September 2008

Volume 17 • Number 9

Smart Card & Identity News

Smart Cards, SIM, Payment, Biometrics, NFC and RFID

www.smartcard.co.uk

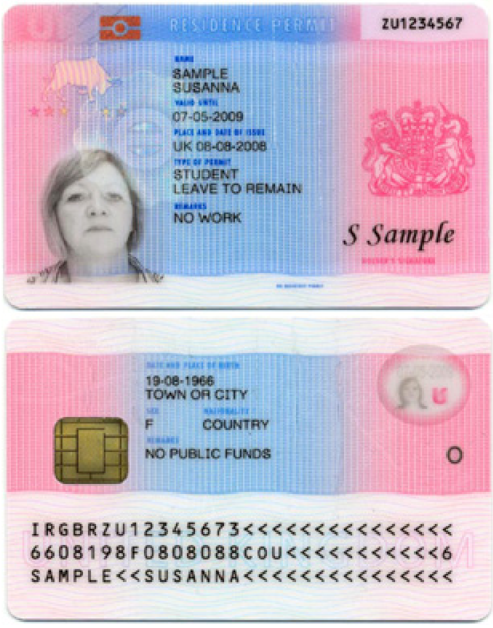
5 • Cryptography Research and Visa Settle Legal Dispute

7 • Fingers will secure our mobile phones

12 • Online fraud – who will take responsibility?

18 • A History of MULTOS: From Mondex to Gemalto

The UK Foreign ID card: Terrorism deterrent or just a soft target?



In late September Home Secretary Jacqui Smith unveiled plans for the first UK identity card for foreign citizens. The move has sparked widespread criticism with suggestions of double motives and brazen xenophobia rife among some sections of the media. Labour's hardy following will be tearing their hair out. Already lagging in the polls, and in the midst of an economic crisis it's a reckless decision by the government to plunder an estimated £351 million on the short-term project.

The Home Office argues that the introduction of an identity card for foreign nationals will tackle 'human trafficking organised immigration crime, illegal working and benefit fraud.' Businesses found employing illegal workers could be subject to imprisonment or fines while all migrants applying to leave or enter the UK will be required to have a card. From November, fingerprints will be taken at six centres across Britain as part of the process in deciding whether an 'applicant' deserves to stay. Ministers predict 90% of foreign nationals will have ID cards by 2015. However, the seemingly endless lists of positives are not as clear-cut as they seem. Many of the benefits will only be recognised when the personal details of large numbers of the British population are stored in a national register, and biometrics hits the

Continued on page 4….

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 691779

Fax: +44 (0) 1903 692616

Website: www.smartcard.co.uk

Email: info@smartcard.co.uk

Editorial

Managing Director – Patsy Everett

Technical Advisor – Dr David Everett

Production Team - Lesley Dann, John Owen

Contributors to this Issue –
Tom Tainton, Precise Biometrics, Hieko Sochart, Steve Brunswick, Herve Naullet

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.

Our Comments

Patsy Everett

Dear Subscribers

This has been a month on identity and biometrics but yet just with the same old chestnuts coming out of the bag. Our lead article this month picks up the media hype of the latest news on the UK National ID card. Yes, it's still moving along and it's going to be mandatory in one or two areas where the audience have no choice. The Tories are still threatening to cancel it once they get into power so no change there then.

Perhaps more interesting is the excitement this time about the e-Passport and the sudden discovery that it doesn't really work and anybody can create a false passport. Now these statements are really a misrepresentation and we have argued against the same accusations about EMV cards. Now I don't profess to be a techie but even I can understand that you can't rely on anything you don't check. So if you don't check the authenticity of the chip then you won't know if you are talking to an authentic chip (e-Passport). Now if it is well known how to read data from a chip and it is not prevented by the requirement to know a secret key then clearly anyone can read the data from a real chip and can also write it to a chip of their choice. For an observer who doesn't check the authenticity of the chip then one e-Passport chip would pass for another.

Now those are the facts but the reality is much more fundamental, an e-passport is in itself a security document which contains a large number of security features which have nothing to do with the chip and the border guards are well trained to look for this level of security. The data on the chip is also protected by a digital signature, which means the data and biometric data, facial image, fingerprints, etc can be easily correlated. Again the same argument holds, if you don't check the signature then you don't know if the data is correct. Nobody has suggested you can create false signatures.

Now we are in exactly the same space as EMV, it is a business decision what data is checked and how. Both EMV and e-Passports (optional) contain non-deterministic secret keys which are not known to the hacker, which means that if a border guard or an EMV terminal (card issuer) does a check then the counterfeit would be immediately recognised. The only problem with the e-passport scheme is that they don't seem to have worked out how to distribute the public keys necessary to check the signatures but hopefully within the UK that shouldn't be a problem.

Closer to home this month we have been having an uproar about the taking of children's fingerprints in schools a scheme which originally started with government sponsorship in 2001. The latest episode is Waverley Primary School in Doncaster, South Yorkshire (UK). Mothers have been complaining about the invasion of personal liberty. Apparently the State is going to collect this information and then lose it so that the children suffer from identity theft. Well I can't really defend the State for losing personal information but I do think this latest uproar is somewhat misplaced in its own right. And up

there at Waverly well they just planned to use the fingerprint as a form of identity for library cards, an object of interest for the children and also an introduction to the concepts of identity verification. I seem to remember we did things like this at school but with ink and a piece of paper, mucky stuff and even more fun. I don't remember worrying about identity theft.

Yes folks its November just around the corner and the event of the year, Cartes 2008 is with us once more. I also have some news, based on well informed insider knowledge, there is not going to be a rail strike this year. Apparently because the exhibition occurs a week earlier the timing would put the rail staff on risk of losing holiday money. Yippee! Here's looking forward to meeting you all once again and this time we can safely stay down town.

Patsy.

Contents

Regular Features

Lead Story – The UK Foreign ID Card ……………………...……...…… 1
Events Diary ………………………………..…...…………………… 3
World News In Brief ……………..……………………………....… 5,8,11,16

Industry Articles

Fingers will secure our mobile phones ……………………………….... 7
Smart Cards and PINs in an Online Environment ……..…..……...……. 9
Online fraud – who will take responsibility? ....……..……………………… 12
Electronic Visas: the future of eTraveling? ……………...…...………. 14
A History of MULTOS: From Mondex to Gemalto ………....……...... 18

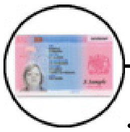
Events Diary

October 2008

14	Travel 2020 - London, UK
15-16	Storage Expo 2008 - London, UK
21-22	Symbian Smart Phone Show - London, UK
22-23	Prepaid Cards Summit 2008 - London, UK

November 2008

4-6	Cartes 2008 - Paris, France
10-11	Mobile Money Transfer 08 - Dubai, UAE
11-13	7th Asian High Security Printing Conference - Bangkok, Thailand
18-20	ID World International Congress - Milan, Italy



…. Continued from page 1

mainstream. That'll be the National Identity Scheme then.

While Jacqui Smith and her cronies continue to laud the brilliant potential of the foreign citizen card, the underlying belief is that the Home Office is bracing the United Kingdom for the roll-out of National Identity cards. It has worked elsewhere, in France for example, 90% of the population carries one. Despite delaying the introduction of ID cards until 2012 Labour is still as committed to the cause as they ever have been. The Home Office said the ID scheme would be £1 billion cheaper than originally planned, and disastrously promoted the supposed benefits in the hope that the project will be 'consumer led' – with people signing up voluntarily rather than being dragged kicking and screaming. Needless to say the plan didn't work. Not helped by Revenue and Custom's loss of 25 million personal details, public support for ID cards is at an all time low.

