

Smart Card & Identity News is published monthly by Smart Card News Ltd

Head Office: Smart Card Group, Columbia House, Columbia Drive, Worthing, BN13 3HD, UK

Telephone: + 44 (0) 1903 691 779

Fax: + 44 (0) 1903 692 616

Website: www.smartcard.co.uk

General Enquiries:
info@smartcard.co.uk

Editorial

Managing Director - Patsy Everett

Editor - Jason Smith

Technical Advisor - Dr David Everett

Subscriptions & Administrator - Lesley Dann

Editorial Consultants - Peter Hawks, Simon Reed, Robin Townsend

Contributors to this issue - Innovision Research & Technology, Karsten Neugebauer, L-1 Identity Solutions, "The Squeaker", Marc Hudavert and John Owen

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 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.

© Smart Card News Ltd

Our Comments



It's been a month of phones, a few of my friends have all upgraded their handsets over the last couple of weeks and it has been interesting to examine the criteria of selection. Just to put you out of your misery at the start none of them had NFC on the list of desirable properties. I think everybody assumes the phone can handle voice calls so that wasn't even mentioned either.

A common thread was the good old text messaging, clearly important to everybody and in some cases with the option of handling pictures. And then the first interesting point, nobody actually cared about the role of the SIM card only where is the data stored, contacts etc and how do you get it from the old phone to the new. The idea that the contacts could be on the SIM and moved from phone to phone wasn't a big selling point, or even the idea of doing a SIM transfer with all the little gizmos available in the market place. Fashion was very high on the list. Slim and sexy seemed to be a totally unanimous requirement regardless of sex and close behind was the need for some suitable ring tone.

The thing that struck me about all this is that the network operators have lost their way with the SIM card, it's the only bit of the phone owned by the operator but it has no significance in the eye of the consumer. They all know its there but it is seen as the bit that makes the voice calls work. Given the capability of the modern SIM card both in functionality and memory size shouldn't it be doing more? Isn't there a market for an all singing and dancing SIM card that makes the user experience more exciting or am I just missing something?

Patsy

Contents

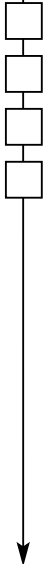
Regular Features

Lead Story - Greater Security for the UK Border	1
World News In Brief	4
Events Diary	3
Rumours From the Front Line	17

Industry Articles

NFC in the Real World - Part 2	10
Document Security is More Than a Secure Document	12
New Uses of ePassports: Automated Border Crossing and Beyond	14
The Enterprise Identity Challenge	18
Directory Services the Backbone of Digital Identity.....	20





In collaboration with organisations such as VISA, MasterCard and UK acquiring banks, Ingenico is playing a leading role in bringing Contactless technology to market - the logical step to addressing high volume, low value transactions. The two companies are working together at the forefront of the rollout of contactless payment technology. As part of the collaboration, Barclaycard Business retailers can select from a range of Ingenico Contactless payment products. These fast, secure payment solutions allow any Barclaycard Business retail customer to accept contactless payments for items of £10 or under.

The new technology will transform the way retailers can accept payments from customers using debit or credit cards. For retailers contactless will provide a range of benefits including reduced transaction times, reduced queue times at the checkout and increased footfall. James McDonald, Head of Contactless payments, from Barclaycard Business welcomed the partnership; "The rollout of contactless technology is an exciting time for the retail industry. We expect it to deliver significant benefits for the retail community, with shorter queuing times and increased sales. By working together, Barclaycard Business and Ingenico will set the benchmark for contactless payment solutions in the UK." Gordon Brown said: "The future of Contactless payment technology has arrived and I would like to congratulate the senior management team at Ingenico. Ingenico has played a key role in implementing this innovative technology set to benefit the UK economy. "



"I was delighted to meet the staff at the Dalgety Bay site and wish to congratulate them for their enthusiasm. I will be working with Ingenico to help grow the business in Fife and look forward to the operation going from strength to strength." Nick Parsons Managing Director of Ingenico UK and Northern Europe said: "We were delighted to welcome Gordon Brown to Ingenico and to have the opportunity to discuss with him the latest developments affecting the UK retail sector

"With over 75% of all cash payments being less than £10, the introduction of Contactless payments will play a major role in encouraging the use of cards over cash for low value transactions. Contactless, which has been a vision of the future, is now ready for deployment. It is going to completely change the way we acquire information and pay for goods and services." Other initiatives that Ingenico are involved in are at a local government level. Ingenico is working closely with Scottish Enterprise to review potential international market opportunities and drive forward to generate business growth.

Amedeo D'Angelo, Chief Executive, Ingenico Group said: "The UK has traditionally been a pioneering marketplace for developments in payment solutions and it is continuing in this role with the launch of Contactless technology. Through our innovation and commitment to research and development, Ingenico is helping to drive this market forward."

Events Diary

July 2007

- 10 - 11 Cardex Asia & RFID Expo Asia - *Bangkok, Thailand*
- 15 - 16 Near Field Communication Australia - *Sydney, Australia - www.terrapinn.com/2007/nfc_au*

August 2007

- 21 - 22 Technology in Government & the Public Sector Exhibition - *Canberra, Australia*



Smart Cards

Gemalto Restructures in France

Gemalto has informed the Employee Representatives of a restructuring project in France. The implementation of the project would result in the ending of the manufacturing activity in the Orléans facility by the second half of 2008, as well as the redeployment of its production activity towards other existing centers of the Group in France and Western Europe. This restructuring project in France aims at lessening the central industrial costs and rationalising the manufacturing centers while making them more specialised. In order to optimize Gemalto's industrial capacity, the Pont-Audemer (Normandy) site would manage the production of SIM cards for Western Europe while Gémenos would gather all the industrialisation and the embedding activities for French banking cards.

This project follows an overall cost reduction program that the company has been pursuing on a worldwide basis, notably in China, the United States of America, Mexico, the United Kingdom, South Africa and Russia. The project would also impact the Manufacturing Coordination department and some support functions. The project does not involve the R&D in Meudon and La Ciotat, nor the personalization center of Tours. The overall net impact of the project would involve 409 positions including 362 positions in the Orléans facility. The Company employs close to 3 500 people in France.

NXP Eyes Indian e-Passports Order

NXP Semiconductors is pitching for a multi-million dollar order from the Indian government to supply chips for electronic passports (e-passport), according to official sources. "With the government of India deciding to go for e-passports soon, we are looking forward to provide our chips and contactless identification technology to the passport offices across the country," said NXP India sales and marketing director Ashok Chandak. The government will undertake a pilot program this year-end to study the pros and cons of issuing e-passports with security features, including bio-metrics in place of the existing passports in book format. About 40 million passports are in use currently and around 10-12 million are issued every year by the regional passport offices.

As the country gets integrated globally and more Indians travel abroad for various reasons, the number of passports is set to multiply manifold. The Indian subsidiary of the NXP is already supplying its contactless Smart Cards to Delhi's metro service for fare payment by commuters.

16m Smart Cards in Beijing by 2008

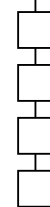
Beijing Development, which runs the Smart Card system in Beijing, has predicted that by 2008 they will have issued around 15 million to 16 million Smart Cards. The Smart Card, similar to Hong Kong's Octopus Smart Card, was officially launched last May to replace paper tickets used on Beijing's subway, public buses and taxis. As of the end of May, 11 million Smart Cards were issued and more than 10 million transactions were registered daily, said executive director Wang Yong. Beijingers may also soon be able to use their mobile phones to pay for tickets on public transit, sources with the city's public transportation group have said. A variant of a mobile phone's SIM card is being developed and tested, said Xu Fa, a marketing manager of the Beijing Municipal Administration and Communication Card Co Ltd. Xu said the card is now being tested on a new Nokia mobile phone, but he didn't indicate when it might come into use.

