pieces of evidence, including the original ATM card and the card's ATM authentication, the judge of the trial ruled in favour of the high street bank, in the country's first ever phantom withdrawal lawsuit. The judge based his ruling on printouts from log files to show that Job's real card had been used for the transactions and that the machine had not defaulted to reading magnetic-stripe data.

Mr Alain Job says that he is currently studying the judgement before deciding whether he wishes to appeal the ruling.

Aviva Malware Infection Exposes Customer Details

550 customers in the United States have received written warnings from insurance group Aviva after their personal data may have been exposed as a result of a malware infection on one of the firm's computers. Aviva believes that the infection was picked up when the company was conducting online research to locate the most current address information for policyholders or beneficiaries whose correspondence had been returned as undelivered.

Aviva admitted to the breach in a letter to the Attorney General of New Hampshire, in accordance with local legal obligations. The letter says the information that may have been compromised included customer social security numbers and names and/or addresses.

According to Aviva, the infected machine has been removed from service and new passwords have been issued to employees whose log-in information may have been disclosed. Aviva has also employed a team of security consultants to check its IT systems and taken steps to secure its environment against future attacks. For those that may have been affected by this break-in, Aviva will be offering a year's free ID protection to cover those that may have been exposed by the malware infection.

G&D Provides Platform for Security Technology Start-Ups

Giesecke & Devrient (G&D) has again teamed with Munich Network, a grouping of tech ventures, to host the second yearly Mobile Security Forum at G&D's Munich headquarters. Twelve start-ups from the IT security segment presented their solutions and applications to an audience of investors and G&D managers. As a leading provider of security technologies, G&D gave these international



companies access to potential partners and is considering signing cooperation agreements itself.

"The increasing mobility of Internet and IT applications on cell phones and notebooks brings with it a need to enhance the security of flexible IT solutions. This forum is an informal and effective way of presenting new developments, identifying synergies, and getting partnerships off the ground fast," informed Dr. Kai Grassie, head of the New Business division at G&D and host of the event. "Engaging with start-ups is important for us, with both sides able to benefit from the exchange."

The 12 companies participating covered a broad spectrum of security solutions from the world of mobile communications. These companies included the likes of ALK Solutions GmbH, who focused on the development of customer communication software, Xmail AG presented a flexible system for e-mail archiving aimed at the mass market, MobiNetS offered modular server solutions for mobile payment and ISA Telematics GmbH, the systems integrator for GPS-based emergency and telematics solutions, used both for people and for tracking vehicles, containers, and mobile goods.

GlobalPlatform Membership Grows as it Welcomes CARDigence

GlobalPlatform, the international specification body for smart card infrastructure has welcomed CARDigence as its newest Consultant Member. As a Consultant Member, CARDigence will monitor developments in GlobalPlatform's card, device and systems technology and debate the organisation's business and technical priorities by participating in the Advisory Council. The company will also have the opportunity to engage in GlobalPlatform's Government and Mobile Task Force initiatives.

Thomas Hagn, Founder of CARDigence, comments: "Open and flexible methods for implementing new business models and application scenarios based on modern smart card technologies are vital if the market is to succeed in delivering a near-field-communication (NFC) mobile world." Hagn added, "CARDigence has identified the value of GlobalPlatform technology and looks forward to participating in the organization's future activities."

Kevin Gillick, Executive Director of GlobalPlatform, remarks: "Consultancies such as CARDigence have a wealth of expertise, market knowledge and experience, and play an important role in the growth and progression of the smart card industry through their advisory services to a range of issuers." Gillick concludes, "CARDigence's clear commitment to creating an open infrastructure and

eagerness to support new business models based on GlobalPlatform technology makes the company a valued addition to our membership base."

Parcelforce Personal Data Disaster

After the BBC discovered that Parcelforce were leaking personal data, Fortify software, the application vulnerability specialist, believes that the data leak was almost certainly the result of shortcomings at the program code auditing stage.

The personal data had been exposed on their website to those that were tracking deliveries after a failure in the system allowed people using the mail tracing service access to the names, postcodes and signatures of various addresses.

According to Richard Kirk, Fortify's European director, the data leak believed to be caused by a "scripting issue" with the site concerned. "What's interesting about the Parcelforce site are the scripts used on the main landing pages appear to have been developed in-house, rather than the firm relying on third-party interfaces. This suggests to me that the site was developed by an in-house programming team using Omniture's SiteCatalyst software," he added.

"The problem with in-house development of Web sites," says Kirk, "is that whilst the staff concerned can be well acquainted with the requirements of the company, they may well lack the facility of looking at the code from an audit perspective." Kirk also explained that things have moved on from the old days of 'soak tests' with programs and Web sites, external professionals are usually asked to conduct tests on the Web site software now.

The Information Commissioner's Office (ICO) is reported to be contacting Parcelforce to work out what actually happened with the Web site errors and what can be done to prevent it happening again, said Kirk. "Almost certainly this will involve some sort of audit. It is to be hoped that, as well as Parcelforce learning from this situation, that other companies realise it could be their own IT team involved in the corporate red face stakes and review their own Web sites as well," he continued.

"Only by efficient code auditing can major errors like this be avoided. We all learn from mistakes. Some more than others," he added.

The data leak comes just before the ICO announced the approval of plans made by the Information Systems Audit and Control Association (ISACA) to increase the ICO's power at the end of the year. This will enable the ICO to raise penalties against data controllers under the Data Protection Act.





An Interview with GlobalPlatform

By Tom Tainton, Smartcard & Identity News

Responses Provided By Kevin Gillick, Executive Director of GlobalPlatform



Tom Tainton

What is GlobalPlatform?

Celebrating its 10th anniversary this year, GlobalPlatform is the worldwide leader in the development of specifications that support smart card infrastructure interoperability. Its proven and widely deployed technical specifications for cards, devices and systems are known as the standard for smart card infrastructure. As an independent, not-for-profit organization, our strategy is defined and prioritized by a member-elected Board of Directors.

GlobalPlatform Specifications are available royalty-free and have been adopted globally by many public and private bodies.

What are the goals and priorities of the organization?