The government's appalling record of data protection, combined with fears of infringements of civil rights and privacy intrusion have led many citizens, including the Tories and Liberal Democrats to strongly oppose the idea. Phil Booth, Director of NO2ID said, "The government is picking on soft targets, People who have no choice but to comply. They are using vulnerable members of our society, like foreign nationals who do not have the vote, as guinea pigs for a deeply unpopular and unworkable policy."
It's a pretty cynical piece of politics to pick on the foreign nationals first. This could easily backfire on Gordon Brown. There are fears that the cards will cause friction among ethnic minorities and force illegal immigrants into avoiding contact with hospitals and police. And let's not forget the £30 initial fee for a stand-alone identity card.

The introduction of cards for foreign nationals will be closely followed by the first cards for British citizens, targeting workers in sensitive roles and locations such as airports. However trade unions and airport workers have protested claiming the cards will not improve airport safety. The initial targets of the compulsory foreign ID card are students, and partners of permanent residents. Jacqui Smith explained, "We want to be able to prevent those here illegally from benefiting from the privileges of Britain." It's difficult to comprehend how a potential illegal foreign student could possibly afford the £12,000 annual fees but fail to afford a visa. And it only gets worse for the student population. From 2010, all students will need biometric cards to apply for student loans, a move that has resulted in protests and marches organised across the country.

Another concern is that the miniscule number of foreign nationals involved in the scheme will have little effect in tackling immigration. Just 60,000 cards will be issued in the next six months to those hailing from outside the European Economic Area (EAA), although ministers expect this to rise to a million cards per year after the system is fully rolled out. The card cannot be issued to people from most parts of Europe as they have the right to move freely in and out of the UK. London's School of Economics professor Dr Edgar Whitley believes for this reason the card may not be commercially viable saying,
"With the cards being issued to a relatively small number of individuals in the first place, its unlikely employers or universities will rush to invest in the necessary systems to perform formal checks."

Home Office ministers expect to sign the key contracts to deliver the £4.7 billion national identity database next year. Officials said contracts would include compensation clauses if the project was unexpectedly cancelled but refused to say how much. EDS and Capita, who are rumoured to have already been promised consultancy jobs, must be licking their lips. The irony is Labour are likely to be unceremoniously removed from power by the time the 2010 election comes around, thus eliminating the chance of an identity register. Of course, the private contractors will still be paid in full.

The government have played it safe and opted not to roll out identity cards to anyone with a vote. The 'plastic poll tax' could undermine hundreds of years of civil rights and lead to racially incited discrimination and abuse. And while Labour are determined to push ahead with such a costly project in any way they can, it seems as if the ID project could make us less, not more, safe. So much for Brown's 'fair Britain'.

By Tom Tainton, Smart Card & Identity News.

World News In Brief

Cryptography Research Inc. And Visa Inc. Settle Legal Dispute

Cryptography Research originally made headlines with the discovery of breaking Smart Card chip security by analysing the power signals to the chip back in 1998.

Inc. (CRI), Fenwick & West on behalf of Cryptography Research filed a complaint in 2006 with the U.S. District Court for the Northern District of California, stating that Visa used its pull in the credit card industry to exclude CRI's solution to a 'smart card' security defect in order to avoid paying licensing fees. Visa originally had a licensing agreement with CRI (Rumoured to be 25c per card), but terminated that agreement and allegedly conspired with MasterCard, creating a monopsony to eliminate standards that integrated CRI's solution to the security defect.

This September Cryptography Research announced that it has signed a definitive agreement settling its litigation against Visa, Inc., under which Visa will become a licensee of Cryptography Research's patent portfolio covering countermeasures to Differential Power Analysis (DPA). The license fee and other settlement terms are confidential per the agreement.

"We are happy to add the world's largest payment system to our growing list of DPA licensees," said Paul Kocher, president and chief scientist at Cryptography Research. "Following the recent announcements of signed agreements with Infineon and Renesas, it is clear that the major players at all levels of the smart card industry are recognizing the value and importance of CRI's DPA technology and the strength of our intellectual property in the area of tamper-resistant semiconductors."

Government Of India Selects Gemalto For Electronic Passport Program

Gemalto has been selected to supply Gemalto’s Sealys eTravel solution to India’s National security printer, India Security Press. This solution is used to start India’s electronic passport rollout for Indian Officials and Diplomats.

This Sealys eTravel offering provides the security and contactless communications component of the electronic passports that are manufactured by the India Security Press. It includes the advanced secure operating system and microprocessor that stores and protects the holder’s digital identity as well as the communications antenna. The passports have been launched for Indian Diplomats & Government Officials initially and in a second stage, the Indian government intends to deploy it for the general public.

Gemalto’s offer is developed in full conformance with the SCOSTA-CL specifications of the Government of India. This combines the international ICAO (International Civil Aviation Organization) electronic passport specification with specifics of the Indian national SCOSTA specifications.

Redesign Of NXP Semiconductors Organisation

NXP Semiconductors (formerly Philips Semiconductors) has introduced a redesign program that will bring NXP to a healthy financial situation and hopefully position the company for future growth. The changes come in response to a challenging economic environment, a weak US dollar, and the reduction in size of the company after moving its wireless business into a joint venture with STMicroelectronics. The redesign program includes major reduction of NXP's manufacturing base, its central R&D, and support functions. This program is expected to affect approximately 4,500 people globally and will result in annualised savings of USD 550 million.

Commenting on the redesign plans NXP Chief Executive Officer Frans van Houten said, "This restructuring is a tough measure and it is regrettable that we need to let people go. However, the changes will make NXP a strong, profitable and growing company, with a positive cash flow. “

As a result four factories are planned to be sold or closed. The fab in Fishkill, New York, USA will be closed ultimately in 2009. Additionally, two other factories are planned to be closed by 2010: the "ICN5" part of the NXP facility in Nijmegen, Netherlands, and part of the "ICH" fab of the Hamburg facility, Germany. NXP's fab in Caen, France will be put on the market for sale. The company is open to offers for this facility from prospective buyers, however, in the event that a buyer is not found the facility could be closed as well during 2009.

Giesecke & Devrient Open Smartcard Indian Development Centre

Giesecke & Devrient (G&D), a smart-card solutions provider, is opening a new Development Centre in Pune, India. The centre's approximately 80 employees are developing products based on smart-card technology for applications in mobile communication, electronic payment and public administration. Over the next few years, the R&D centre intends to double the size of its workforce to 150 by recruiting further IT specialists.

The Pune facility is one of three G&D Development Centres – alongside those in China and at Group headquarters in Munich, the latter being responsible for controlling all R&D activities.

Renesas To Sell German Fabrication Plant

Renesas Technology Corp., is planning a sale of its production facility in Germany – Renesas Semiconductor Europe (Landshut) GmbH (RSEL) – to Silicon Foundry Holding (SFH), a newly established Germany-based company specialising in semiconductor foundry services. The final agreement is expected to be concluded by the end of 2008.

RSEL has been present in Landshut for 28 years and has evolved to produce the highest possible quality of secure microcontroller wafers for smart card applications with 0.35 µm and 0.18 µm processes.

Renesas has examined the future of RSEL carefully as part of global activities seeking to optimise its production resources worldwide, in parallel with efforts to cut down costs and raise the operating capacity.

'Second Generation' ePassports Undergo Tests In Prague

The drive to introduce ePassports originated in the wake of 9/11 when terrorists used compromised passports to cross borders while travelling into the United States. Under guidelines from the International Civil Aviation Authority, ePassports had two central goals: 1) to ensure a forged or modified passport could not be used to cross borders, and 2) to prevent a criminal from impersonating the identity contained on a genuine passport.