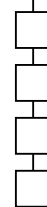
Citibank Selects Gemalto

Citibank Taiwan has selected Gemalto as exclusive EMV migration launch partner and to provide over 1 million banking cards, personalisation services and turnkey solution. "A migration of technology of this scale, being Taiwan's largest foreign bank, is fraught with challenges, and careful planning and extra diligence is necessary," said Daniel Huang, vice president, Transaction Service Group of Citibank Taiwan. "Experience counts for a lot and having a one-stop-shop makes life easier for everyone involved. Migration to EMV microprocessor card technology is an important milestone and we believe our customers will benefit from the enhanced security provided whilst maintaining the same levels of convenience."

Smart Cards for Delhi Metro

The Delhi Metro in India plans to issue multi-purpose Smart Cards for commuters. "We will improve upon the present chip inside the metro pass, which will enable travellers' parking, eating and commuting facility without any hassles," said Anuj Dayal, chief spokesperson of Delhi Metro Rail Corp (DMRC).





The commuter can swipe the card in dedicated machines at eateries and parking areas of metro stations. A 'common clearing house' like a main server would be set up to calculate the share of revenues among the parties concerned, Dayal said. Apart from upgrading the electronic chip in existing passes, the DMRC will issue new metro passes with all these inbuilt facilities. The new initiative, Dayal hopes, will be in place by the year-end.

Inspired Advances Smart Cards

"Inspired", the first European research project entirely related to the advancement of the Smart Card, is drawing to a successful close after three years. Stakeholders from the European Smart Card and semiconductor industries have collaborated to define new standards aimed at giving further impetus to the Smart Card's success story as the portable Trusted Personal Device (TPD) of choice. TPD's are set to develop and protect many new markets. The Inspired project raised many questions covering the technical pre-requisites for TPD's so that they can systematically be made more secure, faster, more cost-effective and more versatile in their use.

Representatives from all areas of the Smart Card industry worked together over the three years in the Inspired project, conducting research, holding discussions and developing solutions. The project's objective was to define and establish new standards for the entire industry of Smart Cards and secure devices. "Consistent standards like the platform defined in the Inspired project enable market players to implement Smart Card technology and services and so increase the number of developers and ultimately the number of users for the Smart Card" said Research & Development Project Manager Carsten Rust, who was in charge of the Inspired project for Sagem Orga.

Data Leak Could Have Been Avoided

Calum Macleod, European director for Cyber-Ark, the data vaulting and security specialist, says that the Bank of Scotland potential ID theft case - involving 62,000 of the bank's mortgage customers - could have been avoided if they had employed encryption for their sensitive data. In the HBOS subsidiary case, a disk containing personal information on customers, including their names, addresses, date of birth and account details, went missing in the post whilst en-route to a credit reference agency.

As a result of the high profile data loss incident, the bank is writing to all the affected customers warning them they could be victims of identity theft, and offering them free credit reference checks. "This case dramatically highlights the need for encryption of sensitive information by companies, especially where customer data is involved. Considering the fact that the bank's sister organisation, also had a similar incident last March, you'd think they would have reviewed their data security policies by now." said Macleod

Smart Cards for NHS Infrastructures

Imprivata, Inc has partnered with Gemalto and Intercede to deliver Smart Card management and enterprise single sign-on services to customers in the UK healthcare market. Imprivata's OneSign appliance will support access to the applications provided by "Connecting for Health" using Smart Cards from Gemalto and with credentials issued by Intercede's MyID. This Smart Card and credential can then be used to provide strong two-factor authentication and single sign-on to multiple locally provided applications belonging to individual NHS Trusts. Integrating secure credential and device management with strong authentication and enterprise single sign-on delivers greater efficiency, tighter security and ease of access for end-users.

Smart Card for Causeway Passage

Malaysia and Singapore are looking into the possibility of introducing a Smart Card to facilitate travelling across the causeway linking Johor and Singapore. Prime Minister Datuk Seri Abdullah Ahmad Badawi said the flow of people would increase once the southern Johor development corridor project gathered momentum. He said that such a card would prevent people from being stuck in long queues. "Everyone will need to show their Smart Card to enable them to cross into Singapore or Johor," he said at the annual Budget 2008 Consultation session.

Gematik Certifies Sagem Orga

Sagem Orga is the first Smart Card and security provider to be certified for all Smart Card products necessary for the upcoming eGK telematics infrastructure, putting it well ahead of the competition. With gematik certifying the secure module card (SMC), which will secure terminals and the vital connector module in the telematics infrastructure, Sagem Orga has now completed the certifications for the patient card (eGK; in December 2006), health worker's card (HBA; April 2007) and secure module card (SMC; May 2007).



Bright Prospects for Smart Cards

The Asia Pacific region has immense potential in untapped markets for Smart Cards and various newly implemented small-scale projects are likely to fuel the growth of these markets. The larger projects such as EMV mandates and National ID projects are also likely to boost this drive. "Contactless modes of payment have also been successful in the Asian countries despite the low acquiring power of the majority of citizens here," says Frost & Sullivan Research Analyst Navin Rajendra. "Through proper coordination and planning, these markets could provide a major market share of Smart Cards in Asia." In countries such as Thailand and the Philippines, the concept of small value payments through contactless cards or short message service (SMS) is already popular.

Thailand has also implemented the national ID project and Vietnam is soon to follow suit, indicating the influence of a country's Smart Card industry on its neighbour. However, the national ID card issued in Thailand has not yet been fully utilised due to the public's lack of awareness about the benefits of the ID card. Educating the public about the advantages of these cards is critical for the success of any Smart Card project. Moreover, in countries with low fraud rates, there is simply no business case for the migration to EMV-compliant cards. This initiative lacks support since the cost of migration outbalances the losses incurred from fraudulent activities. Therefore, rather than focusing on the security aspects of Smart Cards in these countries, it pays to introduce directly the benefits of contactless payments.

Philadelphia Expands Smart Cards

People in Philadelphia, USA, will soon be able to use a Smart Card to pay for transportation needs ranging from parking meters to garages to cab rides. The Philadelphia Parking Authority already has Smart Cards for all parking meters in town. Next year, the authority and a local firm called OmPay will offer a card for a wider range of transportation needs.

The Parking Authority's Rick Dickson says commuters and visitors alike will be able to use the super Smart Card to park at a meter on the street, park at a garage for, say, an evening dinner, or take a cab to the theatre. Officials with the Parking Authority are also talking to SEPTA and PATCO, the regional transit agencies on the Pennsylvania and New Jersey sides of the Delaware River, about joining the Smart Card project.

Smart Cards for Mexican Drivers

Gemalto has successfully delivered Mexico's first Smart Card driving license to the city of Monterrey, Nuevo Leon state, Mexico. The contract includes 900,000 driving licenses over a period of 3 years. This new card also acts as a reliable ID document and opens up the potential for additional e-schemes like healthcare for the benefits of all citizens. The solution includes the Gemalto Smart Card platform that will securely store the driver's information, and a sophisticated card body with specific security features that makes it difficult to copy and counterfeit. Prime contractor Cosmocolor handles the enrolment process and provides on-site personalisation of the solution.

Alliance Scrutinizes PASS Card

The new Generation 2 Radio Frequency Identification tag on the People Access Security Services (PASS) card, which is to be issued by the US State and Homeland Security departments, has come under fire from the Smart Card Alliance. The PASS card is part of the Western Hemisphere Travel Initiative and is intended for use by Americans, Mexicans and Canadians who frequently cross the border. Its design has been controversial because the Gen2 RFID tags have raised privacy worries about unauthorised reading and tracking of cardholders. DHS officials have asserted that the long-distance RFID tags will enable them to quickly process traffic at the borders.