The overarching goal of GlobalPlatform is to maintain and drive adoption of its technical specifications, which provide an open and interoperable infrastructure for smart card devices and systems. Two key areas of focus for GlobalPlatform at present include:

Contactless Mobile Services - GlobalPlatform aims to mitigate the risk of standards fracturing at this critical time of payment applications being deployed on NFC enabled mobile devices by harmonizing specifications and simplifying the adoption of specification technology.

Government Credentials - The association is currently developing and documenting solutions to assist governments seeking to source open and interoperable components – on a non-discriminatory basis – from technology suppliers and integrators. As part of this, GlobalPlatform is enhancing technology to support more rigorous cryptographic standards and the incorporation of biometrics as well as responding to new citizen requirements on privacy related to contactless applications.

Who are the member companies of this organization and what are their main goals?

All parties with an interest in smart card deployment can become a member of GlobalPlatform and contribute to its important industry activity. Currently, the GlobalPlatform membership comprises organizations from Europe, Asia, Australia and the Americas, from sectors such as payment, mobile telecommunications, transit, healthcare and retail. GlobalPlatform's membership continues to grow, and so far in 2009 we have welcomed six new members: Applus+ Corporation, CARDigence, Ericsson AB, Galitt, PayPal, Ranycon Technologies, SBA Technologies and Smart Card Laboratory Inc.

How does GlobalPlatform differ from other smart card organizations?

GlobalPlatform is the only organization that is focused on *establishing* standards for interoperability across the entire smart card infrastructure, and that can support both single and multi-application smart card schemes. The association is also *truly* independent as its technology is platform neutral.

As a result of GlobalPlatform's technical ability and cross-market member representation, it is ideally placed to facilitate technical discussions as markets overlap. As part of this process within the mobile services landscape, for example, it has formed strong allegiances with industry bodies including EMVCo, the European Payments Council, GSMA and ETSI – to name a few!

In what sectors have you experienced the most success?

GlobalPlatform conservatively estimates that over 305.7 million GlobalPlatform technology enabled cards have been deployed to date. Of the cards issued:

- 45% (137.6 million cards) has been by governments, primarily for ID and healthcare applications;
- 32.7% (100 million cards) has been by the mobile telecommunications sector;
- 21.9% (66.9 million cards) has been by the financial sector;
- 0.4% (1.2 million cards) has been by the transit sector.





An additional two billion mid range USIM/SIM cards worldwide are currently estimated to use GlobalPlatform card technology to enable over-the-air (OTA) application downloads for 3G and GSM mobile networks. It is expected that these figures will rise significantly throughout 2009.

What are the benefits of deploying GlobalPlatform technology?

By using GlobalPlatform Specifications an issuer can implement a smart card solution that:

- Reduces time to market as the technology framework is freely available allowing issuers to focus on added-value elements of their program
- Encourages participation from several suppliers on a non-discriminatory basis
- Drives down cost through competitive procurement practices
- Ensures scalability and backward compatibility of the technology, thus protecting the investment over time

Despite the current economic circumstances do you still see a significant demand for GlobalPlatform technology in the industry?

Absolutely! The state of the global economy is a hot topic for discussion and our member organizations and the markets they serve have been affected by the recession. As GlobalPlatform enters its 10th year as a specifications development body, we acknowledge our work to be of great value to the industry in good economic times and in bad. Implementing a smart card infrastructure with proven, secure, scalable and interoperable products based on GlobalPlatform Specifications is an 'investment protection' strategy for all market sectors.

How important is NFC to GlobalPlatform? Why do you feel it has yet to really take-off?

NFC enabled devices that support contactless services (such as payment) are a key focus for GlobalPlatform. One of the main barriers to adoption has been establishing a scalable infrastructure that allows multiple users from multiple sectors and with a need to support multiple business models a means to securely provision and use applications deployed to NFC enabled devices on a mass scale.

In late 2008, GlobalPlatform launched its UICC Configuration, a technical document which outlines a common and neutral environment to facilitate the secure delivery OTA of new and creative mobile services to consumers. The document has been of phenomenal interest to the market as it is the first time a neutral ecosystem for this sector has been presented.

What are the main challenges facing GlobalPlatform in 2009?

The biggest challenge GlobalPlatform faces today is maintaining our historic and rapid rate of development at a time when our member organizations are carefully evaluating the use and availability of their time and resources. We have been fortunate, however, to maintain a high level of member engagement because we are working on developments that are prioritized by the members themselves and, as such, we are moving forward with work items important not only to GlobalPlatform, but to the member organizations as well.

What does the future hold for GlobalPlatform?

Looking ahead, the association envisages that its expertise will soon be required by organizations implementing public and private partnerships such as between financial institutions and government agencies, and joint alliances between public agencies that are responsible for identity and healthcare.

GlobalPlatform will also aim to update and align its core technology to respond to the evolution of cryptography to meet the security requirements of different market sectors. Additionally, we look forward to completing work on Card Specification v3.0 which will support the industry's integration of smart cards into IT and telecom infrastructures, and will be compatible with Java Card v3.0.

For further information on GlobalPlatform or to inquire about membership, please visit www.globalplatform.org or contact secretariat@globalplatform.org.





Go with the Flow - Offline Transactions!

By Nigel Beatty, Aconite



Nigel Beatty

In many countries around the world EMV migration is either complete or well advanced, yet in only a small number are many transactions authorised offline. “What’s the point of allowing offline transactions if you can authorise everything online?” one may ask.

The world has changed since the answer to that question was an emphatic ‘None’. In the old days of magnetic stripe cards, issuers had no control over risk management at the point of sale – every offline fraud and risk control was implemented and controlled by the merchant or acquirer, from setting floor limits (sometimes overriding card scheme guidelines) to checking signatures. Little wonder that issuers wanted to see all transactions go online for authorisation. In many countries issuers banded together and agreed to issue their cards only if floor limits were zero; and once such a regime is in place it’s tough to shift.