On September 7-12 in Prague the European Commission held an event to test second generation ePassports for EAC Conformity and Interoperability follow widespread reports of alleged vulnerabilities in ePassport technology. In addition to standard conformance and crossover interoperability, the tests were the first organised attempt to verify EAC PKI operation in accordance with the European Union Certificate Policy, including bilateral exchange of EAC certificates. Twelve of the 27 participating countries completed the first PKI test round, and four countries participated in all four phases of the PKI testing, demonstrating a complete end-to-end system.

"The rigorous testing in Prague was a critical step in the European deployment of second-generation ePassports," said Chairman of the Brussels Interoperability Group, Bob Carter, who also represents the United Kingdom Identity and Passport Service. "All countries that participated in this first test of the Extended Access Control PKI infrastructure successfully completed the tests, and with that success, the vision for an EAC-enabled ePassport deployment is becoming a reality. Entrust's PKI operated flawlessly last week, and it will serve as a strong security foundation for our deployment of EAC- enabled ePassports."

ActivIdentity Files Patent Infringement Action Against Intercede Group

ActivIdentity Corporation filed of a patent infringement (U.S. Patent 6,575,360) action against Intercede Group PLC the producer of the Intercede MyID Identity and Credential Management System.

The action, filed in the United States District Court in the Northern District of California, alleges that the defendants have infringed a patent owned by ActivIdentity, and seeks damages and a permanent injunction.

According to the details of the filing, this patent was issued to a 3rd party on 10 June 2003 and ownership was transferred to ActivIdentity on 6 July 2006. As such Intercede does not believe this patent was derived from ActivIdentity's own research and development activities.

"The timing of this filing is questionable as it so closely follows recent press releases about Intercede's commercial successes in the US market. I believe ActivIdentity are resorting to the distraction tactic of litigation because their value proposition in the card management software market is failing. Should ActivIdentity proceed with this action, Intercede will vigorously defend itself," said Richard Parris, Chairman and Chief Executive of Intercede.

Fingers will secure our mobile phones

By Precise Biometrics.

Your mobile phone is getting more and more complex. Within a few years you may carry your door key, bankcard and ID card in your SIM card. But security issues will emerge, as PIN codes won't be a sufficient means of protecting this sensitive information. Fingerprint recognition and Match-on-Card will be the key.

As more services and function are added to our mobile phones, consumer will demand higher security. PINs are easily forgotten, misplaced or borrowed. Fingerprint recognition and Match-on-SIM offers an efficient and easily integrated mean of cardholder verification.

The industry is excited and discussions of the future possibilities of using mobile phones for payment, ticketing and identity management are held at all the major smart card events and forums. The emerging contact-less NFC technology enables all these features to be integrated within a few years.

But security will play an important role. If you have sensitive information and services, such as credit card, address book, keys and travel card, collected in your mobile phone it is important to make sure that only you access the information.

Today's PIN codes are weak links from a security perspective as they may be stolen, borrowed, forgotten or misplaced.

With fingerprint recognition and Match-on-SIM consumers will be able to make full use of the possibilities offered by NFC technology on mobile phone without compromising security or user-friendliness.

What is NFC?

Near Field Communication is a short range contact-less mean of transferring information between for example mobile phones, or between a mobile phone and a fixed terminal. The NFC technology communicates with the SIM card in a secure way through SWP (Single Wire Protocol), which enables the SIM card to act like any contact -less smart card.

The range of communication between a NFC phone and an external terminal, or another NFC phone is approximately 4 centimetres. The short distance adds security since it assures that the SIM card communicates with the intended terminal.

As the set up time is less than 0.1 seconds, to be compared with Bluetooth's several seconds, NFC is well suited for transactions in environments where there is a high level of throughput, such as public transport and airports.

So far there are only a few mobile phone manufacturers that offer NFC phones, but this number is expected to increase dramatically within the years to come. According to several market forecasts one third of all hand sets will be NFC enabled within a few years*.

Matching fingerprints on SIM

By adding fingerprint recognition to a mobile phone verification process you make use of the traditional advantages with biometrics such as a physical proof of the phone holder's identity. You also eliminate the need for unsecure knowledge based authentication, such as password or PINs.

Match-on-SIM is the concept of matching the fingerprint on the SIM card. As the NFC technology enables the SIM card to act as a contact-less card the scanning of the fingerprint can take place outside of the mobile phone, on an external fingerprint reader.

This means that a mobile phone holder will identify himself by holding the phone against an external terminal, such as a ticket vending machine, and putting his finger on a fingerprint reader on the terminal. The terminal sends an encrypted fingerprint template to the mobile phone via NFC and the information is matched against a reference fingerprint stored on the SIM card. If the match is correct the SIM card sends back a positive signal to the vending machine and the transaction is accepted.

SIM cards are established as secure platforms and as the fingerprint template is matched on the SIM card itself the integrity of the phone holder is protected. This also means that there is no need for a network-connected terminal, otherwise considered a weak link in a security chain.

As NFC uses energy from the fixed terminal, phone holder don't have to worry about phones that have run out of battery. Both fingerprint authentication and other transactions will function anyway.

Most SIM cards are based on Java platforms, which mean that applications can be added or removed during any phase of a SIM cards life cycle. SIM cards that are already in deployment can download software for fingerprint recognition functionality by connecting to the Internet.

But how do you add fingerprint recognition to an existing and established product such as the mobile phone? The key lies in the possibility to make use of fingerprint sensors outside the mobile phone, resulting in the least possible hardware adjustment on the mobile phone itself. This is possible with Match-on-SIM in combination with NFC technology.

SIM credit cards?

We have already seen the beginning of the merging of the mobile phone industry and the payment industry as several successful trials of enabling payment through the mobile phone have been done.

NFC enables payment transactions to be processed either by using the SIM card as a traditional credit card or by adding the payment to you mobile phone account.

The industry also sees great advantages in using NFC phones for ticketing. It may enable phone holders to buy electronic tickets from a terminal. Tickets may include an airplane ticket to Buenos Aires, a concert ticket to the latest Bruce Springsteen concert or a simple season travel card in the London Metro.

Ticket could be downloaded over the air from a ticket vending machine while you verify yourself through either PIN or fingerprint. When boarding the plane, entering the concert area or passing through the turnstile at the metro you simply hold the phone against yet another external reader. Depending on the service and security demand you may need to verify your identity again.

Proven technology

The Match-on-SIM technology has already been proved to function, as it was the runner up in the global SIMagine competition announced at the GMSMA conference in Barcelona this spring. And it was also demonstrated together with IER in combination with one of their newly launched gates for airplane boarding. There is a strong belief within the mobile phone industry, supported by the formation of the NFC forum, that the NFC technology has a lot to offer when it comes to extending the function of the mobile phone and several market surveys show the same result. But security will have an important role in the consumer acceptance of extending mobile phones to services such as payment transactions. Fingerprint recognition and Match-on-SIM will probably play a key role in the future security of mobile phone usage.

** 1/3 of all mobile phones will have NFC technology within 3-5 years according to a forecast from Frost & Sullivan. 450 million phones will be NFC enabled phones by 2011, which equaled 30% of all handsets worldwide according to ABI research.*

World News In Brief

Motorola To Supply Norway's Biometric Enrolment Kiosks

Motorola is supplying the Norwegian Ministry of Foreign Affairs (UD) and the National Police Computing and Material Service (PDMT) with biometric enrolment kiosks and divided models.

The Motorola Bio-Enrol Stations will enable Norway's multiple public agencies to digitally capture and store biometric data for passports, visas and other official identity documents. Around 500,000 applications for Norwegian passports are made every year, and over 150,000 visas applications.

The implementation of the Motorola Bio-Enrol Stations began in September 2008 and will be completed in June 2009.