The Smart Card Alliance, have accused the US National Institute of Standards and Technology (NIST) of certifying the so-called Gen2 RFID card architecture without using "the appropriate standards and best practices relevant to human identity applications. The Smart Card Alliance has also accused NIST of failing to properly evaluate whether the Gen2 RFID is appropriate technology for a personal identification card. The Gen2 RFID chip was designed for tracking merchandise in warehouses and on shipping pallets. NIST Director William Jeffrey responded by saying that NIST's review was thorough and in compliance with the request from Congress.

Bolton Lines up sQuid Card Scheme

The UK northwest town of Bolton looks set to introduce a new facility to its Smart Card scheme whereby consumers can pay for lower-priced items at various retailers across the region. Utilising a 'tap and go' method, the sQuid e-money option allows holders to pay for goods after they have loaded the card with an amount up to £50.



Council chiefs have given the go-ahead for sQuid to be incorporated into the town's existing system - the Bolton Smart Card - which can be used at leisure and library services and was originally introduced last November.

Smart Cards to Control Petrol Usage

Iran's method of keeping petrol prices low to increase people's spirits throughout the country has not only caused a huge hole in Iran's budget but it has also increased the number of cars in Iran. In order to control this situation Iran President Mahmoud Ahmadinejad and his administration aim to ration petrol with Smart Cards, which were scheduled to begin on May 21. The plan of reducing lavish consumption of petrol is basically supported by most Iranians. The initial idea is to issue Smart Cards for about eight million cars in Iran, setting a daily ration of three litres for private cars and 15 to 20 litres for taxis at the current price of 11 cents. Anything above the ration quota was to be sold at 33 to 44 cents.

Indian Army Smarten Up

To prevent the misuse of identity cards, the Indian Army has decided to issue Smart Cards to its troops across the country. The decision was taken after a few Army identity cards were found in the possession of militants in Jammu and Kashmir, a couple of months back. Informed of this, General Officer Commanding-in-Charge, Northern Command, Lt Gen H S Panag said "concern about the misuse of Army identity cards has been mooted by the top brass of the Indian Army to the Central Government". He also said the DRDO was working on these cards, which would be prepared on the lines of the access cards issued by multi-national companies (MNCs) to their employees.

New Smart Health Cards for Qatar

HAMAD Medical Corporation (HMC), a non-profit health care provider in the state of Qatar, plans to issue new smart health cards, equipped with the E-purse, from October. The E-purse would allow electronic payment for medical and medical related services, sources said. The new smart health cards are to be introduced in a phased manner with fresh applications and those for renewal of existing cards. Cardholders will be able to deposit funds into the E-purse at designated smart health card issuing points. The current coupon-based payment for medications will now be gradually phased out at healthcare centres.

Biometrics

Facial Scans for Singapore Borders

People travelling to Singapore will soon be required to have their face electronically scanned at immigration checkpoints amid efforts to boost security. Nearly 1,000 computers at all of the island-nation's ports, land borders and airports, will be installed with face-recognition technology over the next year. The face-matching system will be used together with the fingerprint scanners currently in operation, the report said. The biometric system would process more than 250,000 face scans daily when fully operational. Singapore's immigration authorities confirmed in a statement that the government had issued a tender for a face-recognition system to be deployed at checkpoints, but declined to give details on the implementation of the system as it was in its early stages.

Biometric Smart Cards for Indians

Public-sector Indian Bank has launched its biometric-enabled Smart Card banking in Dharavi, one of Asia's biggest slum pockets. The Smart Cards have been launched in association with Financial Information Network & Operations Limited (FINO), the leading technology-provider of biometric cards in India. The Bank had recently launched its biometric cards in the Cuddalore district of Tamil Nadu. The card captures the fingerprints, signature and a digital photo of the customer in adherence to KYC (know your customer) norms stipulated by the RBI.

"The cards would facilitate the banking transaction link of the common man with the bank. The card is a good tool for migratory labourers in Dharavi to become a partner in inclusive growth," Bank's CMD K C Chakravarty said. It plans to replicate the project in 15-16 branches all over India. FINO Chief Executive Manish Kherra said apart from being a card for convenience, the smart card was also secure and reliable. As many as 15 different applications can be loaded on the card, including savings bank account and loan details.

UK School Kids Get Fingerprinted

Thousands of school children are potentially being fingerprinted, the Liberal Democrats claim. A survey of Local Education Authorities (LEAs) discovered 285 schools regularly fingerprint pupils and store their biometric details on record, adding, the real figure could be higher.





Despite this, the Department for Education and Skills (DfES) has not issued any guidance on when and how biometric data should be collected and stored. Only a quarter of LEAs have any guidance available and in the vast majority of cases do not know if parental consent was given to collect fingerprints. LibDem education spokeswoman Sarah Teather said: "These figures confirm an extremely worrying situation where schools are fingerprinting pupils without any guidance on whether it is legal to do so. Insecure school computers holding precious unique personal information are a gift to identity thieves."

Biometric Data for UK Visas

The UK is following the United States in requiring all visa applicants to submit biometric data, the British Trade & Cultural Office (BTCO) has announced. Starting on July 26, all applicants in Taiwan for a British visa must undergo a fingerscan and have their digital photo taken as part of the visa application process. "The new procedures are part of our commitment to provide the best possible service to visitors to the UK. Biometric visas provide a higher standard of security and will in time make entry clearance into the UK simpler and easier," said BTCO Director Michael Reilly said.

The British Embassy in Qatar has also rolled out technology to capture biometric data from visa applicants in Qatar. The electronic Biometric scanning and Visa Application Centres are the two major changes the British Embassies across the region are introducing to their visa services. "It is our determination to ensure that visiting the UK remains stress free, enjoyable and a memorable experience for people from this region starting the minute they apply for a visa, by implementing electronic biometric scanning and Visa Application Centres," said Simons Collis, British Ambassador to Qatar. Collis said the new system is global and is being implemented in over 70 different countries around the world.

Biometrics for Vietnamese Market

BioLink has partnered with ADC company, a Vietnamese supplier of advanced security solutions. Cooperation of both companies will be targeted at implementation of biometric identification technologies with state authorities and commercial structures. Their collaboration will aim at participation in governmental programs of development and deployment of brand new identification documents with embedded biometrics (passports, visas, e-documents, etc.) meeting modern internationally accepted standards.

RSA Joins TWIC Team

RSA is to support Lockheed Martin on the Transportation Security Administration (TSA)'s Transportation Worker Identification Credential (TWIC) program. To further secure the nation's transportation system, the TWIC program involves the rapid, nationwide deployment of biometric identification credentials to maritime workers. The TWIC credential will enhance port security by requiring all workers with unescorted access to secure areas of vessels and maritime facilities to complete a security threat assessment successfully and carry a biometric credential.

New Products/Services

Smart Card Framework for Vista

Giesecke & Devrient (G&D) has become one of the first companies meeting the quality criteria of Microsoft's Ireland-based Smart Card Certification Center for Windows Vista with its StarSign IT security solution products. Using Smart Cards from the StarSign family of products, PC users can securely authenticate themselves on networks and for IT applications. The compliance with Microsoft's certification requirements confirms that StarSign lives up to the quality standards set by Microsoft.

Microsoft's Smart Card Certification Center has been working closely with early adopters of the Windows Smart Card Framework to develop a certification program that balances the needs of both Microsoft and IHVs. The result of this close cooperation will be a fully fledged certification program that will award "Designed for Windows" logos for card minidrivers and smart cards that meet the Windows Vista logo program requirements for smart card minidrivers. Microsoft's Smart Card Certification Center is located in the Ireland based European Development Centre.