Fast forward to the twenty-first century and things have changed. EMV programs have been successfully implemented in many countries, but the main driver has been fraud or the fear of migrating fraud. Liability shifts and, more recently, issuing mandates have driven EMV rollout, but for card issuers, the business case has been tough. Fraud as a percentage of turnover has historically been low and so for many the cure has been more painful than the disease. Which leaves card issuers asking what they get in return for their investment? On the other side of the fence, merchants are asking: “Is that it? What can this technology do for me to improve my profitability?” The good news is that, for once, there’s a win-win for issuers and merchants.

The big change with EMV has to do with risk. EMV shifts risk management out of the terminal and onto the card – its processor can perform sophisticated checks to determine the outcome of a transaction without contacting the issuer’s host and, thanks to Chip & PIN, without any active participation from the merchant. In effect, EMV has handed the issuer a means of moving part of their risk management policy out of their host and onto their cards, and has relieved merchants and acquirers of the responsibility for implementing risk management controls that were primarily for the benefit of card issuers. This is more of a paradigm shift than many issuers, acquirers and merchants at first realised. While the focus was on fraud reduction, many of the more sophisticated features of EMV went unrecognised due, in part, to the perception of EMV as a technical compliance issue.

From the merchant perspective, there’s a logical train of thought that goes: a) issuers are now in control of risk; b) their cards decide which transactions should be sent online; c) why do we need floor limits at all? This reasoning is born out of the desire of the large chains to increase throughput at the checkout. The two elements of a card transaction that are viewed as the main culprits for slowing things down are online authorisation and signature.

Unless you are one of the large merchants in the UK or elsewhere with your own authorisation switch, online authorisation time is largely composed of the dial-up and connection time of between 6 and 8 seconds; actual processing and network time should be in the 1-2 seconds range. So there’s a 7-10 seconds saving to be made per transaction if authorisation can take place offline, using the limits set in the card by the issuer. Those would be a pretty blunt instrument if they were fixed, but EMV has, of course, provided a dynamic solution to offline risk management with EMV scripts – updates that are sent securely to the card by the issuer during a normal online transaction. Scripts can be used for regular card management such as changing the PIN or blocking a stolen card, but their use for risk management is potentially far more powerful – changing the limits that control a card’s decision on whether a transaction should be approved or declined offline, or sent online for authorisation.

However, it would not be feasible to have an army of risk analysts making changes to each card’s risk profile manually. What’s needed is some glue between risk management systems and a script engine so that changes in a card or account’s risk score can be translated into a change in its risk profile, delivered in an EMV script. A card that is going from good to bad – maybe in arrears or close to exceeding its credit limit – can have its profile set to force it online more often – every 2 or 3 transactions or when offline spending since the previous online





authorisation exceeds a limit of, say, US\$50. Conversely a card with consistently low risk scores could be set to 'VIP status', where only 1 in 20 transactions comes online. Raising floor limits would incentivise issuers to invest in more advanced risk management, and the overall number of online authorisations would fall. In turn this would allow issuers to scale back the capacity of their online authorisation systems, which currently operate on something like the 80/20 rule – only 20% of the capacity is used 80% of the time, but the peak capacity may only be used during the busiest times, such as Christmas or Chinese New Year.

However, there's a bigger potential pay-back for issuers. The biggest single cost in the credit card business is write-offs due to bad debt, which are typically many times higher than fraud losses. If advanced risk management coupled with EMV scripting can prevent some of those accounts from going bad, that can represent a significant bottom-line saving for issuers.

Cardholder demand for new products and the inexorable move away from cash and onto cards means that the impending trend towards offline transactions cannot be ignored. Top of the list of innovations is contactless, such as Visa payWave and MasterCard PayPass, where the convenience of a "no signature", "no PIN", offline transaction is driving the massive expansion of contactless products both in retail and in new sectors for bank cards such as transit. Merchants love it, consumers love it and card schemes love it insofar as the initial low limits on such transactions are increasing. While the UK limit is currently set at US\$15, other countries are enjoying higher limits – some AsiaPac countries have limits up to US\$65 in selected merchant categories, including supermarkets. From contactless, the next stop is mobile, where the pressure for offline 'wave and go' convenience will be even greater, but where issuers will be able to deliver EMV script-type updates over the air to exert even greater control over offline spending.

The future is more new products, more cards and more transactions, and the future is offline, with issuers being able to manage credit risk at the point of sale without needing online authorisation of every transaction. Contactless and mobile products will accelerate the move to offline even in markets that have traditionally been 100% online. Switched-on issuers will seize this opportunity to work smarter, reducing their overheads in authorisation capacity and bad debt.

World News In Brief

Chip & PIN Drives Taxi Revolution

With 60 years experience between them, three taxi drivers have transformed taxicabs by bringing them into the cashless society. Park Taxis, set up in Newcastle by Steve Bell, Mark Fulcher and Perveais Mirza, fitted CabCard Chip & PIN machines into their cars to meet the growing demands from passengers.

There is huge demand for Chip & PIN payment within taxi businesses, with more people going cashless, preferring things to be paid for on their cards. Mr Bell said, "I've had a Chip & PIN in my car myself for four years. It's fabulous, our lads are now probably doing 30 Chip & PINs a day. It's the done thing now." Bell adds, "It's excellent for the customer, who doesn't have to stop at the cash-point, there's no risk of being mugged, and it's safer for the driver as they don't have to carry as much cash or worry about the banking."

Scammers Divert UK Bank Calls

Police in Perth are investigating an elaborate bank scam in which customer calls to the Bank of Scotland were being intercepted and diverted to fraudsters who duped the callers into handing over

personal account details.

Up to 25 people are thought to have been targeted by the scammers, including a 66 year old woman who had £1500 taken from her account and a 78 year old who almost lost £2,700 after handing over her IBAN number to the fraudsters. The Bank of Scotland became very suspicious on the latter and intervened, stopping the transfer of funds to a bank account in India.

In both incidents, customers were initially contacted by a person claiming to be a Bank of Scotland employee. The caller already had some personal information about the account holders, helping the fraudsters to lull customers into a false sense of security.

Tayside Police said that they believe the scammers had managed to tamper with their victim's phone lines, allowing them to divert the call when the customer rang the genuine Bank of Scotland telephone number.

