

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

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

Telephone: +44 (0) 1903 734677

Fax: +44 (0) 1903 734318

Website: www.smartcard.co.uk

Email: info@smartcard.co.uk

Editorial

Managing Director – Patsy Everett

Technical Advisor – Dr David Everett

Production Team - John Owen,
Lesley Dann, Suparna Sen

Contributors to this Issue – David
Everett, Suparna Sen, Tom Tainton,
Alexander Kurz, Stephen Beecroft,
Dave Abraham, Peter Hodgson, Peter
Tomlinson, Pamela Bells

Photographic Images - Nejron -
Dreamstime.com

Printers – Hastings Printing Company
Limited, UK

Disclaimer

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

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

© Smart Card News Ltd

Our Comments

Dear Subscribers



Patsy Everett

It's Spring, the daffodils are out and at long last the sun is starting to shine. Mixed in with a little rain I know but then this is the English weather we are talking about. Anyway at this time of the year people start to smile and everything just seems to be that much nicer.

However that doesn't stop gloom and despondency from wandering around the marketplace, this time it's chip security as discussed in our lead story this month. Otherwise the chip manufacturers seem to be busy with little slack in their fab lines. What I find so fascinating is the different views you get from people on a subject when we are all faced with the same facts. On this chip security I have got everything from I don't care (i.e. don't believe it's a problem) right the way through to this is a show stopper for smart cards. Curiously the Tarnovsky attack has not made the big headlines even though by just about anybody's estimation it's a pretty fair achievement.

Actually the Digital Money Forum (Hyperion's annual event at the Charing Cross Hotel) caused most of the in house discussion this month. The full story is reported separately but it was the tales from James Allan that stirred the emotions. After one of those late night foolish wagers James bet his friends that he could live in London for a year without cash, just cards. Now you could be cynical and say what a good way of scrounging from your friends but I don't think James is that sort and anyway it's interesting to think about those things that cause you a problem. At the end of the day there is that question, can you get rid of cash?

Well it was actually meetings with friends that caused most of the problems, those little P2P payments that we never think about. How about 'Putting a fiver in the glass' to pay the kitty for a night out at the pub? Then there's paying a couple of pounds for those raffle tickets. Then there is the contribution, Jane is sick so let's buy her a card and some flowers, give me a fiver. I could go on, the truth is we never think about those little P2P payments but our whole social life is based on them. Any cash replacement system that can't handle P2P and that really means person to person in the street, pub, office, etc, seems doomed to failure. At the other end of the scale and caught a little bit by surprise is that there are some higher value transactions where cash is still the order of the day. Putting down a deposit on a flat for instance is often met by a demand for cash on the grounds that cash is irrevocable, which is clearly not the case with credit and debit cards. So there's another one for the pot, any cash replacement system has to be irrevocable. I feel I've just made the list of contenders pretty small.

Anyway the other interesting story is of course to turn the argument around and ask if you can live in London for a year without cards, just cash. Now I'm probably biased here but cash seems pretty powerful to me, I've never forgotten the bank manager who explained to me that he lived on cash because he always got a discount, there was nothing personal here but he then proceeded to get the biggest wadge of notes out of his pocket that I have ever seen. Perhaps this was all before the day of the mugger or bag snatcher which I have experienced firsthand. That's when you end up with no cash or cards.



So what happens if you haven't got a card? Well just about every form of remote payment goes out the window and more and more of the machine payments, rail tickets and parking are now moving to cards. No more waiting in the queue for somebody at the machine to find they're a £1 coin short and it won't accept the £10 note, in fact it's a game of bluff to see who else in the queue blinks first and hands over a £1 coin. Perhaps this is what the bank manager meant, a neat way of getting a discount.

This is of course a particular problem of the poor also discussed at the Forum that they tend not to have cards and it's really our new world of the internet and mobile phones where we are increasingly buying our goods and services. No more going down to the shop, testing it out, and then buying it on Amazon. Not me I hear you say.

Patsy Everett, Smartcard & Identity News.