H-P Smart Cards for Government

Hewlett-Packard has launched a new Common Access Card that federal agencies will need to issue to comply with Bush administration directives on homeland security. Federal employees can use the H-P Common Access Card to authenticate their access to government networks and for secure printing and imaging solutions, as required by Homeland Security Presidential Directive-12. It will be available in the United States in July and elsewhere later in the year, according to H-P.



ST Partners with Gemalto

STMicroelectronics (ST) has announced a single-chip microcontroller solution intended for both PC-integrated and freestanding Smart Card applications resulting from a partnership agreement with Gemalto. The new ST7GEM is a secure MCU in ST's ST7 family, pre-programmed with Smart Card interface software from Gemalto, and requiring the addition of only a few passive external components to become a complete embedded Smart Card reader solution.

Sagem Launches Biometric Terminals

Sagem Défense Sécurité has launched two new biometric access control products. They are the MorphoAccess 500, a physical access control terminal, and MorphoSmart 1350, a logical access control reader. The MorphoAccess 500 has a new electronic platform and a new biometric (fingerprint recognition) sensor, and it can identify up to 50,000 people. The MorphoSmart 1350 is a new USB fingerprint reader for logical access control applications. It meets the needs of companies looking to use Smart Cards with biometrics to secure computer access via strong authentication.

New Card and Fingerprint Reader

Assa Abloy Identification Technologies (ITG) has introduced a new OMNIKEY Smart Card reader that combines contact Smart Card technology with fingerprint recognition. The contact based desktop device is especially designed for logical access control systems in high security environments. Using modern stripe sensor technology, the OMNIKEY CardMan 7121 allows threefold authentication via card, pin and fingerprint.

New Smart Card Based Encryption

Wrocklage Intermedia GmbH has launched the Aloaha Smart Card Connector. The Aloaha Smart Card Connector allows applications to use Smart Card based cryptographic services via Microsoft Cryptographic API, PKCS #11 or Aloahas native Card Interface. "The Aloaha Card Technology existed already for a long time in our PDF Products and it was just a logical step to open our proven technology to other applications," explained Stefan Engelbert. "With the Aloaha Smart Card Solutions any user can now experience the advantages of the new electronic ID Cards such as National ID Card, Health Cards or commercial Signature Cards."

On The Move

Ex Australian Minister Joins ASG

Former Australian federal minister Ian Campbell has joined the board of ASG, a Perth-based Smart Card company, that could tender for the \$1.1 billion Smart-card project - one of his projects. During his time in government, Mr Campbell - who was forced to resign in May after admitting he had met disgraced former West Australian (WA) premier Brian Burke in his Perth office - had responsibility for the Human Services Department, which controls the highly technical Smartcard project. The troubled project aims to issue 16 million photographic identity cards for Australians to replace 17 existing welfare identity documents with a single piece of plastic. ASG has contracts with a number of federal and state government departments including Prime Minister and Cabinet, WA's Justice and Victoria's Education departments, and a spokesman for ASG said the company would continue to seek state and federal Government contracts.

L-1 Bolsters Federal Marketing Team

L-1 Identity Solutions, Inc has added further depth of experience and expertise to the Federal government marketing team with the addition of Rear Admiral Jeffrey J. Hathaway and Frank E. Moss. Admiral Hathaway is the former director of the Joint Interagency Task Force South for the US Coast Guard and will serve as a full-time Vice President of Federal Programs for L-1, beginning June 1, 2007. Former Deputy Assistant Secretary for Passport Services for the Department of State, Frank Moss, began serving as a consultant to the L-1 Federal Program on May 1, 2007. Both individuals will leverage their extensive backgrounds in Homeland Security-related issues to develop relationships with various Federal agencies driving identity-related national and international programs.

e-Smart Welcomes New COO

e-Smart Technologies has announced that Richard Barrett has been named Chief Operating Officer of the Company. As COO, Barrett will oversee the Company's product development and implementation and serve as a strategic partner with the Chief Technology Officer and engineers. Barrett will manage operations to deliver payment solutions and secure financial transaction systems for the company's clients around the globe.



NFC in the Real World - Part 2

By Innovision Research & Technology Plc



This article follows on from Part I of Innovision's '*NFC in the real world*'- which took a high-level look at NFC applications, technology and markets - and aimed to help NFC product and service developers identify the suitability of the four NFC Forum-mandated tag types for various applications. The first mass-market applications for NFC will almost certainly be in relatively low-financial value applications - with low risk of fraud - that do not require large investment in new back-end infrastructure. These applications are likely to build on existing payment and communications infrastructure and user behaviour, where the user benefits are most compelling, the business case is strongest, and the commercial risks are lowest.

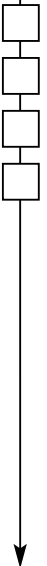
Section 1: Key NFC applications - Innovision sees three key areas of application for NFC: service initiation, where the technology is used to 'unlock' another service (such as opening another communication link for data transfer); peer-to-peer, where NFC is used to enable communication between two devices; and payment & ticketing, where NFC will build on the emerging smart ticketing and electronic payment infrastructures. In peer-to-peer applications, NFC can be used to set up local communication between two devices. For relatively small amounts of information (up to a few kilobytes), NFC can be used to transmit the data itself, as this can be exchanged during the short period of time the NFC devices are touching each other. However, for larger amounts of data, NFC is more likely to be used to establish a separate wireless connection (such as Bluetooth or WiFi) to carry the content to be exchanged. A typical peer-to-peer application would be printing photos straight from a picture phone or digital camera: the user would simply select the photo or folder to be printed and then touch the device against the NFC-enabled printer to establish a Bluetooth connection to transmit the digital photos.

Credit card merchants, banks and mobile network operators see value in putting payment and ticketing applications on NFC-enabled mobile phones, and this was one of the drivers for the creation of the NFC standard. For the credit card merchants, NFC-enabled payments are much easier and less costly to handle than cash and other traditional payment methods. In addition, users will have a record of even the smallest payments, which they do not with cash today. Initially, NFC-enabled devices are likely to be used for low-fraud, limited-value payment situations, such as quick-serve restaurants, kiosks, vending machines and parking meters. With service initiation, the user touches an NFC-enabled device against an NFC tag, which then transfers a small amount of information to the NFC device, which may be some lines of text, a web address (URL), phone number or other simple piece of data. Smart posters promoting new products, services or events are examples of this type of application. By touching an NFC-enabled mobile phone against the NFC tag embedded in the poster, the user may be directed to a web site for further information or to book tickets without the need to key anything into the phone to open the browser or input the URL.

Section 2: NFC mandated tag types - The service initiation use case requires two devices to communicate using NFC, one device is an NFC reader/writer and the other a passive NFC tag. In June 2006, the NFC Forum introduced standardised technology architecture, initial specifications and tag formats for NFC-compliant devices. These include Data Exchange Format (NDEF), and three initial Record Type Definition (RTD) specifications for smart poster, text and Internet resource reading applications. In addition, the NFC Forum announced the initial set of four tag formats that all NFC Forum-compliant devices must support. These are based on ISO 14443 Types A and B (the international standards for contactless smartcards) and FeliCa (conformant with the ISO 18092, passive communication mode, standard). Tags compatible with these mandatory formats are available initially from Innovision, Philips, and Sony, and already more than one billion tags of this kind have been deployed globally, albeit for non-NFC applications like mass transit and access control. The NFC Forum chose the initial tag formats to cater for the broadest possible range of applications and device capabilities:

- Type 1 is based on ISO 14443 A and is currently available exclusively from Innovision Research & Technology (Topaz). It has a 96-byte memory capacity, which makes it a very cost-efficient tag for a wide range of NFC applications





- ❑ Type 2 is also based on ISO 14443 A and is currently exclusively available from Philips (MIFARE UltraLight). It has half the memory capacity of Type 1 tags
- ❑ Type 3 is based on FeliCa and is currently exclusively available from Sony. It has a larger memory (currently 2kbyte) and operates at a higher data rate (212kbit/s), which means it is suitable for more complex applications
- ❑ Type 4 is fully compatible with ISO 14443A/B and is available from a number of manufacturers, including Philips (typical product example is MIFARE DESFire). It offers large memory-addressing capability with read speeds of between 106kbit/s and 424kbit/s - making it suitable for multiple applications.