Detective Chief Inspector Bruce Kerr, in charge of the Criminal Investigation Department in Perth, says "We are working closely with the Bank of Scotland in a bid to track down those responsible."



Crushed Contactless Olympic Dreams

By Rebecca Kimberley, Smart Card & Identity News

The next evolutionary step for payment is Contactless technology. Contactless has already been proven in the transport and access-control industries, and now we are beginning to see the introduction of contactless technology in the payment industry. The Olympic Games is a chance for the technology to expand and show-off its full multi-purpose/multi-application potential. However, whether we will see a 'Cashless Olympics' as promised is still unclear.

Last June the Evening Standard newspaper, announced that the London Olympics 2012 would be 'entirely cashless.' Now a year on, I am going to look at whether there is real prospect of having a cashless Olympics.

After waiting for the Games to return to London for 64 years, many are against the idea of London holding the Olympics because of chaos - even the 2012 Olympics logo has caused migraines and epileptic fits. Others believe that with the UK playing host, the display at Beijing will make our efforts for a good performance stand out like a sore thumb, as though we as a nation have not made a good enough effort or have the capacity to reach the standards left by the Beijing Games. This, I believe is even more of a reason to ensure that the cashless Olympics card is implemented and a success.

"The Olympics offer an opportunity to showcase new technology; for example it is hoped that spectators will be issued with electronic tickets integrated with a cash card and the London Oyster travel pass," announced by POST, the UK Parliamentary Office of Science and Technology, an independent body that advises MPs on matters of science and technology. POST hopes to publish its recommendation report on the subject entitled 'Technology for the Olympics' in the House of Commons Library next month, where it will be used to provide policy guidance for MPs.

"I think that we have the opportunity to do something special. I hope that what this POST report does is enthuse people to think in those terms," says Andrew Miller, chairman of the Parliamentary Information Technology Committee (Pitcom). In an attempt to urge the Olympic Games' organisers to embrace the cashless payment research, Miller suggests that the use of a cashless system would boost the 2012 Games and revolutionise the future for such systems at major public events. "There is huge potential to improve the visitor experience, the management of cash flow and security and identification issues using integrated smartcard technology. For instance, I went to watch the cricket at Headingley in Yorkshire and wanted to buy tickets. They didn't take cheques or credit cards and I had to walk into the village to use a cash machine with 100 other people, which is ludicrous in this day and age," Miller added.

Research analyst at Canalis, Alex Smith, praised the concepts of having a contactless ticketing scheme and stated that this scheme should go ahead. Smith feels that work should have already begun on putting the cashless infrastructure in to place and is now worried that it may be too late for the technology to be fully working by the deadline. "Managing the transport for the London 2012 Games is going to be a bit of a nightmare with the numbers of additional people coming in. Any IT management they can put in place will make it run a bit more smoothly," he said. "But if they are serious about getting it in place for the 2012 Olympics then it really should be under-way today. If that is the route they want to take they really cannot afford to delay any further."

The concept of combining a contactless payment card with ticketing capability has been used before. The Barclays OnePulse Credit card, launched in 2007, combines both Oyster card and Visa Pay-wave applications. It is thought that, under POST's examination, Olympics tickets would follow the OnePulse functionality.

Visa has already announced that it hopes large areas of the UK will have readers for contactless payWave cards in retailers by the time the Olympics take place in 2012 and is aiming to have six million cards in use by the end of 2009. Lloyds TSB have also been pushing the idea of the Games being a cash-free environment, including schemes that aim at speeding up the payment of taxi fares and parking tickets.

Many of you will agree nobody likes to carry a lot of coinage around with them. I have, on many occasions, crawled around the floor of my car scrabbling for some change for the parking meter. The idea of having a contactless card means there isn't any need to keep all that copper shrapnel lying about the car and saves wallets from bulging.





London 2012 Chief Information Officer (CIO), Gerry Pennell, in an interview with Computing.co.uk, implied that there was uncertainty behind the Olympic contactless cards. "Contactless is an interesting concept and we have had a few conversations around that, but my suspicion is that it isn't something we are likely to do." The 2012 CIO said. "I don't think that it is because contactless isn't the way the world is going to go, but the issue would be whether there is enough return on investment in implementing the infrastructure to support that technology for an event that is gone after a few weeks." Pennell intends to keep the 2012 Games a sustainable and cost-effective event, and addresses the possibilities of an increase in Olympic ticket pricing as a result of the new technology being implemented.

The 2012 cashless dream is not the first, Australia was promised contactless tickets for the 2000 Games in Sydney. The contactless payment card, the T-card was first conceived as a smart-card transport ticketing solution for the Sydney Games, underwent several trials but never came to fruition. "Smart Cards for Australia Transport" in SCN's October 2006 newsletter refers to the contactless ticketing project in Australia as "a technical and legal minefield." The article explains that Sydney commuters were promised the T-card for the Sydney 2000 Olympics; however, "After a series of technical problems and a legal dispute between prospective suppliers it still hasn't arrived."

Also in May 2008, the chief of the UK Border and Immigration Agency announced at the Security Document World Conference that an Olympic accreditation card had been planned for the 2012 Games, with the card providing access not only to the Game's venue, but to the country as well.

While companies and the public sector debate the future technology for the Olympics, Pitcom's Andrew Miller said the organisers should seek to build on systems already in place, which have been used successfully in the past. "I urge the 2012 Games organisers to learn the lessons from previous events. It is an opportunity to fly the flag about what we are good at," he concluded.

From the issues that have arisen, I am sure that with the little time left, a significant clue to the final decision on implementing the contactless payment scheme is sitting on the horizon. There are still many questions to be answered by the Chief Information Officer, including that of whether they are going to implement the UK Border access with the contactless card and whether or not the cashless Olympic promise will ever happen.

Sources:

POST: http://www.parliament.uk/parliamentary_offices/post/current.cfm

Computing.co.uk: <http://www.computing.co.uk/computing/analysis/>

Silicon.com: <http://www.silicon.com/retailandleisure/0,3800011842,39435177-2,00.htm>

SMART EVENT '09

Taking place annually in September in the Sophia Antipolis technology park on French Riviera, Smart Event continues its role in the Industry & Research key events calendar and a major forum of knowledge-sharing, learning, and networking in the fields of e-ID, e-mobility and Smart Security. Smart Event has proven to be a precious meeting place for world-class researchers, innovators, developers, and business decision-makers.