Contents

Regular Features

What the silicon manufacturer has put together let no man put asunder. . .	1
Events Diary	3
World News In Brief	9,14,16,17,19

Industry Articles

India Faces Up to International Card Fraud	5
Stopping the Counterfeiters	7
How secure is the biometric passport?	10
Smart Thinking For Local Authorities.	11
The Death of the Token	13
Biometric Data Protection in the Education Sector.	15
Beyond Conferences	18

Events Diary

April 2010

21-24 Prepaid Cards Asia Summit 2010, SUNTEC Singapore Int'l Convention & Exhibition Centre - <http://www.terrapinn.com/2010/prepaidcards/>

26-28 Cards/2010, Sao Paulo, Brazil - <http://www.cards2010.com.br/ing/evento.htm>

27-29 Infosecurity Europe 2010, Earls Court, London, UK - <http://www.infosec.co.uk/>

May 2010

10-13 IFSEC 2010, Birmingham, UK - <http://www.ifsec.co.uk/>

10-13 MiddleEastRail 2010, Al Bustan Hotel, Dubai, UAE - <http://www.terrapinn.com/2010/merail/>

10-12 Prepaid Expo Europe, Brussels, Netherlands - www.iirusa.com/prepaidexpoeuropa/

12-14 Cardist, Istanbul - www.cardist.com.tr/en/default.asp

16-18 22nd Annual Card Forum & Expo, Orlando, FL. USA - <http://www.americanbanker.com/conferences/cfe10/>

20-22 WIMA-NFC Conference, Monaco - http://www.wima.mc/content/Home-page/home_pageUK.php

20-21 SIMposium 2010, Rome, Italy - <http://www.simposiumglobal.com/>

21-24 Prepaid Cards Asia 2010, SUNTEC Singapore Int'l Convention & Exhibition Centre - <http://www.terrapinn.com/2010/prepaidcards/>

26-28 Cards/2010, Frei Caneca Convention Center, Sao Paulo, Brazil - <http://www.cards2010.com.br/ing/index.htm>

27-29 Infosecurity Europe 2010, Earls Court, London, UK - <http://www.infosec.co.uk/>





What the silicon manufacturer has together Continued from page 1

Infineon SLE66. Since that time he has been the key engineer behind Flylogic Engineering which according to their web site is a professional chip evaluation/reverse engineering house. I understand they have their own FIB machine which at \$1 million per pop is not the normal back bedroom toolkit. So let there be no doubt that Christopher is a highly skilled chip reverse engineer with access to the best equipment.

The target for Tarnovsky's attack was the SLE66 family of secure microprocessors from Infineon. This is a 10 year old design (maybe more) but is none the less the mainstay of the Infineon product line for smart cards and similar products including TPM (Trusted Platform Module) chips as used in the Xbox360 for example. For the avoidance of doubt the SLE66 would be considered a secure microprocessor chip and has been evaluated under Common Criteria to EAL 5+.

What Tarnovsky has managed to do and demonstrate is that over a six month period he has painstakingly analysed the chip and using a FIB machine has managed to bypass the shield protecting the core logic and probe the data bus of the CPU at a point at which it is not enciphered. Although he only probed one data line at a time he managed to disable the dummy cycle generator that would throw the synchronisation necessary to recover the complete 8 bit data bus (effectively you need to repeat a fixed cycle probing one data line at a time, the insertion of random dummy CPU cycles would break the necessary synchronisation). Of course it wasn't really six months because Tarnovsky was working on this chip before his last Black Hat presentation in 2008. In his work he also claims the cost of this attack to be about \$200,000 on a commercial basis (just for me – who is paying this bill, I know it's not Infineon?).

Now here is the real story, what Tarnovsky has done is a fantastic achievement in reverse engineering of a security microprocessor. Nobody would have said it impossible but most (me included) would have argued that nobody with the necessary skills and resources is likely to sit down and do this. I confess to being quite surprised because the real cost in terms of skilled people and equipment is really much higher than the claimed \$200K. Again I can speak from experience because in the 90's I set up a laboratory to do just these sorts of exercises and we couldn't afford to have our own FIB machine.