Visa And Nokia Develop Mobile Payment Applications

Visa Inc. and Nokia announced plans to deliver Visa payment and payment-related services - including contactless payments, remote payments, money transfer, alerts and notifications - for Nokia's next generation handsets beginning with the Nokia 6212 Classic.

The Visa applications will first be made available for trial use by interested financial institutions and will allow consumers with the Nokia 6212 classic and a relationship with a participating Visa issuing bank to use their Visa account to pay for goods and services, initiate mobile money transfers to other individuals with Visa accounts and receive near real-time notifications of activity on their Visa account.

Smart Cards and PINs in an Online Environment

By Heiko Sochart, Senior Consultant, Health & ID, Sagem Orga

Heiko Sochart

The technical security provided by smart cards is only one part of the overall security story. The use of a smart card and the necessary PIN by its owner in a given system infrastructure and in an environment fraught with unknown security threats can decrease the level of overall security.

Today, plastic cards are used in nearly all areas of business and private life. Each card is a machine-readable identification token of its user. Most of us use more than one card – a separate card for each application (e.g. a credit card for payments, a passport to travel abroad, a card to use a phone account).

Current security requirements are forcing a migration from existing user/password login and simple plastic (memory) cards to smart cards and security tokens (e.g. banking, health, ID, public transport, PC and Internet login). That is why – as the smart card expert Sagem Orga is experiencing – card issuers all over the world are now replacing simple plastic cards with smart cards with built-in security mechanisms. One reason for this is the increased demand of users and operators for more protection of private data and defence against fraud. Other reasons are obvious – smart cards offer new built-in functionality that allows completely new applications not possible with dumb cards. Due to these mechanisms modern smart cards are predestined to protect private data and secret cryptographic keys. Besides the introduction of these new smart cards, the use of two-factor authentication is also becoming more common. The possession of a card is combined with the knowledge of a secret password, for instance, because it is presumed that only the legitimate owner knows this secret. In the world of cards the use of PINs (Personal Identification Number) instead of alpha letters is common, as card terminals normally are equipped with only a numeric keyboard.

Adding a PIN to a smart card

PINs are normally stored in a secure area of a card-based system. Smart cards represent such secure storage. A PIN entered via a PINpad by a user is directly sent to and verified inside the chip of the smart card. The stored PIN never needs to be communicated and therefore never leaves the chip. This is a major advantage compared to other plastic card-based systems where PINs are stored on servers and the entered PIN needs to be transmitted over insecure communications lines (e.g. the Internet). With billions of SIM cards, the PIN is used at least once when switching on the phone, with millions of bank or credit cards the PIN is used whenever a withdrawal is made at an ATM. In modern systems the PIN can be easily changed by the user.

How does one get a PIN? Normally a PIN is distributed at the same time as the card (but not in the same envelope with the card). If the card issuer wants to avoid the costs of sending an extra PIN letter, the card comes with a “Transport PIN” or “Empty PIN” . Despite all the technical security features built into the smart cards to protect the secret PIN, the characteristics of the overall system and the behaviour of users represent major elements of weakness in the whole security chain.

Security risks require security provisions

A PIN must be entered on a keypad of a card terminal to be sent to and verified by the chip of the smart card. The environment and the location of the card terminal and its PIN keypad must be arranged in such a way that a user is able to enter the PIN unobserved. Everyone knows how easily PIN entries at payment terminals in shops can be observed by customers waiting behind in line, and often the security cameras on the ceiling also record the use of the secret PIN.

To increase security it must be ensured that the PIN entry can be easily performed unobserved. If this is not possible – or even if it is – there must be an appropriate service and legal framework to limit the possible monetary loss or damage for the individual user to a minimum in case a card and PIN are used in fraudulent activities.

The installed PIN entry devices (e.g. for payment, ATM, etc.) vary greatly. It is therefore not always easy for a user to be sure that a particular card terminal and PINpad are secure and have not been manipulated by hackers. Only laws and industry standards for card terminals and their design can help minimize fraudulent hardware and software attacks at terminals. Users must not be liable for personal losses incurred due to manipulated system components. They cannot be made responsible for the state of security of a card terminal and how it technically secures the handling of the PIN.

The more different cards a user has, the more complicated it becomes for the user to remember all his or her PINs and to associate them with the right card. This could force users to write down their PINs, something that runs completely counter to all efforts to increase security.

To solve these issues providers and systems must offer users the possibility to modify the PINs of the different cards as they like.

The more frequently a PIN has to be entered, the greater the possibility that the PIN is no longer a secret known only to the legitimate owner. To reduce this security flaw, systems and especially the use cases must be designed in such a way that PIN entries are reduced to the necessary minimum.

The German eHealth card and its PIN function

An up-to-date example of smart cards with PIN functionality is the upcoming German electronic health card , for which Sagem Orga is a leading vendor. The new e-health infrastructure that is currently being set up in Germany will require doctors to use Health Professional Cards to authenticate themselves for the system and to create – using the patient card as well – an electronic signature on electronic documents such as prescriptions as the patient's physician. Entering the signature PIN more than 100 times a day is not acceptable for doctors because of the time and effort it entails and because of the risk of a breach of secrecy regarding the PIN.

One possible solution is the so-called comfort signature. The doctor enters the signature PIN once in the morning and at the same time registers a certain contact-less token. This token can then be used during the day instead of entering a PIN to sign for its holder.

The use cases for PIN and PUK letters are also potential sources of non-acceptance of the card scheme and can cause security leaks.

For example, in the German eHealth program, more than 72 million smart cards are to be issued to insured persons or their representatives (e.g. parents for children). As such a smart card is used to prove entitlement for free medical care and, more importantly, as an access key during treatment for relevant medical data, measures have to be taken to prevent unauthorized use and access. The PIN functionality is not needed for medical treatment. But as soon as a patient uses the security-related functions, the correct PIN entry is required. This is comparable with the declaration of intention embodied in the physician's electronic signature – it is the consent and statement of the card holder (the patient) to grant access to private medical data.

The smart card with PIN-controlled access in a technically secure environment, together with the presence of a health professional card, is seen by the German institution in charge (gematik) as today's most suitable solution for privacy in ehealth.

But PINs must be distributed by the issuer to the right card holder and must be remembered by patients many months later. And an ill person waiting for treatment by a doctor must know the correct PIN despite fever and nausea, or else they cannot grant access rights to medical data. In such situations, the PIN letter is not generally available and the PIN the patient defined a year before is not remembered. This means that PIN-dependent functions cannot be used or cause wasted effort on the part of the user when trying to unblock the PIN by use of the PUK or even requesting a new PIN or ordering the mailing of the PUK. This unpleasant situation can easily lead to a refusal on the part of the consumer to accept the new health card scheme, thus leading to security flaws (e.g. writing the PIN on the card).

The solution

The approach taken by smart card expert Sagem Orga is to find solutions that are cost-efficient and minimize risks at the same time. To order the PUK via phone or Internet from the health insurer is a security risk, because this could just as easily be done by someone with criminal intent. Today the only secure transport path is personal delivery, which entails avoidable costs. It would also be possible to visit a health insurance office personally to receive a new PIN or PUK, but this is linked with extra effort for the patient.

There is a solution, based on the following facts:

1. Normally a patient visits the same doctors and usually has a very trusting relationship with them.
2. Medical practitioners are forced to use a secure IT infrastructure and secure equipment, licensed for the electronic health card.