It encompasses 3 international conferences covering complementary areas:

The future of digital security technologies, *e-Smart*

The Building trusted mobile applications, *Smart mobility*

The next generation of e-ID management technologies and services, *World e-ID*.

Smart University, training program, completes the agenda



www.smart-event.eu – September 22-25, 2009 – Sophia Antipolis French Riviera





Service Delivery: Leading from Behind

By Peter Tomlinson, Iosis Associates



Peter Tomlinson

When we look at smart media in the hands of the citizen, or embedded in the equipment that we use, it is almost universally the contribution to service delivery that counts, not any gee-whizz factor about having the smart media itself. When in this country we look at our public sector's involvement in smart media, the overwhelming feature of that involvement is mere enabling (trying to enable) the use of smart media, followed by claims to be encouraging its deployment and use – and very rarely does the public sector ensure that the related service delivery is right. Worse, deployment is too often partial, in small patches, clumsy even, but hailed as major successes.

There is, of course, one spectacular public sector success in the use of smart cards by the public, namely the London Oyster card for public transport, but that result was only achieved after years of travail and at enormous cost, and also via a contract that has now had to be broken (albeit at a built-in contract breakpoint). Here we can note that the new contractual arrangements for Oyster have been entered into by a rather special autonomous public body, Transport for London, as a route to improve the services and their delivery. The new London contract is there to enable replacement of life expired equipment, to safeguard the next stage of investment in delivery methods, and to improve Infosec (information security). Included is linking TfL's network to possible (encouraged, but not guaranteed to be delivered) national deployment of ITSO-compliant smart media ticketing across all surface and sub-surface public transport.

Throughout the last few months I have been reporting on a season of conferences in which smart media ticketing and high speed (contactless) smart media bank payment featured. On those topics we are soon (July?) to see a DfT consultation on a ticketing (and possibly payment) strategy for public transport, but not backed up by anything other than encouraging service operators to deploy smart media methods – we are no further forward than we were 12 years ago. Also featured on the conference scene has been eID using smart media in the hands of citizens, or rather the lack of eID in UK national schemes (i.e. the lack of provision for using smart media in on-line secure transactions from home and office). In all of this time the feeling has been of growing frustration at the inept functioning of our public servants, frustration increasingly being seen in report after report from MPs and even occasionally in statements from Ministers. Thankfully, the frustration is now being articulated, often expertly, by a growing number of people.

The frustration stretches back to the end of 2004. From 1997 there had been a number of smart media and secure transaction initiatives and many studies launched, alongside and sometimes mirroring other work across the EU, but after 7 years most of the work in the UK at best stagnated or even closed down. A twin track of Infosec and service quality was there, however, from 2002, in the Information Assurance (IA) policy work by the Office of the eEnvoy and its spin-off CSIA (Central Sponsor for IA). That went on to support a major revision of the Manual of Protective security for government systems behind the scenes, but at the citizen level we saw next to nothing by way of smart media as a tool for better delivery of bulk services.

From 2006 there has been a revival in the public sector's interest in IA, but so far most of it is only enabling activity as far as the citizen is concerned, still not translating into securing service delivery across the board or even into generally improving those services. Again we must applaud some isolated successes, of which directgov is one (e.g. easy online renewal of car tax – but that is very carefully and appropriately designed not to need an eID token). More recently I hear that there has been widespread IA awareness training across Whitehall's public facing departments...

The 2006 IA revival started with the major architectural change in the ID card project, and a re-write of the IA documents. Botched, unfortunately: no eID in the ID card, IA concentrating on on-line services with only a passing comment about secure tokens in the hands of the citizen. What little input was possible at the end of preparation of the 2006/7 IA documents pointed out the narrow scope and poor quality of the work (e.g. Prof Ross Anderson's comments and my own attempt to get a hearing for a few of us in the supply chain).





Conferences were held (IA 07 and IA 08) at which we now know that there were calls for improved service delivery, and for regulation to be used to make it happen (skilled, expert, and to some extent independent regulation – a long way from being synonymous with micro-management).

To go with IA 07, 08, and in July IA 09, there is an Information Assurance Advisory Council (IAAC), which at last is beginning to think about 'digital data privacy': more comprehensive measures to ensure privacy of digitally held personal data and also of transaction records. Attempts are now being made to explain to them that this, like smart transport ticketing, does not require micro-management from the centre, but it does require that the centre is both leading and pushing for competent and complete service delivery.

This all reminds me of an old cat that I used to have, who was very brave at chasing other cats out of her garden as long as I was behind her throwing clods of earth – such activity on my part did not solve the underlying problem (she was really a softie), and mere 'encouragement' by the public sector falls into the same trap.

World News In Brief

Biometrics Raise Alarms Over Data Misuse

A top US executive in the biometrics industry says Canadians need to be vigilant as Ottawa embraces fingerprint and facial recognition technology in Canadian passports and at its borders. Roger Sullivan, President of the Liberty alliance Project representing around 150 companies involved in biometrics and identity issues, said 'the technology' can be trusted to prove someone is who they say they are.

However, Sullivan warns that people should "keep a close eye", to ensure governments are not compiling databases on them, for unintended purposes or sharing the information with the private sector. Sullivan also addresses the government, heeding them to ensure the data is protected from identity thieves. "The danger is that, somehow, that thumbprint is disassociated with my name or is also associated with some bad guy," he said.

Sullivan's concerns are clearly evidential; with Consumer Reports in 2008 revealed that at least 44 million consumer records were lost or exposed by all levels of U.S. governments over a three-year period.

Deputy Minister of Immigration and Incoming CSIS director, Richard Fadden, revealed this week that Canada will require digital fingerprints or face scans for all foreign visitors after 2013.

With the European Union gradually following suit, the use of biometrics for identity purposes puts the government ahead of fraudsters in the battle of identity theft, although people can replace driving licenses, names and credit cards, they cannot change their fingerprints.