It is worth noting that Type 1 and 2 tags and Type 3 and 4 tags are two very different groups, with very different memory capacities. There is very little overlap in the types of applications they are likely to be used for.

Section 3: The right tag for the job - With four NFC Forum-mandated tag types to choose from, designers need to consider carefully the relative merits of each before committing to one type or another. With initial mass-market deployments likely to be in low-financial value, low-risk applications, it is important that NFC tags meet the requirements with the right balance of cost and performance. There will also be more specialist applications that require greater tag capabilities, and that are less sensitive to cost and size considerations;

1) *Smart Poster* - In this application, the user touches his or her mobile phone against a tag embedded in the poster itself, which triggers the transmission of a URL to the phone. This URL could be used, for example, to direct the user to a web site where he or she can find out further information or download a special coupon or token. The trade-off here is to have a tag that is small and low-cost enough for mass deployment, but with sufficient memory to contain a reasonably long URL and some additional security features.

2) *SMS or phone number shortcut* - in this case the user can automatically send a text message or phone number by touching the phone against a tag that could be embedded in all sorts of objects. One possibility is the provision of 'tags in a box' with new mobile phones. The user would be able to save a phone number or text message on the tag, which is embedded in a sticker. Tags could be affixed to photo frames and used to obtain the phone number of the person in the picture, which could be for fun or be a very useful facility for the elderly or disabled. Tags containing SMS text could be stuck just inside the front door at home so that children returning from school could touch their phones and automatically send a text message to their parents. In this case, small size and low cost are the main considerations, as the memory requirements are small.

3) *Bluetooth pairing* - This is essentially a 'handshake' between two devices - for example, a mobile phone and a hands-free headset, or a digital camera and a printer. This is a fairly infrequent occurrence, but is made much more convenient by NFC. Generally, only a small amount of memory is required, and small size, low cost - with low risk of 'tearing' the data transfer - are also the watchwords here. Larger memory may be useful in applications that also involve the automatic transfer of some data between the two devices.

4) *MMS or ringtone downloads* - In this application the user could touch a product or promotional piece, for example, to get an associated picture message or ringtone automatically transferred to his or her phone. Once again, small size is important, but so are sufficient memory and security features. The larger the memory capacity on the tag, the more information that can be transferred directly to the phone. However, one has to consider the limitations arising from the short 'touch time' between the NFC device and the tag. In practice, this sets an upper limit for the amount of data exchanged to just a few kilobytes during the touch.

Type 1 and 2 tags are dual state, which means that they can be read/write or read-only (as shown in Figure 1). Type 3 and Type 4 tags are single-state, which means that they can only ever be read-only, rather like officially published CDs or DVDs. This means that in applications such as the 'tags in a box' one described above, only Type 1 or 2 tags can be used, as Type 3 and 4 tags cannot be personalised by the user. The read/write memory capacity offered by the NFC tag is an important consideration, particularly in mass-market applications, as more memory comes at the expense of unit price and footprint. For example, in smart poster applications, greater memory translates into longer URLs and greater security options. The larger memory offered by Type 3 and 4 tags could be useful in certain applications - for example, for high data content downloads such as MMS or ringtones - but is overkill for smart posters and Bluetooth pairing.



However it is important to balance cost with capability in this area, especially when some level of security is required. For example, it will be desirable to protect smart posters from fraudulent copying or tampering to change the URL or phone number provided in public environments. There needs to be sufficient memory to provide a full URL even when a digital signature is required. After writing data to a tag, it can be locked to read-only mode to prevent it being overwritten or altered in any way. Locking the tag to read-only means no-one can modify the tag once it has been published, and is an irreversible process. This is an important security and privacy feature that only Type 1 and 2 tag formats offer.

The unit price of NFC tags is influenced by a number of factors, including memory capacity, the number of additional features and IC complexity. The price of the tag is naturally a key factor in determining its suitability for certain applications. For example, if the IC is only to be used for Bluetooth pairing in a hands-free headset - which users only need to do on a handful of occasions - features like high read speed and large memory are irrelevant. The die size area of the NFC tag is influenced by the amount of memory, the complexity of the chip and the efficiency of the IC design. Compact tags are clearly better for applications where unobtrusive positioning is important, and where integration on to other chipsets may be required. In smart poster applications, Type 1 and 2 can provide a much more appropriate balance of cost, size and memory capacity than Type 3 and 4 tags. The read speed offered by a tag is an important factor. The higher the read speed, the less chance there is of a read/write 'tear' occurring, where data is not fully or properly transferred while the tag and reader are in close proximity. Therefore the read speed has a direct impact on system reliability and user experience. In smart poster applications this will be important, as users will appreciate speed and convenience and not wish to keep trying and retrying. The proprietary 'Read All' command in Type 1 tags enables the whole content of the tag to be read in one shot, rather than a block at a time - which improves read performance considerably.

Section 4: Summary - The large-scale success of NFC is dependent on the availability of NFC tags with the right capabilities and the right price point. It is important for designers to consider what the best balance of tag capabilities and cost is for their applications. It is likely that the first mass-market applications for NFC will build on existing infrastructure, initially in relatively simple shortcut, identification, service discovery/initiation or device pairing applications. This implies the need for a standardized tag format that is small, low-cost and flexible enough to be successfully integrated into existing form factors and integrated circuitry.

Part 3 will be published on our website - www.smartcard.co.uk

Document Security is More Than a Secure Document



By Karsten Neugebauer, CEO, SAFE ID Solutions



Karsten Neugebauer

Identity verification of travellers is one of the most discussed topics in the government sector caused by growing tourism and globally operating terrorism - especially in combination with the promises raised by the introduction of electronic passports. The following article wants to give an overview of the market's status quo in the view of a personalisation solution provider and analyses central challenges as well as approaches to face them. Increasing demand for secure passport issuance systems has tremendously pushed the availability of innovative solutions in the market:

Various printing technologies, security features, RFID devices, chip operating systems as well as complete management platforms for full control from passport application to final hand out can be delivered. A perfectly customised solution enabling full loop security and maximised efficiency is no more a vision but a realisable demand - at least on the technological side, the required products and preconditions are available.



Document security depends on the entire process chain - Exaggerated promises created the impression that RFID is the ultimate answer to all security needs by simply implementing it into travel documents. Resulting unrealistic expectations led to massive confusion when governments and citizens are confronted with press headlines saying that national ePassports have been cracked within only five minutes. Perhaps ePassports are only an expensive but useless version? Let's first analyse the case of the UK passport hackers that have attracted a lot of attention a few months ago: They were able to read personal data from a passport chip and to copy it to another device. What sounds alarming first is really not worth placing the whole ePassport in question. To reproduce this feat no security hurdles have to be circumvented.

The only requirements are a passport and a standard scanner with the capability to read the chip access keys from the passport's machine readable zone (MRZ). This is neither impressive nor very dramatic as long as the data set cannot be manipulated. Personal information included in a travel document can be seen by every person who is in possession of it - reading out the chip reveals no details that would not have been discovered by simply looking at the data page. Also the cloned chip is no real threat because who else other than the original passport's owner can use a cloned document containing his face image and signature? This case indicates that the security of a passport personalisation and issuance system not only depends on the final document but much more on the underlying processes. Facing these challenges requires a holistic security concept that e.g. considers factors concerning the personnel level, the data flow and the overall process tracking.