So now to the interesting bit, how worried should we be? By Tarnovsky's own admission the SLE66 was a difficult chip to beat and as he pointed out the active shield required extensive analysis and testing to circumvent. The flaw in the design of the chip in his view was the availability of the unencrypted data bus in the CPU which Infineon have already corrected in their newer chip the SLE78.

Will we see lots of hackers decoding the SLE66? No, it really is beyond the scope of anything but a commercial (government) reverse engineering laboratory. In my view it is beyond the scope of even a well resourced university department, this chip is a different ball game to the NXP Mifare chip which has been successfully hacked over the last few years.

So how about all those EMV cards out there or the GSM SIM cards, should the Financial Institutions (FIs) or the Mobile Network Operators (MNOs) be concerned? Frankly no, they all operate with unique chip keys and in both cases individual cards can easily be identified and processed accordingly. How about cards with global keys? Well that would be a concern but does anybody still do that? Then there are those TPM chips as used perhaps in the electronic games market, Mmmm now here is a target like PayTV that hackers feel is open house, there is also a history of commercial resources being brought into play. I think I would be (already) using a newer chip here but also notice that these guys usually build a lot more into their systems than can be destroyed by the vulnerability of a single chip.

Then last of all (for the moment) how do we look on the Common Criteria process? Should the SLE66 have an EAL5+ rating? Does it need to be re-rated? This is more difficult to answer but let us not forget that a CC rating is a measure of how well a Target of Evaluation (TOE) meets its specification, it's like a security quality measure not necessarily a statement of how secure a device actually is, although the chip's resistance to attack is part of that measure. Of course you wouldn't normally evaluate a low security functionality device to a high CC level but conceptually you could. So has the reverse engineering exercise by Christopher Tarnovsky changed the perception of how difficult the work function really is? Well it has moved my goal post but just a bit and I shall happily carry on using EMV cards and my mobile phone with little fear of being compromised because of chip hacking.

And just as an afterthought lots of FIs and MNOs use chips far less secure than the SLE66. In America they are still using magnetic stripes for financial payment cards.



India Faces Up to International Card Fraud

By Suparna Sen, Smartcard & Identity News



Suparna Sen

Arrests began late Sunday evening on the 6th March. Location - Kolkata airport and suspected kingpin, 37-year old Nigerian Peter Orenubi Oluwagbenga is handcuffed on arrival by a special team of police detectives.

It has been a game of ‘cat and mouse’ for the Kolkata police, as they finally crack the million-dollar credit card fraud racket in the city, one of its first kinds in the city and of India.

Peter Oluwagbenga, the mastermind had been using various methods to cash-in on cloning credit cards. He purchased expensive jewellery and electronics only to sell afterwards and also make bookings in 5 star hotels, only to cancel them for cash refunds.

The rest of the gang, footballer Benson Oladetan Adams, who played for Mumbai Football Club (BMFC) and wife Leeanna Jordasn, Manish Agarwal and commerce student Ankit Shaw were picked up from different locations through the night.

From Leeanna’s residence in Picnic Garden (an area in Kolkata), the detective department seized a “credit card reader” that was used to copy data from the magnetic stripe. Also seized was a bunch of cloned cards with the data stolen from cards issued by various US banks, including such majors like ICICI, HDFC, Centurion and Citibank.

The accused employed a technique called “skimming”, which involves using the small card-reading gadget to secretly copy data from cards while they are being taken for swiping at payment counters in merchant establishments, mainly restaurants or petrol pumps. Even the most primitive versions of these card readers, available on some foreign Internet sites, can store up to 3,200 swipes to memory.

The captured data is then used to personalise the copy-cat card - said to be easily available in countries like China, Taiwan and Bangladesh.

Thanks to ICICI Bank for lodging a complaint on February 23rd that brought in front such revelations. A special team of officers comprising Soumya Banerjee, Nilkantha Roy, Ayan Bhowmik and Mriganka Das cracked the case but Damayanti Sen, the chief of the city’s detective department, has not disclosed anything more on the present status of the case, as she says: “We are still at it. More people and more money might be involved”.