3. Nearly all PIN-protected functionality will be available and usable in online environments.

From these facts one can derive a convenient solution. If the PIN is lost or blocked, the doctor orders the PUK or the clearance for a new PIN from the card issuer online via the existing ehealth infrastructure. An inserted, functional, non-blocked electronic e-health card and its identified owner are the preconditions for this. The doctor is authorized and authenticated to the system during this process by his or her health professional card and by using a qualified electronic signature. This electronic PUK order will be logged on the card issuer's card management system (CMS). The result of this order is that the CMS directly communicates in encrypted form with the inserted eHC. The CMS uses the PUK securely stored (or calculated at time of need) in this communication process, which ultimately leads to the request to the patient to enter a new PIN. Neither the doctor nor the doctor's system nor the patient can see or influence the communication between the CMS and the eHC since it is encrypted.

This solution is a realistic possibility. It takes less than 3 minutes and it does not require a modification of today's card specifications. It is based on the specified PIN and PUK functionality; it does not override it, as it is just a simple but effective and secure enhancement. Costs can be reduced considerably. For follow-up and replacement card issuance, this solution also offers a cost-effective alternative to PIN and PUK letters.

In summary, the PIN technique itself is very secure. Still, it is important that this functionality is supported by instruction of its users and especially by implementing user-friendly mechanisms to reduce human risks.

World News In Brief

Verayo Launches, "Unclonable" Silicon Chips

Verayo, a security and authentication technology provider has introduced security solutions based on "unclonable" silicon chips. The core technology that makes these silicon chips unclonable is called Physical Unclonable Functions (PUF). PUF is like a biometrics technology for silicon chips. It extracts a type of "electronic DNA or fingerprint" that is unique to each silicon chip, and uses it for authentication and security applications. It is effectively impossible to model or copy the electronic DNA in another chip, which makes PUF-based solutions more secure and robust. PUF technology was invented at MIT and Verayo has the worldwide exclusive license to develop and market PUF-based silicon chips.

Conventional security solutions require storing of keys on the silicon. The security of the entire system depends on the integrity of these stored keys. Verayo's key generation solution eliminates the need for stored keys. Using unique electronic DNA or fingerprint of the silicon chips it dynamically generates a virtually unlimited number of secret keys. This significantly enhances the security and flexibility of secure systems, such as smart cards, NFC cards, SIM cards, trusted processors commonly used for financial transactions, service provisioning and trusted computing.

"PUF technology exploits the physical characteristics of the silicon and IC manufacturing process variations to uniquely characterise each and every silicon chip, this provides a secure, low-cost mechanism to authenticate silicon chips," said Professor Srini Devadas, co-founder and CTO of Verayo.

Barclaycard To Invest 7 Figure Sum Into Alternative Payment

Barclaycard announced it was investing a seven-figure sum in new ways to make payments.

The group said it was looking at enabling consumers to use the things they carried around with them, such as their mobile phones, key fobs and even their eyes or finger prints, to make payments, rather than relying on cards.

It is also developing paperless ticket applications that could be used for cinemas or train journeys and has introduced a new-style cash machine in the United Arab Emirates enabling people to use their fingerprints to withdraw money.

Barclaycard said in the future, people could be alerted to special offers in nearby shops through their mobiles. Other ideas include enabling people to hover their mobile over the price label of an item in a shop. People would then be able to confirm their purchase and take it away without having to go to a checkout or get a receipt.

Online fraud – who will take responsibility?

By Steve Brunswick, of the Information Systems Security activities at Thales

Steve Brunswick

Internet retailing is experiencing exponential growth: since 2000, the total value of online shopping transactions has increased by 871 per cent. Even in the face of the credit crunch and a fall in 'bricks and mortar' retail sales for the fifth consecutive month, the British Retail Consortium (BRC) figures for July revealed that online shopping increased to record levels. While this news is welcome relief to retailers trying to combat the detrimental effect of the current economy, the boom in online shopping is proving the perfect opportunity for fraudsters to commit card-not-present (CNP) fraud.

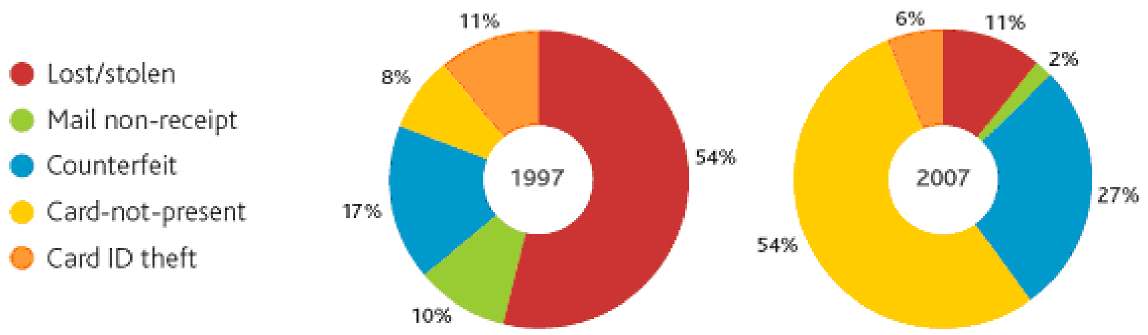
As of last month's BRC figures, Internet shopping sales were at a record £26.5 billion for the first half of 2008. According to the BRC, British consumers now spend more than three days a year shopping online, making it a more popular online activity than banking, listening to the radio and downloading music. Despite the fact that the rise in online shopping has been mirrored with the increase in CNP fraud, there has been little movement to address this worrying trend. Moreover, the perception of the risk when shopping online is not only denting the reputation of online retailers such as Cotton Traders, who have fallen victim to a highly publicised fraud attack, but it could also impact banks' brand and image.

The scale of the problem

As the below figures from APACS reveal, CNP transactions clearly pose the biggest fraud challenge today, resulting in £290.5 million in losses in 2007. However, confusion surrounds who should take responsibility for this type of crime. A recent survey by PayPoint.net revealed that 99 per cent of the 350 online businesses surveyed for the study did not believe they were liable for fraud on their site. The majority preferred to pass the buck to banks and credit card issuers instead. This shows just how heavily the onus is on banks.

UK banks' reputation for pro-actively reducing fraud following the migration to EMV and the resultant fall in face-to-face and ATM fraud is now being threatened by the risks associated with online shopping fraud. Consumer propensity to spend increasing amounts of money online coupled with a lack of strong authentication for online shopping transactions means that financial institutions can be sure that CNP fraud will continue to be a blot on the horizon unless they start to take a new approach.

Card fraud losses split by type (as percentage of total losses)



Many banks are beginning to move to address this new fraud phenomenon. In the UK, banks have already addressed one area of online weakness – online banking. The introduction of smart card or CAP readers to provide two-factor authentication is a significant step forward in improving the security of online banking. Such solutions are now offered by banks and building societies including Barclays, Nationwide and RBS. By making customers strongly authenticate themselves using an unconnected smart card reader and their bank card for online banking, the banks confirm the identity of customers before transactions are initiated.

The introduction of two-factor authentication for online banking seems to have had a positive impact on online banking fraud. Figures from APACS show that the battle against online banking fraud alone is starting to be won with losses reduced by 33 per cent between 2006 and 2007. The roll-out of card readers in the UK is steadily improving online banking security and showing a return on investment.

For those banks which have not migrated to the CAP infrastructure, there are other solutions available to address online banking fraud, namely mobile authentication. A mobile phone can be used for strong authentication by the bank sending security details to the customer via SMS. SMS password confirmation serves as dual-channel

identity authentication, making the transaction stronger, but not as secure as Chip and PIN. The need for reliable network coverage to enable timely receipt and processing of the SMS password is another possible limitation of this authentication method.

A customer's handset can also be used as a two-factor authentication device by pushing an application onto it. The handset acts as a PIN-activated challenge-response device, providing a code to authenticate the online transaction. The advantage of this method is that there is no requirement for network coverage at the time of authentication.