Fulfillment of the Security Levels - The document layer defines the security of the physical ID document itself which is defined and increased by features like RFID, holograms, security inks and special laminates. All other layers are related to elements and processes preceding the final document issuance. The infrastructure comprises the physically secure personalisation center and secures network structures. Safeguarding and controlling on the production level is e.g. realised by the assignment of keys for chip personalisation and unique system setup while the subordinated process security needs a more holistic including a sophisticated system of e.g. key management, log files and quality checks.



Document security does not only focus on the document itself, but the entire environment from infrastructure to production.

At least it is also important to setup a management system to control and track the operations within the production and to provide secure logins to the personalisation system. The fulfillments of all these levels require that the solution provider knows the environment and situation of the customer.

Secure Personalisation of ePassports - The secure production and administration of state of the art travel documents therefore requires, next to the latest production hardware, a well defined, highly secure production and personalisation process along with proper key management and life cycle management capabilities. The production of electronic passports is significantly different to standard passport manufacturing as two mechanisms are of critical importance:

- 1) The electronic component received from a semiconductor manufacturer, must have a unique identification number; the same applies to the passport booklet from the security printer. Additionally, once the ePassport manufacturing is completed, the chip identification number and the passport identification number must be linked together as one entity, thereby uniquely identifying the booklet for the entire life cycle of the document.
- 2) The chip must be protected against read and/or write access by unauthorised parties trying to tamper with the device in any stage of the production or personalisation process.

Passport forgery and fraud mainly rely on the fact of limited control over the issued document and the exploit of known weaknesses. A state of the art system automatically controlling all process steps tightens the security around the passport.



Managing the personalisation process - One of the most impressive progresses in the passport market is the availability of complete personalisation management systems that can centrally manage, control and monitor all elements and processes involved in a personalisation workflow. These products are becoming the core of every passport project and are defining its overall reliability, security and efficiency. The personalisation management system houses the production database, receives batches of passport personalisation jobs from the government and distributes those batches to all the personalisation systems available for production, be it in a single personalisation facility or in various remote locations. For the communication to the government site and the personalisation equipment, the system needs to use encrypted links in order to protect personal data against eavesdropping. The hardware and software of the system is authenticated after each start-up including mandatory operator log-in. All personalisation systems connected to the system must authenticate them before receiving personalisation data from the server to ascertain that only proper machines are used in the proper environment.

In the case of an electronic passport, the personalisation management system will receive the access keys from the key management system and will pass it on to the equipment for personalisation of the chip. Furthermore the personalisation management system oversees: **1)** Tracking the personalisation of all passports, **2)** Allocating of personalisation jobs to the equipment and controlling of production status of each document, **3)** Monitoring status/performance of all equipment and reallocating jobs to other machines in case of a machine breakdown. All information about personalisation jobs received and all passports produced will be stored in the proper database. The software allows the supervisor to run daily, weekly or monthly production reports by machine, operator, and passport number or production status, thus effectively monitoring the production environment and proposing corrective measures.

Security concerns are well addressed by the personalisation management solution, taking care of a number of security related functions such as: **1)** Machine start-up, logging and software sanity check, **2)** Access control system based on user log-in via PIN, Smart Card and PIN or biometrics, **3)** Communication with the Personalisation Management System via encrypted lines, **4)** Key handling and personalisation of the RFID-Chip using customer specific encryption formats and protocols, **5)** Retrieving passport personalisation data, logging and feedback of all production data of each individual passport to the Personalisation Management System.

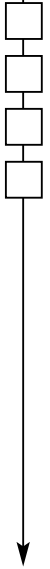
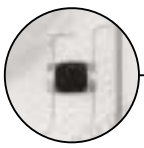
From the point of view of a supplier in the passport personalisation sector this means that the solutions offered should be based on latest technological achievements and be easily customisable or in best case totally modular. They need well defined interfaces to guarantee optimal integration into existing infrastructures and provide high scalability, perfect reliability and a highly user-friendly design. A company has to offer more than just a convincing product portfolio but needs deep understanding of all processes related and adjoined to its core competence as well as long-time experience in realization of passport systems.

New Uses of ePassports: Automated Border Crossing and Beyond



By L-1 Identity Solutions

The electronic cards industry is maturing quickly, most recently with ePassports blazing new trails and methods for identifying people around the world. In a few short years we have moved from static "dumb" passports to smart ePassports which hold a wealth of identity information in a remarkably small chip on the card. The chip in the passport, typically housed on the printer page, is the enabling technology which leads us to call these credentials "smart". The chip, which conforms to international standards, simultaneously, turns the passport into an electronic read/write record most commonly containing biographical data, digitized face images and fingerprints, and the key to unlocking this identity information. The combination of ePassports, biometric solutions and document reading and authentication technologies enables basic access control (BAC) - the process of providing a secure means to read the data on the chip through decryption of the chip, reading the data via the machine readable zone (MRZ), and producing a result to allow or deny access - to work effectively.



Since conception, ePassports were designed to enable higher security in international travel and the promise is being fulfilled. The introduction of ePassports has ushered in a new era of security and convenience for both organisations and card holders as the capabilities of this new passport allow travelers to own their identity data and organisations to use the data for automated border crossing, immigration and secure identification. Now we are just beginning to realise the added benefits and potential of ePassports, from superior identity theft and fraud protection and more efficient immigration through unattended crossing points, to new concepts such as elections quality assurance, worker permit vetting, secure banking, informed health-care, and convenient e-commerce.

As the world progresses toward this new, smart form of identification, today there is a mix of traditional passports and ePassports on the market, therefore internationally the former means of identity document authentication coexist with the new cutting-edge methods of identity document authentication. Both traditional passports and the new ePassports may be authenticated using automated document authentication technologies which are flexible in terms of reading contact and contactless, or "dumb" and "smart" forms of identification. While estimates indicate that traditional passports will be phased out over the course of ten years, there are two unmistakable truths: 1) the move toward smart ePassports is inevitable and 2) the momentum on transitioning to smart ePassports is growing worldwide.



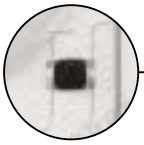
Recently, Portugal's Faro airport launched a groundbreaking pilot program designed to test the effectiveness and efficiency of ePassports in unattended border crossing. Imagine a secure border crossing process that quickly processes your passport, checking the validity of your identification and your identity information to determine your eligibility to enter the country, while simultaneously expediting the process, eliminating the need for human intervention and allowing you to hold the keys to your identity.

This is the solution available today in Portugal. In seconds, your passport and identity information, including biometrics such as face and fingerprints, are scanned against watch lists, authenticated against passport source data, and cross checked to match the printed document data against the data on the chip. The early success of the pilot in Portugal is already expected to lead to a full deployment of automated document authentication and unattended border crossing kiosks throughout all of Portugal's international airports and maritime ports. In 2004, Pakistan also launched an ePassport in combination with the country's national ID card. The integrated solution was designed to heighten national security, most notably through mitigating terrorism and ethnic violence, and prevent problems related to identity theft and the fraudulent use of identity documents by leveraging the instant access to biographical identity data, face biometrics and fingerprint biometrics. This solution has been highly successful in accomplishing its goals and furthermore, connecting Pakistan's citizens to the country's public and private services from government programs and law enforcement to banking, education and travel.

Today the United States, twenty-seven European Union countries and several Asian Pacific countries such as Japan, Malaysia, and Thailand have begun issuing their ePassports, and countries like Portugal and Pakistan are leading the charge on how to take advantage of this significant investment, maximising the application of ePassports and meeting the modern demands for the use and security of individual's identities. Successful ePassport cases are leading to more innovative thinking around the use of passports.