To detect card skimming, the card issuer must first have a large pool of fraudulent transaction complaints. The data pool is then analysed for common traits, for example all the defrauded card-holders ate at the same restaurant within a close proximity of time. Once enough evidence is collected the merchant is investigated for the usage of illegitimate equipment.

Representatives of ICICI Bank declined to say anything on whether complaints from US-based banks about its payment gateway being illegally used prompted the complaint or not.



(Calcutta Police)



(Seized ‘card reader’)





(Leeanna's seized passport next to one of the cloned cards)

Peter Oluwagbenga's contacts in the US would help him steal data from the country's credit card holders. The Nigerian would then mail this data to his associate Benson, biding time in Calcutta as a footballer and his alleged wife of convenience, Leeanna.

While the trio was big-time players, they cunningly involved two local youths named Manish and Ankit to make their operations run all the more smoothly. It is said that Peter met Manish in his father's Camac Street sari shop during one of his previous visits to the city. Ankit joined the gang at the request of Manish.

Ankit, a GNIIT (Graduate from National Institute of Information Technology) diploma holder knew software technology well enough to master skimming rather easily. He, with Manish not only helped the Nigerian duo and Leeanna steal card data "but were also the designated users of the cloned cards in Calcutta," said a police officer.

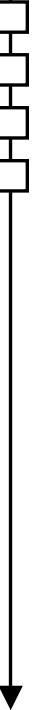
Although India is moving towards unique ID cards adoption for all its citizens, yet the country lags behind introducing an EMV 'Chip n Pin' system. Tourists, arriving in India and other Asian countries armed with Chip and PIN cards; often don't get to use the added security of Chip and Pin. Cards revert back to using the easily counterfeit-able magnetic stripe.

Debit & Credit cards has limited popularity in India (except in ATMs), as the merchant is charged for each transaction. Indians rather prefer cheque, DD or Demand Draft or cash as viable payment modes and most of the shops (except big ones like Big Bazaar and Indian Silk House) are unwilling to accept payment by card. I try to buy things using my debit card, although I too often face problems while shopping from small retailers that do not have card reader installed in their stores.

It's not that the non-EMV countries are unaware of increasing card fraud, but part of the reason, as experts say, being fraud issues haven't been as prevalent in third world countries as it is in European nations. Moreover, the expense of converting to chip-and-PIN is prompting many such countries like USA, India and Thailand from switching to EMV.

Javelin Strategy and Research, a consulting company for the financial services industry, has estimated the cost for the United States' to migrate to the technology at \$5.5 billion, mainly for new payment terminals, is an expense that neither retailers nor banks want to shoulder.

Doug Johnson, vice president for risk management policy at the American Bankers Association, said that the American banks were concerned about security but that there were no plans to move to chip-and-PIN cards, as there is "lot of hurdles," he said, both from a cost as well as a network standpoint.





Stopping the Counterfeiters -

Using Authentication Devices to Prevent Product Counterfeiting (and Potential Revenue Loss)

By: Alexander Kurz, Atmel Corporation



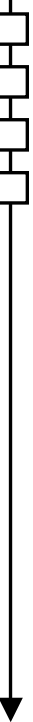
Alexander Kurz

Manufacturers of microprocessor-based systems where the product manufacturing costs are low but the development and marketing costs are high often find themselves victims of product counterfeiting attacks. Fraudulent manufacturers have little or no development costs and therefore can make a nice profit selling “clones” at a much lower price than the legitimate manufacturer. Since counterfeiters are often hidden in countries outside cooperative legal jurisdictions, fighting them directly is difficult, if not impossible. Fortunately, there is a simple solution: raise the counterfeiter’s “development” cost to the point where counterfeiting is no longer viable. But this must be done without significantly changing the legitimate manufacturer’s product cost. The most complete and cost-effective way to thwart this type of attack on a company’s products is to integrate a hardware authentication device into the product itself.