However, online banking is only a small element of the online financial activity that consumers conduct and banks are yet to make any announcements regarding the extension of such security measures to the wider online environment for all types of transactions.

How are other market players getting involved?

It is, in fact, the card schemes that are currently leading the CNP fraud challenge outside of online banking. Verified by Visa and MasterCard SecureCode are initiatives that encourage customers to register in order to protect transactions with an additional password. The systems allow financial institutions to confirm a cardholder's identity to the online retailer. However, of the 83 million credit and debit cards currently in circulation in the UK , only 20 million are registered with either scheme. Despite such efforts by Visa and MasterCard, retailers feel that the Government and payment industry are not doing enough to support them in tackling the epidemic, according to a report by CyberSource published in January .

Yet the response to such criticisms need not be complicated. Security advisors in banks are now in a strong position to advocate the business benefits of extending the success of strong authentication beyond online banking to cover the whole online payments space and to support MasterCard and Visa's move towards a more secure online shopping environment.

Many UK banks have already invested in the software and hardware to support MasterCard and Visa's Chip Authentication Programme initiative (CAP) through their investment in card readers and CAP compliant cards to secure online banking. Either CAP or mobile authentication could be used as a common platform that offers strong user identification within a cryptographically secure environment for all online transactions. The fact that the infrastructure to use two-factor authentication for e-commerce has already been put in place for online banking means that the business case to employ two-factor authentication more broadly online is a strong one.

By adding mobile or CAP authentication to MasterCard SecureCode or Verified by Visa, users can make online purchases using secure two-factor authentication in the same way as they verify their online banking transactions.

The tipping point

In the past, many banks were able to absorb fraud losses as they were insignificant compared to the overall profit generated by the business. But addressing the fraud committed in card-not-present transactions is not only about direct bottom line impact; there is a growing concern that customer retention and brand value could be affected by fraud losses.

According to a recent survey by enterprise communications company, Thunderbird, almost two-thirds (63%) of consumers are actively considering "switching" banks in the next 12 months. Only a very small number of the consumers surveyed felt a sense of "loyalty" to their banks (17%). A single case of fraud on their account could prove the tipping point to make customers change banks.

Financial institutions are all too aware of the decreasing opportunity to differentiate their services, making the loyalty challenge all the more taxing. However, with security breaches constantly highlighted by the national press, banks are presented with an opportunity to allay consumer fears about safety online and benefit their brand image at the same time. Implementing stronger security will enable a bank to offer customers greater peace of mind in the knowledge that they are reacting to the wealth of fraudsters who operate online, and will improve their customer retention as a result.

The future of online security

The overwhelming increase in card-not-present fraud attacks is moving up financial institutions' list of priorities year-on-year. Combining the financial losses of this type of fraud with the growing consumer impact of security breaches, banks must start taking preventative measures now. The investment in two-factor authentication for online banking is showing promise and should be regarded as a solid platform from which to progress a wider online security strategy to combat CNP fraud. For those banks which have not made the investment in CAP, mobile authentication is an attractive option. With few opportunities to differentiate services, it is time for banks to take the security opportunity to the next level and implement two-factor authentication for e-commerce.

Electronic Visas: the future of eTraveling?

By Hervé Naullet, ASK

Hervé Naullet

In a world where citizens' mobility keeps increasing, facilitating the travel and therefore border crossing became a clear challenge for authorities. This challenge then evolved to include the establishment of comprehensive border security schemes. Establishing tighter controls, together with a shorter border control processing time, electronic documents have become the de facto technological platform of choice for people's identification.

Electronic passports were the first of these new media to emerge; then electronic ID (eID) cards for border crossing or Enhanced Driver Licenses (EDL) in the US followed. Now, governments are considering the need to secure the visa issuance and control, evaluating two approaches. A first response is about using a unique identifier similar to a barcode printed on a visa; this identifier is then pointing to a visa holder record stored onto a central database. A second approach is about relying on a chip based technology similar to the ePassport platform. This second model provides benefits related to the protection of citizen privacy avoiding the duplication of personal data, limits the requirements for a central database, and also provides a response for off line checking. Vendors involved in the electronic Visa (eVisa) development face however a new challenge as they must overcome the technical issue of several chips within the same booklet. Indeed, these chips should not communicate together but should be read individually at the border gates.

To address this market, ASK, dedicated to contactless technology since its incorporation in 1997, relies on its unique technology of silver ink printed antenna on paper and die chip process. This patented technology is the basis of the 120 million products that have already been delivered throughout the world.

The unique capability of the ASK technology makes it ideally suited for a paper based eVisa product. It also paves the way in demonstrating the concept of "Electronic Documentation", adding electronic capability to any official documents such as birth certificates or diplomas.

A dedicated portfolio:

ASK's portfolio for the Identity market includes SPID®, a product range of inlays for e-passports, CoreLam®, prelaminated inlays for ID cards or driving licenses, all these products embedding the contacless technology and chips required by the various applications. ASK also developed the eDoc® product range to meet the growing demand of secure official paper based documents such as birthdates certificates, visas, diplomas or marriage certificates.

The technology of a silver printed antenna and die chip directly attached to the antenna provides outstanding mechanical characteristics and adds the requested physical security to the document. These ASK core technological components marry perfectly the paper and the chip through the antenna.

Meeting the market demand:

eVisas are electronic sheets inserted into an ePassport booklet. They offer the following benefits:

- Prevention of immigration fraud thanks to biometric elements such as the ID photo or fingerprints stored into the chip. A traveler with a similar attribute cannot simulate anymore the citizen who officially requested the document.
- Prevention of the document forgery, bringing the most advanced security features available to date:
    - Contactless technology storing both the country and document certificates in the chip ensures that the visa is genuine;
    - Advanced printing features, per ICAO 9303 part 2 recommendations
    - Size and layout of the sticker format compliant to the ICAO 9303 part 2 recommendations

Since these are documents to be used for border controls, such documents request interoperability and compliance with ICAO 9303 part 2 and ISO 14443 type A or B standards.

With today's technological know-how and anti-collision features, coexisting eVisas within the same passport booklet are limited to 2 or 4 depending on the embedded chip. Yet, the electronic feature enables the upgrade of the chip data to update validity date and the person's rights thus allowing only one visa issuing which could partly solve the problem.

As for the chip itself, available microprocessor chips on the market hold a memory size of up to 72 Kbytes of EEPROM so that sufficient personal data and biometric information can be safely stored with the level of security required by the ICAO standard. Apart from the contactless feature eVisas have to hold enhanced visual security features and comply with current personalization equipment.

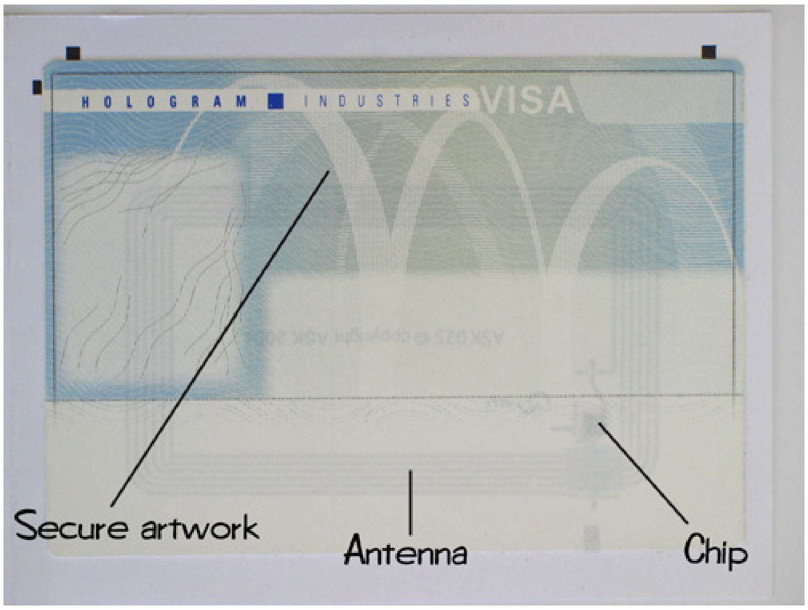
Smaller EEPROM chips may also be considered, depending on the type of data targeted to be stored. For example, instead of storing completed JPEG fingerprint images of 10K, the storage of templates of 1KB or smaller may be considered. 12KB EEPROM chips may well respond to the requirements. It shall be noted that the border control system that controls the visa is under the responsibility of the country issuing the same visa, thus the interoperability requirement is less stringent compared to the electronic passport scheme.