NAB introduces Voice Biometrics for Phone Banking

National Australia Bank (NAB) has introduced biometrics into its banking system, for improved identity checking. The bank has implemented the biometric technology of voice recognition and verification for telephone calls from its telephone banking customers.

After implementing a successful internal pilot run, involving 2,000 branch staff in May, the speech security function is now available to NAB's 3.3 million personal banking customers.

Upon calling the contact centre of NAB, customers can now register their voice pattern, which, according to NAB is harder to steal than a password or PIN, improving the customers' authentication.

In addition, the new biometric calling system will be more convenient to customers because it does not require them to remember passwords and PINS, and once they have registered their voice patterns with NAB, they will not have to go through endless amounts of identity questions.

Warren Shaw, executive general manager, nabretail, NAB Personal Banking, says: "With identity theft related fraud increasingly moving to the phone channel, the use of voice biometrics enables the effective identification, authentication and verification of customers, offering an extra layer of protection."





Cryptography Research Announces License Agreement with Samsung

Cryptography Research, Inc. (CRI) announced that it has signed an agreement with Samsung Electronics Co., Ltd. regarding the use of CRI's patents to enhance the security of Samsung's tamper-resistant smart card chips against Differential Power Analysis (DPA) and related attacks.

Under the agreement, Samsung can use CRI's patents as part of its strategy to develop and enhance its security chips used in smart cards. The license also covers software executing on Samsung chips, allowing Samsung's customers to develop their own security countermeasures without a separate license from CRI.

"Cryptography Research is pleased to have reached this agreement with Samsung," said Kit Rodgers, Vice President of Business Development & Licensing at CRI. "Samsung is a leading producer of smart card semiconductors, and this agreement is a significant milestone for both our licensing program and security efforts in the smart card industry."

DPA is a form of attack that involves monitoring the fluctuating electrical power consumption of a target device and then using advanced statistical methods to derive cryptographic keys and other secrets. Strong countermeasures to DPA help protect smart cards used in applications such as banking, pay television, mass transit, secure ID, and wireless telecommunications.

Cryptography Research has been awarded a portfolio of approximately 50 patents covering countermeasures to DPA attacks.

Is Economic Slowdown Affecting Hacking Behaviour?

Major Internet threats have been revealed in the first quarter of 2009 after VASCO Data Security International, Inc. have announced the results of its aXsGUARD(tm) Gatekeeper Internet Threat Survey, an authentication and internet security appliance. VASCO surveyed 700 small and medium sized enterprises with 5 to 250 internet users, revealing malicious activity during the first quarter of 2009.

The results of the first quarter of 2009 (Q1 2009) are weighed against the first quarter of 2008 (Q1 2008) and major trends have revealed that there are still vast quantities of viruses being introduced, including

a steady increase in "money hunting" fraud tools such as Trojans and phishing. There is stability with spam as more blocking technologies are in place and an increase in the amounts of employees surfing the Internet.

There are three times as many viruses as in Q1 2008, with the quantities of various types on the increase. There is a steady increase in phishing and Banking Trojans, whereas more standard type viruses such as Netsky and Bagle have remained constant. VASCO, upon giving a press release, have concluded that hackers are immune against the current economic slowdown and are more focused on password theft and account hacking to steal money from innocent PC users.

More employees are surfing online, with an increase in surfing behaviour to 32%. Blocked websites are almost doubled and steadily increasing, whereas the visit to blacklisted sites remains stable. VASCO have concluded from these results that more and more companies are putting policies in place, regulating accepted and unaccepted surfing behaviour, e.g. visiting e-commerce and social network sites during working hours.

According to Jan Valcke, President and COO at VASCO Data Security: "Surveys such as our aXsGUARD Gatekeeper survey are necessary to demonstrate the vulnerability of companies on the Internet. Surveys as these clearly indicate that all companies, including SMEs, are vulnerable to Internet fraud. We cannot stress more the importance of being vigilant."

Gang Caught Downloading Own Music with Stolen Credit Cards

A gang of 9 have been arrested for downloading their own music from Amazon and iTunes with stolen credit cards.

The gang uploaded their music onto the sites, before using stolen cards to buy their music, and receiving nearly £200,000 in royalties for their fraudulent actions.

DCI Terry Wilson from the Metropolitan Police Central e-Crime said. "This has been a complex investigation to establish what we believe to be an international conspiracy to defraud Apple and Amazon".

"This investigation, with its national and international dimension, exemplifies why we have set up this national response to e-crime. It shows the success that can be achieved through our close working relationship with the FBI."



Designing a Real-World Secure ID Strategy

The everyday challenges of ID credential inspection and authentication

By Steven Price-Francis, Vice President of Marketing, LaserCard Corporation



Steven Price-Francis

No matter how advanced the technology in an identity credential, the authentication method most commonly used worldwide is still the human eye. Whether by airport security officials, law enforcement officers, or border inspectors, ID documents are inspected by people, rather than electronic readers, more than 95% of the time. The effectiveness of an ID credential is not just a function of its sophistication, but is dependent on its ability to be used in a variety of real life situations.

While the focus of attention in the ID credential industry tends to fall almost exclusively on which machine readable technology to use, we often lose sight of a fundamental reality – automatic ID readers are not always available or functional. Given the high cost of document readers, they are usually last to be deployed in any ID project - and then only in a fraction of checkpoints.

Machine-readable credential programs encounter more stumbling blocks than program managers and their suppliers ever anticipate. In the UK, for example, the media is still having a field day pointing out the woes of the nation's ID card plan and the current absence of readers in many critical locations.

Another issue with readers is the inconsistency in selection and implementation of machine-readable technologies. Take chips as an example, whatever the type – contact chip, contactless chip, a hybrid of both, or RFID: they are all in use, but there is no initiative – more importantly, there is no central budget - to place multi-functional readers at key points where they might be needed, such as Departments of Motor Vehicles, airports, or at the border.

Given these realities, the capability of confident visual identity checking is therefore an essential element for a robust secure ID program.

The Four Challenges

We believe that there are a number of key challenges that must be addressed if we are to create a strong and effective bridge from today's reality of visual inspection to the world of tomorrow, where hopefully we will see a widely available e-ID infrastructure delivering convenience, security, better service levels and comprehensive ID fraud protection.