Just as national ID cards and driver's licenses have been frequently repurposed and used for general identification in banking, healthcare, and commerce, the ePassport has the same potential. The capacity of a chip on a passport is vast, and exceeds the thoroughness, convenience and security of any other form of identification. Envision the scenario in which your passport carries critical healthcare data, personal banking information, credit access, voter rights, worker eligibility, and a range of other government and private services. Each of these systems could benefit from the security, efficiency and convenience of a universally accepted and advanced form of identification such as the ePassport.



Healthcare is perhaps the most personally compelling application for the extension of the ePassport. As healthcare worldwide has become more complex and we have become a more mobile society, the healthcare system has been challenged to find a solution for maintaining electronic healthcare records for individuals and providing instant access to patient data. Further, as technology has made access to worldwide resources and opportunities more readily available than any other time in history, international travel is more commonplace, and therefore the need for mobile electronic healthcare information is all the more prudent.



The ePassport is a fitting option for identifying individuals and accessing their vital healthcare information that may be stored elsewhere. From a macro-economic view, the influence of banking and commerce on our global welfare provides incentive to extend the ePassport in this direction. Again our new found, ultra-mobility and need for protection of our identity drives the case for inclusion of banking and credit line access using our ePassports as electronic forms of identity verified with embedded biometrics.

As with other applications, the finance industry bears a heavy burden for verifying identities in order to prevent identity theft and identity fraud which often led to more destructive crimes. Once again, the consumer is an integral part of the solution as the individuals maintain ownership of their identity document and data. When we further consider the advanced uses of mobile phones, which are quickly becoming mini-computers helping to organise our lives, conduct transactions, and link into our mobile society, the chip on the ePassport would complete the solution for full identity verification and secure commerce in combination with other wireless communications technologies like 3G wireless, Bluetooth and WIFI/WIMAX.

Moving into the political world, we find additional potential for innovative applications of the ePassport. Worldwide, the quality of elections and voter verification process has come into question in several high profile cases. The fact is that paper based electoral and voter authentication systems are quickly becoming outdated due to the static nature of these conventional processes and the significant loop holes that exist in these systems. Appending voter rights information to ePassports would enable many countries to efficiently authenticate voters, build quality assurance into the election systems, and process voting results more quickly. Passports, by purpose and design, are tied to government services; therefore the extension of ePassports into other government services is not a stretch. Take for instance the systems for providing foreign worker permits which vary from country to country. It is generally accepted that most of these systems would benefit enormously from having instant access to worker eligibility information on a trusted and universally accepted form of identification, such as the ePassport. Again, ePassports deliver unparalleled processing times, reliability, and convenience, particularly for on-site verification of workers.

Each of these ePassport applications has the potential to help further develop and evolve the ePassport into a broadly used form of identification providing exceptional security, efficiency and convenience to both organisations and individuals. However as we advance toward these uncharted territories we must also step back and consider some of the broader issues that will enable the successful evolution of the ePassport. For example, we must agree upon the standards for ePassports.



Most all countries follow the recommendations of ICAO and adhere to the ISO standards for the electronic chips and images, however there is still wide variation among countries. While certainly there will always be differences among the countries' ePassport solutions, we will be wise to stay focused on solutions that enable all ePassport holders to access the advantages provided through this new technology, including international travel, security and added conveniences in public and private services. Migrating from our established systems to take advantage of the capabilities of the ePassport would require collaboration from every sector and country.

As we learned through the early implementations of ePassports, these solutions take time to implement, especially when the standards are being set almost simultaneously with the solutions. However when considering the tremendous opportunities and benefits presented by the ePassport, the case for collaboration is compelling.



Rumours From the Front Line

By "The Squeaker" (*a source who wishes to remain anonymous*)



How do you charge more for a cup of coffee? Economists the world over dedicate themselves to answering this question, not just for coffee of course but also for their own particular commodity of choice and in our case Smart Cards and I think by now we've all agreed that it's a commodity we are dealing with. The case of coffee has been well studied, after the Location, Location, Location criteria for the retail trade we can get around to sprinkling on those extras and by having a variety of sizes which attract the higher margins.

We can even appeal to people with the Fairtrade ingredients which seem totally balanced in favour of the retailer but in short we need to give people what they need at the highest possible margin. For those of you interested in hearing more I can recommend "The Undercover Economist" by Tim Harford which also tells you a lot more than just about the coffee. So let's look at the Smart Card business, location here has a different meaning. Where should I site my factory to have the lowest overheads? And that usually means labour costs. All the major card manufacturers from Gemalto to ID Data are moving their factories to the cheaper parts of Europe or even to Asia. We might conclude that this should have a neutral effect because all the major companies are playing in this area at least on level playing fields.

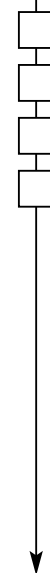


Now in terms of choice the consumer, in this case the Network Operators for SIM cards and the banks for EMV cards have pretty well a fixed specification. What is the differentiator? How can the card manufacturers add a little bit of chocolate for which the customer will pay more? It's difficult to see any real margin on the plastic, after all the security has been moved to the chip and all the card companies have access to the same chips no matter how much the memory which is the main price contributor.

So what does all this tell us? In the first instance there is not much scope for new entrants, the current incumbents will be fighting to hold market share. In fact there must be even more consolidation on the way. It's clear that the major card companies have to adopt a new business model and the only differentiator is the software. That can be at any layer in the value chain from the operating system, through card applications and middleware to the scheme application. The problem here is that in the core of the business, SIM cards and EMV cards the functionality of the card is fixed and open to all suppliers. The terminals that handle the cards are however more proprietary but are not within the traditional business of the card companies who neither make phones or POS terminals. Card management systems are very much within the remit of the card companies and the bureau services for provisioning the cards. Moving just a little up the value chain is the middleware that uses the card usually as some part of an Identity Management process. The question is who owns this space?

The first issue to look at is card personalisation, is that also going to become a commodity? The answer depends on what is likely to be involved, simple card configuration can easily be undertaken, and there is no real barrier to entry. Security is undoubtedly going to be the name of the game. Once you start getting involved with public key infrastructures and all that goes with it then you are entering a different world and here in my view is the new battleground. In one field we have the major card companies such as Gemalto with a long history in Smart Card security and the surrounding cryptography. In the other field there are the security companies such as Entrust well established in the management of public key infrastructures and then in the middle the specialist card management companies such as ActivIdentity and Intercede.

How will the pot get distributed? Back to the coffee again, the greatest barrier to entry is in the control of the security domains. The customers are going to be filtered down a small number of paths, that's where I would like my coffee shop.





The Enterprise Identity Challenge

ActivIdentity

By Marc Hudavert, Vice-President & General Manager, ActivIdentity



Marc Hudavert

Identity management is acknowledged as one of the key priorities for enterprises to address but, the separation between physical and logical controls in organisations has a huge impact on their ability to manage access effectively and demonstrate a strong financial return. In this article I'm going to outline some of the limitations of identity management and address how the evolution of identity assurance is helping the enterprise to increase security, productivity, achieve compliance and return on investment (ROI).

Challenge 1: Complexity of the IT infrastructure - One of the greatest challenges in identity management is the sheer complexity of the IT infrastructure. The need to add applications and functionality to support the growing business, while maintaining established core elements of the network, indicates that continued expansion is inevitable. Mainframes still support the infrastructures of many large organisations, and the variety of operating systems in use and demand for countless applications to sustain the business cause two major problems in the context of managing identities. Firstly, there is the technical issue of providing and controlling access to each system or application and, secondly, the onus is placed on the user to find ways of managing the log-in details for a plethora of applications. The latter explains why the practice of writing password and log-in details on Post-it notes has become so endemic. The overwhelming majority of users are not tech savvy - it's not their job to be - and streamlining their interaction with the IT infrastructure is an essential component of effective identity management.