Assessing the technology:

Thanks to its expertise and experience in developing products based on a paper substrate with an embedded chip for the mass transit and related markets combined with several millions of ePassports delivered, ASK has identified important criteria to take into account regarding the manufacturing of eVisas:

- durability of the substrate and of the contactless feature;
- compatibility with the paper-based booklet structure of the passport and visa documents, keeping the needed flexibility of the booklet;
- compatibility with the embassies' current personalization equipments that are issuing the existing visas;
- security of the document which shall include security features for level 1 verification, but also anti-delamination features in order to prevent counterfeiting;
- using a chip and an Operating System that will provide the adequate performance combined with high security.

ASK eVisa meets all these criteria. As a paper sticker, the eVisa complies with the existing personalization equipment. The antenna is printed onto the paper visa sticker and the chip is directly connected to the antenna, providing a very thin and flat layer.



Another benefit lays in the technology of the silver ink printed antenna. The antenna can be printed onto the backside of the security printed paper, therefore, totally disabling the possibility of extracting the contactless feature from its substrate. The eVisa is a unique tamper-proof solid block.
The eVisa may also be supplied as a blank paper with the contactless feature on the back side, in order to be printed with an offset machine.

ASK developed a dedicated product with Hologram Industries in order to be entirely compliant with the existing equipment of personalization. A contactless sticker is delivered with a hologram foil that can be laminated on the sticker after the personalization. The sticker is first personalized with standard inkjet printers, then the hologram foil is applied with laminators, followed by electrical personalization of the chip with the applicant data.

Approach applicable to other official documents:

With eID documents based on ASK technology, citizens and governments can benefit from a state of the art technology. Such technology helps strengthening the security level contributing to the safety for all of us. It will also help establishing new document management paradigm either already established or yet to be emerged. For vehicles, it can be stickers on the windshield providing access control to secured areas or parks. Such stickers may also be considered addressing car registration needs or insurance of the vehicle, such verification being enabled on the streets using standard contactless reader equipments.

Business cases for such application shall be carefully considered, finding a good balance between privacy management and targeted objectives. In the case of fraud to insurance, clear benefits have been already identified, the challenge being mostly about building the proper momentum within the deciding parties.

Paving the way for eVisas:

Electronic Passport programs are being gradually implemented in various countries validating the concept of embedding contactless technology into Travel Documents. Main benefits include faster processing at the border control, and an unrivalled security level of foreign and domestic people's travelling. This is also true for eVisas upgrading immigration control on a worldwide scale. ASK technology durability has been field proven with holders who have been using ASK contactless smart cards for several years in a row. Silver ink printed antenna and die chip attach technology was once again demonstrated with the 14 million contactless paper tickets for the visitors of the highly secured 2008 Beijing Olympic Games where product's reliability was of essence.

Electronic visas provide great benefits in the border control process, enabling for example off line control. As a paper based document, it also opens new opportunities such as the processing of official documents, adding a highly secured authentication response.

World News In Brief

Cryptomathic Launches High Speed e-Passport Inspection Technology

Cryptomathic, has launched a solution to speed-up the inspection of e-Passports. The new technology addresses government concerns that the extended time taken to retrieve e-Passport biometric data will result in unmanageable queues and costly delays at busy international border points, by eliminating the need to transfer data from the e-Passport chip onto the border control system every time a traveller enters the country.

The technology will enable Basic Access Control e-Passports to be read almost instantaneously, while increasing the speed of inspecting Extended Access Control e-Passports by a factor of four. Known as the 'encrypt and destroy technique', the solution satisfies EU e-Passport privacy and data protection laws.

The Cryptomathic solution is a special sort of caching mechanism, a storage area that holds an encrypted version of the e-Passport biometric data, scrambled using an encryption key and identified by a pseudonym which are both derived from the e-Passport itself. When the e-Passport has its initial contact with the border control station, the biometric data is transferred from the chip into the inspection system, and at the same time a unique key is calculated from the e-Passport chip, which is used to encrypt the stored data. Crucially, the storage key is then deleted from the memory of the border control system to make it impossible to retrieve the stored data. In order to recreate the decryption key for the record and view the biometric data, the original e-Passport document must be connected to the inspection system.

"The global investment and commitment to deploying e-Passports is considerable. If a country's implementation is too hurried or poorly thought out, border controllers will have to compromise in the inspection procedures. They may only inspect e-Passports for travellers already identified as suspicious for example, which would weaken the security benefits of the technology, and travellers would soon be asking why they had to pay so much for their e-Passport if it is hardly ever read. By securely caching traveller details upon passport application or first border crossing, these delays can be significantly reduced saving both time and money. Cryptomathic is delighted to bring this important solution to market."
Said; Mike Bond, Security Director at Cryptomathic UK

15% Annual Growth Of Globalplatform Based Smart Cards

GlobalPlatform, the international smart card specifications association, has released figures showing a conservatively estimated annual increase of 15% in the total number of smart cards, which utilize the GlobalPlatform Card Specification as the basis for card infrastructure, that have been deployed globally.

The organization approximates that since October 2007, the number of deployed GlobalPlatform based smart cards has risen from 265 million to 305.7 million worldwide. Ninety GlobalPlatform-based card implementations have now been reported across Europe, Asia, Australasia and the Americas.

Of the 305.7 million cards deployed to date:

. 45% (137.6 million cards) has been issued by governments, primarily for ID and healthcare applications;

. 32.7% (100 million cards) has been issued by the mobile telecommunications sector;

. 21.9% (66.9 million cards) has been issued by the financial sector;

. 0.4% (1.2 million cards) has been issued by the transit sector.

Sagem Orga To Roll Out its Electronic Health Card in Germany

The purchasing cooperative of the IKK, the Knappschaft (Miners' Guild) and the Landwirtschaftliche Krankenkassen (Agricultural Health Insurers) has awarded the order for supplying 9 million insured persons with electronic health cards to the smart card specialist Sagem Orga. Sagem Orga will handle the production, personalization and shipment of the new health cards for the involved insurers.

Sagem Orga has been awarded the production of its e-health card by the purchasing cooperative led by the IKK's National Association. A total of 26 different health insurers are involved in this award.

Sagem Orga is committed to run the entire process, from development and production to personalization of the health cards in Germany, so that highly sensitive data for insurees never leaves the country. Additional production security will be offered by its partnering concept, which involves Sagem Orga cooperating with Winter AG and D-Trust.

Oberthur Technologies Provides Mifare NFC Sim Cards In Malaga

Oberthur Technologies, has been providing Orange Group with Near Field Communication (NFC) SIM cards and Over-The-Air (OTA) management of transit devices based on the Mifare technology. This solution is incorporated in mobile phones used in the urban transport network in Malaga. The FlyBuy solution enables to store Mifare tickets in the SIM card and to validate tickets by simply waving NFC handset close to the ticket reader. Customers buy new tickets that will be loaded via a SMS mechanism in their SIM card.