1. Can the card be reliably and consistently authenticated by a reasonably diligent person with a minimum level of training? This requires a credential with strong counterfeit resistant and distinctive visual security features, which must be easy to validate without the aid of tools or devices. A key element is consistency and quality of manufacture – if inspection agents are accustomed to seeing variations, it becomes more difficult to detect fraudulent documents with the human eye.

One of the most effective security technologies, delivering fully on this requirement, is optical memory – a stripe of optical recording medium encapsulated into a laminated polycarbonate card structure. Digital data is encoded into the optical stripe using a laser beam (somewhat analogous to the writing of data onto a CD-R) and, since the process is destructive, the data cannot be fraudulently altered or erased, making it literally tamperproof.

The optical stripe exhibits very distinctive visual characteristics which are inherently extremely difficult to simulate. Add to this the ability to permanently mark this stripe with very high resolution images (up to 24,000 dots per inch) and security printing features, such as guilloche patterns, plus binary optical variable devices, and we now have a strong additional layer of tamper and counterfeit resistance. These images can be overt and covert, contain deliberate anomalies, and even be resolved at a forensic level, suitable for examination by a 'questioned document' lab. Experience shows that relatively inexpert "examiners" can make a sound judgment about the card's authenticity based on these characteristics.



This is the combined and layered approach used in the current U.S. Permanent Resident Card (“Green Card”) and by governments around the world for citizen and foreign resident ID programs. Data stored to the optical memory varies by program but can include a high resolution facial image, demographics, digitized signature and biometrics (both original images and templates).

2: Can a confident visual identification of the cardholder be made using the information printed (or laser engraved) on the credential’s surfaces? One of the most popular forms of fraudulent ID tampering is image substitution, despite advances in preventive technologies.

One way of making the visual identification process more reliable is to laser “etch” the cardholder’s facial portrait into the optical stripe itself. The result is a feature called “Personalized Embedded HologramHD” a high resolution, high contrast, photo-like image which *cannot* be altered. The combination of inherent visual characteristics, high resolution security images and the Personalized Embedded Hologram builds a third, blended layer of tamper and counterfeit resistance and gives optical memory what one industry expert has called “self referential authentication”.

This forgery countermeasure is used in the Saudi Arabia National ID Card, among many others, and serves to support visual inspection of the card in a wide variety of settings where readers are unlikely to be present.

3: Are *real* biometrics being employed to verify the cardholder’s identity? The visual comparison, by a human inspector, of a portrait to a person’s face may be reasonable reliable but it is *not* biometrics. To reliably verify identity, we must use digital biometrics.

Assuming our society values such benefits as ID theft protection, faster clearance through airport security or passage through our borders, we can expect to see biometrics in wide scale use at some point in the future. Possibly the most acceptable approach would be to allow the individual to choose the method(s) by which he or she prefers to be identified from a range of choices such as fingerprint, face, or iris. And certainly, biometrics is made more reliable by applying a combination of methods, say face and fingerprint.

The most effective approach to using biometrics requires an integrated approach:

- A. Implementing more than one type of biometric;
- B. Providing storage capacity on the card to add new data;
- C. Assuring secure off-line verification ability;
- D. Providing the ability to select the appropriate biometric depending on the application

Experts agree there is no absolutely perfect biometric system. Each has its own strengths, weaknesses, and vulnerabilities. However, using truly transportable biometrics on a high data capacity, counterfeit-resistant, secure identification card will lead to the creation and implementation of the “*trusted identity*” card.

This latter is the approach used in the optical memory-based Costa Rica Foreign Resident Card program, where the overriding objective was to develop the most counterfeit-resistant document possible while implementing machine-readable biometric elements, tamperproof data storage *and* interoperability with the U.S. program.

4: Are we equating hi-tech with high security? If hi-tech imbues a credential with *perceived* authenticity and reliability even in the absence of authentication readers, what can document examiners rely on when presented with a convincing look-alike document?

Counterfeiters are skilled not only in creating plausible forgeries but in social engineering –playing upon the preconceptions, assumptions or expectations of the law-abiding and the enforcers of law. Criminal elements will find it all too easy to prey upon the weaknesses of a card that is assumed to be secure but cannot be verified without access to a reader.

Layered technologies and security provide the solution here. For example, the combination of optical memory as the visual enabler, tamperproof data storage, robust physical card construction and additional fall-back options will exponentially increase the credential’s security.

By addressing these challenges, the industry can create a strong and effective bridge from today’s reality of visual inspection to the world of tomorrow based on a widely available e-id infrastructure delivering convenience, security, better service levels and ID fraud protection.





World News In Brief

LaserCard Corporation Joins Smart Card Alliance

LaserCard Corporation has announced that it has joined the Smart Card Alliance. Through this alliance, LaserCard aims to enhance its collaboration with industry peers in delivering innovative, technology-inclusive solutions to meet the ever increasing complexity of requirements of large-scale ID credential programs.

Bob DeVincenzi, president and chief executive officer of LaserCard explains, "The Smart Card Alliance is driving a new generation of products and solutions based on smart card technology and we are very pleased to be counted as a member."

DeVincenzi adds, "We look forward to sharing our expertise in incorporating multiple technologies on the same credential platform, and to exploring new opportunities and expanding our partnerships with fellow members of the Alliance."

Executive Director of the Smart Card Alliance, Randy Vanderhoof, comments on their new addition, "We look forward to LaserCard's contributions to the alliance as we continue to develop new solutions for current and future ID card needs."

Australia Shares Little Biometric Data

Australia is not participating in the international efforts to share biometric data in the fight against crime and terrorism, according to experts speaking at the Biometrics Institute Conference held in Sydney, Australia.

Representatives from both the international crime database service Interpol and the United States Department of Homeland Security attended the Biometrics Institute Conference. Both explained that Australia shared little biometric data, including fingerprints, with the international community.

Head of the OIPC Interpol Fingerprint Unit, Mark Branchflower highlighted the fact that all the fingerprint data Interpol collects from over 100 member countries is "available to the Australian Government" via its National Central Bureau office in Canberra. "As for Australia sending fingerprint data to us? It's very, very limited. Very limited. Nearly non-existent," he told delegates.