Challenge 2: Mobile and remote working - The complexity of the IT infrastructure is compounded by the growing demand for mobile and remote working practices. This trend is expanding the contact perimeter of the modern enterprise and brings with it an inevitable security challenge. The means through which access is made available (e.g. terminal server, PDA, laptop, smart phone, etc.) are many and varied, with each type of access requiring its own technological solution to ensure effective control. Not only does this incur extra cost, the inconsistency of the various interfaces also further complicates the experience of users who may be using tokens for certain applications, encryption for others and single sign on for web applications.

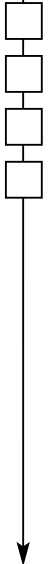
Challenge 3: Budget pockets - The structure of many large organisations can be a significant hindrance when it comes to effective identity management. With logical access traditionally under the domain of IT and physical building access controlled by facilities, or even HR, it's not uncommon for disparate budgets which fund technically un-related systems to exist in an organisation. Furthermore, it's not unusual that physical security budgets are considerably larger than those available to IT, despite the increased reliance on the network by some physical security components. This is a particular problem for the global enterprise. In addition to the expense associated with managing individual physical and logical systems, there may be no common infrastructure between the systems used in different offices, and sometimes even between different departments on the same site.

Strategies for identity assurance - Faced with these challenges, the case for collapsing logical and physical access is being realised and implemented by a growing number of organisations. Underpinning this trend is the increasing appreciation of the capabilities and developments within Smart Card technology. Although, the Smart Card was invented more than 20 years ago, it's only over the past three to five years that its development has really accelerated. Initial Smart Card implementations tended to be stand alone, single function add-ons which were application focussed in their nature (i.e. providing PKI certificates for email signing). They also tended to be static. As such, once the card had been issued it could not be amended and additional cards had to be used for each new application. Because this results in staff carrying multiple cards and the organisation financing the administration and management of each card, there is a perception that the technology is both cumbersome to use and expensive to deploy. This view is not entirely unfounded, but it does not apply to the Smart Card of today. The Smart Cards that are now deployed in the enterprise are neither static, nor single function.





With the ever increasing pressure on IT budgets to deliver more functionality for less, it's no longer economically viable to have multiple cards per staff member. Furthermore, the rise of governance and compliance demands has also placed greater emphasis on the importance of the integration of authentication technologies with the broader IT network, and major IT infrastructure vendors, such as Sun and Microsoft, have recognised this and made their latest platforms Smart Card ready. Smart Card technologies are now enabling organisations to consolidate multiple credentials onto a single device to provide consistent, secure access to both building premises and IT systems alike across the entire business.



The enterprise Smart Card is not just limited to these functions, though, and organisations are already exploring additional capabilities, such as using the physical card as a visual identity badge, or emerging applications like logging employee time and attendance and making payments in the staff canteen. This practice indicates that businesses are acknowledging the importance of converging digital identities into a cohesive identity assurance strategy to maximise the benefits of identity management tools. This approach also facilitates a reduction in security expenditure by eliminating the need for separate budgets to manage individual components (for example, USB keys, tokens, encryption, single sign on, etc.).

It's a marathon, not a sprint - Despite these significant developments, and the growing recognition that the Smart Card has much more to offer now than before, in some arenas the technology continues to be received unenthusiastically. To understand why this view is held, one needs to explore how Smart Cards are being deployed. The reality is that introducing such wide-ranging changes to the IT infrastructure does not just have a technological impact.



It also dictates significant cultural change, the likes of which are bound to provoke negative feedback from users if they are not handled in the right way. The "Big Bang" approach to Smart Card deployment puts huge pressure on technology and human resources, the two key factors which influence the means through which senior management will judge the success of the implementation - ROI. To navigate through the implementation process, businesses must create an identity assurance strategy which demonstrates a quick success and use that as the platform upon which to develop longer term initiatives, both from a technological and business perspective. After all, Smart Cards may be central to a future strategy, but they don't necessarily have to be there at its point of introduction. One trigger for identity assurance strategies that a growing number of our customers are acting on is the password management headache. Password management's pain points are well documented.

The cost of helpdesk calls and impact on frontline workers' efficiency while they wait for password resets are pretty well known throughout the enterprise. In lieu of this, the case for deploying single sign on (SSO) to significantly reduce these overheads is an easy one for the budget holders, end users and the IT department to support. SSO targets a very specific problem and, as such, is able to prove its worth very quickly. By demonstrating this success, it becomes easier to get the organisation on-side and eases the process of introducing further identity assurance measures. However, when evaluating SSO technologies one of the key criteria for any large organisation must be the ability of the new solution to integrate with and underpin future identity initiatives, such as the deployment of Smart Cards. Not only does this add value to the SSO deployment, it also enables the consolidation of other access controls into a single card.

This phased strategy, which places emphasis on ensuring the new or existing infrastructure can provide the foundation for long term identity assurance, is being adopted by more organisations with Smart Cards at its heart. Instead of asking whether or not they should use Smart Cards, they are starting to question how they can leverage the technology to facilitate business requirements such as mobile working and remote access. As a result they are able to gain support from their users and demonstrate clear ROI to key stake holders. The identity challenges outlined above should be seen as opportunities to increase the efficiency of the security infrastructure. Rather than adding further layers to the already complex IT infrastructure, identity assurance enables organisations to streamline access to applications and systems by bringing together the critical security elements and simplifying their management. By failing to create this linkage, enterprises are unable to realise the full benefits of identity management tools.



Directory Services the Backbone of Digital Identity



By John Owen, Technical Consultant, Smart Card News Ltd

We may never have seriously sat down to consider how our corporate identities are stored. However within a corporation each employee has a profile which may include a username, email, photograph, position, role etc, the storage and organisation of this data has close ties with the security design of the system and the digital identity of the users. In this article I would like to give a brief history of directory services and how it has now escaped the realms of the telephone directory and evolved into a much broader storage of digital identities

The International Organisation for Standardisation (ISO) and the International Telecommunications Union in 1988 released the X.500 directory specification standard. The initial goal of the X.500 specification was to set a standard for developing interoperable electronic lookup services. The X.500 standard specifies a directory as being hierarchical in structure consisting of a root object, sub-ordinate objects and object attributes.

This design follows that of a paper phone directory where objects are categories and object attributes are phone entries. X.500 however utilises computer networking so that regional Directories can be linked together to form one national or even global Directory. A user is then able to login to a single web page and obtain up-to-date information from all around the world.

The series of specifications defined by the X.500 standard not only defines the structure of a directory but also the added complexities brought about by a distributed database such as; access control, trustworthiness of data, compatibility & redundancy. The X.500 directory can also resemble that of an organisational tree. People (Objects) relate to each other by rank and each person has their own profile (Attributes). The diagram to the right shows how an army might be organised and managed. In the same way Directory Services are used to manage user accounts on a computer network.



On the release of Microsoft Windows 2000, Microsoft sales teams put a big emphasis on its own directory implementation; 'Active Directory'. The buzz technology phrase was 'group-policy'. Microsoft had tightly integrated directory architecture within its operating systems security sub-system. This enables systems administrators to manage users and computers more effectively. Security is managed by policies, which apply permissions to objects that propagate down to sub-ordinates. Active Directory does not implement a full X.500 directory.

LDAP (Lightweight Directory Access Protocol) first implemented by the University of Michigan in 1993 is a TCP/IP alternative to X.500's Directory Access Protocol (DAP). A Directory Access Protocol defines the format of communication between a Client (The application performing the lookup) and Server (The X.500 Directory). Because of LDAP's compatibility with TCP/IP, it has become the most popular directory protocol. Microsoft chose to make Active Directory LDAP compatible

Directory Services are behind every major computer scheme in operation today, often invisible to the end user but core to the operation of the system. The trick for the future is achieving interoperability between different systems.

www.smartcard.co.uk

Technology Insights