California Tackles RFID Skimming

The state of California has become the second American state to make it illegal & punishable to skim RFID identity cards after governor Arnold Schwarzenegger on Tuesday signed Senate Bill 31.

"It's an acknowledgement from the governor that any technology can be abused and that as technology changes, the law has to keep pace," he says, adding that he was also happy to be able to attain broad-based support for the bill from both industry groups and privacy advocates. "It was not without much discussion along the way, but ultimately we were able to come together on this one." Said California State Senator Joseph Simitian.

Earlier this year, Washington became the first state to pass a law against theft of RFID data.

Lumidigm Multispectral Technology Extended To Whole Hand

Lumidigm, Inc., a fingerprint biometrics company, has applied its multispectral technology to the capture of multiple characteristics of the hand. The ability to image concave areas that are not naturally in contact with the platen is a clear advantage that multispectral technology brings to the challenge of whole hand biometrics. Because the Lumidigm technology is a direct imaging process, all areas of the hand are imaged.

A advantage of Lumidigm's whole hand technology is that it is capable of capturing the thumbprint, four fingerprints and a palmprint all with a single placement of the user's hand on a single sensor.

A History of MULTOS: From Mondex to Gemalto

By Tom Tainton, Smart Card & Identity News

Tom Tainton

Since it's inception in the early nineties MULTOS has gained a reputation as the most robust, flexible and secure smart card platform in the market. The multi-application operating system enables a smart card to carry a variety of applications, from chip and pin payment to secure ID and ePassport. Previously, application developers had to write a separate version of the application for each type of smart card. MULTOS changed all that. Whereas earlier systems did not allow new applications to be installed, MULTOS enabled several applications to reside at once, regardless of microchip used.

Today, millions of MULTOS smart cards have been issued across a range of industries including contactless payment, Internet authentication, biometrics and healthcare. More than 75 issuers are now committed to issuing cards on the MULTOS platform, as well as 70 companies supplying MULTOS-related products and services. It's fair to say MULTOS is in demand. Earlier this month, French giants Gemalto acquired MULTOS, the latest in a long line of companies battling to gain control of a seriously lucrative asset.

The smart card platform has a multitude of benefits. For starters, it's the only operating system for smart cards to have been certified with the prestigious ITSEC Level E6 security rating, the highest available. MULTOS also boasts true interoperability, allowing multiple vendors to supply components and the ability to load and delete multiple applications. MULTOS is also ably supported by several of the industry's leading organisations known as the MULTOS consortium, a group of international blue chip companies whose objective is to promote MULTOS as the smart card industry standard across all market sectors.

Natwest Group and Platform Seven

In 1993 the Natwest Development Team (NWDT), a department led by our very own Smartcard News founder David Everett, invented MULTOS. It was originally developed to support the Mondex International e-purse application. The NWDT undertook the ground breaking technical design, development and implementation of the Mondex electronic purse and other Mondex devices. The team played a pivotal role in one of the most security demanding projects ever when they developed a smart card operating system, brought to the market as MULTOS.

Then, Natwest Group decided to exploit its extensive knowledge of security in the smart card industry with the creation of Platform Seven, a UK-based centre offering secure component products and a wide range of services for the e-commerce market. Members of the new unit were drawn from the former Natwest Development Team.

Mondex International

In 1996, MasterCard purchased a 51% stake in Mondex, promising to promote MULTOS and support the technology's development. Although no financial details were disclosed, the gross value of Mondex was estimated at around $100 million. The merger proved a great success and three years later the MULTOS chip became the first commercial product ever to achieve a security rating of ITSEC Level E6. In the same year, Mondex International set its sights on conquering the Internet, with intentions to become one of the first online e-cash services. Having become a major global firm in the e-cash business Mondex agreed a deal with ActivCard to develop secure ID and access information for the MULTOS smart card environment. In return, ActivCard's access tools technology would transfer over to MULTOS enabling Mondex e-cash cards to arrive with e-commerce facilities already built in.

MasterCard

By 2001, MasterCard International assumed full ownership of Mondex, snatching direct control of all the companies operations, most notably MULTOS. Under the agreement, Mondex continued to provide service to the MULTOS consortium, MasterCard's preferred operating system for multi-application smart cards. However, despite it's previous success MULTOS experienced fresh difficulties under the leadership of

MasterCard. Once a contender to become the standard operating system for smart cards MULTOS now found itself in fierce competition with Java Card, a US based operating system threatening to dominate the market.

The MULTOS consortium announced plans to develop a low-cost version of the operating system aimed at banks gearing up for the inevitable conversion to smart cards known as 'Step-one'. By providing a cheaper stepping-stone to fully-fledged MULTOS, the consortium hoped the project would convince card issuers to embrace the technology without forcing them to bear the cost and complexity of a full rollout all at once.

MULTOS backers characterised the move as a logical strategy that would allow financial institutions to make a more gradual transition to MULTOS based chip cards. Conversely, critics suggested it was a futile effort to keep MULTOS relevant in a market increasingly saturated by Java Card systems. It's easy to see why this assumption was made. In 2002, the industry shipped 5-million microprocessor cards carrying MULTOS property compared to a staggering 170 million cards with Java Card properties.

One reason for this was Java card software governing the mobile phone SIM market. Since MULTOS was not a player in such a market it was crucial to consolidate its position in banking if it were to survive in the long term.

StepNexus

In 2006, a deal to move control of the MULTOS smart card operating system from MasterCard to a new consortium of companies was completed. The holding company revealed its new corporate identity, StepNexus Inc. The name was derived from Secure Trusted Environment Provisioning, with Nexus providing the connection between the technology and the consumer. In a partnership with Hitachi, Keycorp and MasterCard StepNexus acquired full jurisdiction over MULTOS technology. John Wood overlooked the consortium. Today he is the CEO of MAOSCO Ltd, a legal company set up to promote and develop the MULTOS specifications as an open industry standard.

Aiming to reverse the fortunes of MULTOS StepNexus devised several initial solutions with the main focus being on security and flexibility of the product. These were:

- To make MULTOS the world's standard secure multi-application smart card operating system. This was implemented using a similar project to 'Step-one' although this time StepNexus particularly targeted the SDA payment markets.
- To reach new markets and sustain current ones. The solution aimed to extend to other environments where users were 'seeking to benefit from enhanced trust and security'

StepNexus announced the acquisition of GlobalPlatform on MULTOS technology from Sentry, a privately owned Sydney-based company. The application enabled any MULTOS chip to support GlobalPlatform services and meant that the flagship platform MULTOS could provide compatibility with existing Global Platform systems.

Keycorp

In mid 2008 Australian-based Keycorp bought out the UK subsidiaries of StepNexus and subsequently acquired MULTOS as well as intellectual property rights and registered patents. As part of the deal Keycorp relinquished it's existing shareholding in StepNexus and was forced to pay the holding company $1million. After the completion of the deal Keycorp owned the majority of shares, although former StepNexus partners Hitachi and Mondex International retained 20% of the shares in the new venture.

Gemalto

Keycorp's reign was short-lived. By September Gemalto confirmed it had attained all Keycorp smart card business assets including trademarks, IP portfolio and of course, MULTOS. And all for a cool £22 million. As well as taking over the operating system Gemalto have also bagged the Key Management Authority (KMA) that manages MULTOS cards worldwide. Around 40 technical experts will join the company, most of whom are based in the UK and Australia. Gemalto hope the deal will contribute over $15 million extra revenue to the secure transactions and government program segments of Gemalto on an annual basis.