Michael Hardin, senior policy analyst at the US Department of Homeland Security backed Branchflower's comments by adding that Australia shares surprisingly little biometric data with the United States.

Branchflower expressed his concerns, as the biometric data would be useful in helping to track the activities of international criminals. In expressing these concerns, Branchflower believes that Australia isn't including important subsets of Interpol's fingerprinting data in its own national fingerprint database. Branchflower also informed media sources that Australian authorities have enlightened him that the oversight will be rectified in the not so distant future.

ACS Launch World's First NFC Card Reader compliant to Microsoft CCID standard

Advanced Card Systems Ltd. (ACS) will launch its ACR122T NFC (Near Field Communication) Contactless Smart Card Reader Token in Q3, 2009.

The ACR122T is specially designed for mobile applications. Its compact and extractable USB plug design is highly portable and easy to use, making it suitable for integration into fast-paced environments.

It is ideal for a wide range of NFC applications, such as secure computer log-on with corresponding contactless cards or NFC tags in public places like a coffee shop or public library, balance checking and reloading of an e-Purse, and online payment.

"Our strategy is to keep building and strengthening our reader technology for the fast-growing global NFC and other contactless reader markets," said Gilbert Leung, Sales Director of ACS.

The ACR122T was developed based on the 13.56 MHz RFID technology and the ISO/IEC 18092 NFC standard. It supports various types of contactless cards, including ISO 14443 Type A and B, Mifare(r) and FeliCa cards and NFC contactless tags. Compliant with CCID (Chip/Smart Card Interface Devices) and PC/SC (Personal Computer/Smart Card) specifications and supporting NFC peer-to-peer communication, the ACR122T facilitates smooth integration of a large variety of applications.



Has Biometrics Finally Come of Age?

By Tom Tainton, Smartcard & Identity News

At the turn of the nineties, the explosion of the internet and e-commerce created tremendous difficulties in identifying people who could not be met face-to-face. Tired methods such as passwords and PINs no longer cut the mustard anymore. Easily forgotten, and effortlessly hacked, the security industry cried out for a viable alternative to these old authentication systems. Then, just over a decade ago, biometric security devices crept onto the scene. Touted as the final word in security technology, biometrics were supposed to change the face of the identification industry. So what went wrong?

A biometric record is a mathematical representation of an individual's unique characteristic, stored in digital form. The record can be based on a wide range of methods including fingerprint scans, iris scans and facial recognition. Although it carries distinct advantages over driver's licenses and passports, (it's near-impossible to steal someone's fingerprint for one), biometric security is still fairly unreliable. Despite the technology being around for many years, biometrics have been restricted by large running costs and the complexity of the devices which use it. Thus, its take-up has been limited to military and other high-security applications where security takes precedence over cost and convenience.

But the landscape is finally changing. Biometrics devices are rapidly gaining market acceptance by private companies, governments and consumers who recognise the potential of the technology. Now providers need to repay the faith by developing ironclad security products which are cost-effective and easy-to-use. The security industry is seeing a convergence of physical and virtual devices and access is becoming integrated with computer networks and databases. But biometrics aren't quite good enough just yet. Even as microphones and digital cameras become standard equipment, voice or facial recognition devices are scarce. For this to change the technology needs to find the right balance between rejecting legitimate users and allowing unauthorised ones to log on.

One way biometric security technology can improve is in the way in which it detects stress levels. Currently, that type of recognition is reserved for harsh image and sound variations in the surrounding area. For instance, a user could be denied access if he tried to use a voiceprint security gateway in a noisy room. In similar fashion, a facial recognition program could reject a user who is sporting a new hair cut or has naturally aged. Alternatively, it may accept an unauthorised user who bears a strong resemblance to a legitimate one. In fact, research by Atos Origin, who ran the UK Passport Agency Biometrics Trial, showed that the failure rate for face recognition was one person in ten. In addition, they warned facial recognition could be fooled simply by obtaining a good image of an individual's face with a high-resolution photograph or a video recording.

Finger print patterns present a different problem. Because they are not unique to any one individual, a print on a passport or identity card could easily be the same as that of someone else. Also, finger prints required careful expertise to ensure a good print is recorded. Worn finger prints (such as manual workers), and dirty fingers will result in the scan failing. This means that fingerprint verification in shops and banks would be very unsuitable. To make matters worse, research in Germany revealed that fingerprint recognition could be cheated by 'lifting' prints using adhesive tape and using them hundreds of times. Or even worse, the technology might not recognise any prints at all. Take the story of a cancer sufferer in America, for instance. The gentleman was detained at an airport after side-effects of his treatment drug left immigration officials unable to take a print from his fingers.

Iris recognition requires specialist cameras and good lighting to work properly. In other words, it's damn expensive. Even under perfect conditions there is still a failure rate of 1 in 100 people and companies admit that iris photography is not yet proven on a scale required to support the whole UK population. Typically, the proposed biometric passport will use the two most unreliable applications (face and finger recognition), while the identity card will have all three. The Home Affairs Select Committee has suggested that all three biometrics should be taken to reduce the risk of error. In contrast experts contend that this merely increases the failure rate. Add to that the impracticality of providing three separate biometric scans every time you travel and you have a non-starter.

But it's not all bad, biometrics are gradually improving. New devices can sense an electro-magnetic pulse so any villain-style use of chopped off hands and fingers are thankfully a thing of the past. And the future's looking rosier too. Experts predict that by 2013 the biometric security market will be worth £650 million dollars. They also predicted profound changes in the industry in the coming years now that the technology has completed its proof of concept stage and can start turning a profit. Governments are likely to be the early adopters, with business applications taking a backseat.

Eventually, widespread adoption will bring about consolidation in the industry, as investors push for profits and the companies that win the big private and government contracts will be at a considerable advantage over smaller start-ups. When the dust settles, it's possible that hundreds of small companies will have merged with others, leaving only a handful remaining. What's definite is that we will be hearing a lot more about biometric ID management. It's time for biometrics to live up to their reputation.