Authentication is the process of identifying a system peripheral (daughter card, network card, etc.) or replaceable item (battery pack, ink cartridge, other consumable) as genuine, authorized for connection to or insertion in the system being protected. Figure illustrates the process of validating a consumable item. A description of the process follows.



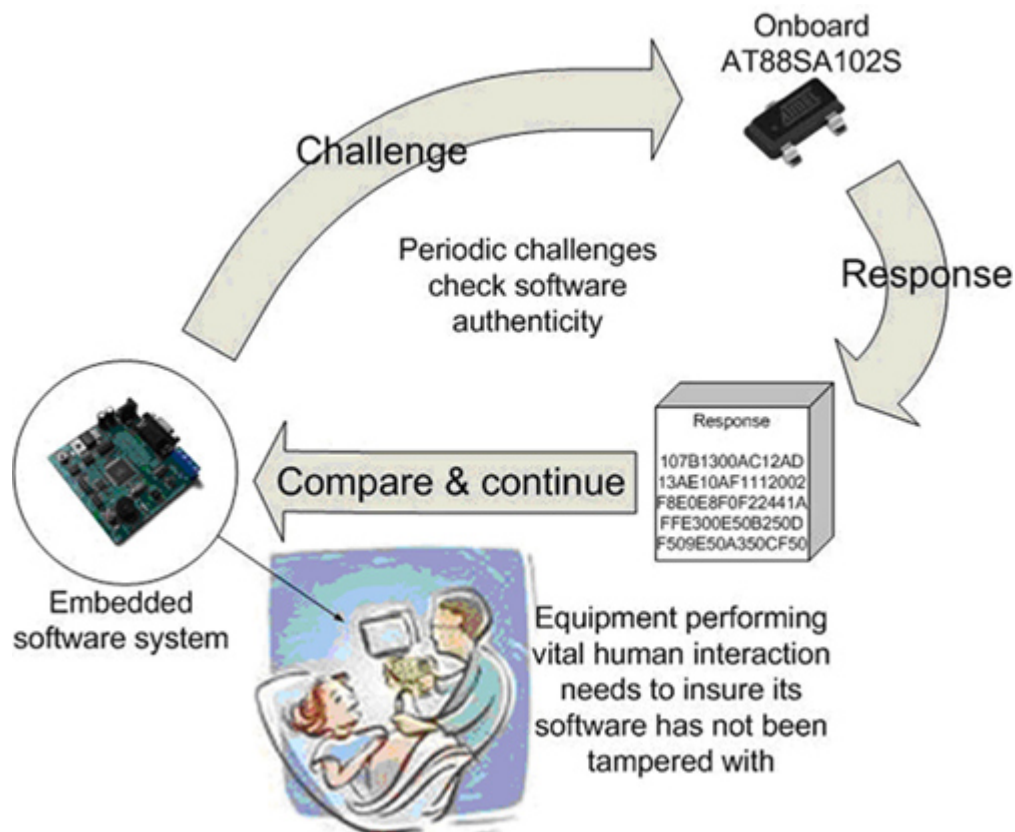
A small authentication device is embedded in the consumable client product and when connected, acts as a slave to the microprocessor (in the host system). Using a secure challenge-response process, the host microprocessor issues a challenge to the client which encrypts a response back to the host. The same secret contained in the authentication device is stored in the host microcontroller to enable it to calculate an expected response which it compares to the actual response and if successful, validates the client (permitting its operation in the system).





Modern microprocessor-based systems always include system firmware and often include an electronic interface to a PC, network, USB flash drive, daughter card, replaceable battery or consumable item. In all these situations, and more, including a hardware security chip on the system board can provide a host of additional benefits which include; (1) preventing unauthorized firmware copying, (2) implementing secure identification and (3) enabling encrypted communication.

- (1) **Embedded Software Clone Prevention:** Usually firmware development is the most costly and time consuming part of embedded system development. An authentication device can help prevent fraudulent cloning of that firmware – only systems that contain a device with the correct OEM secret will function properly. The basic operation of this security model is displayed in Figure and described following the figure.



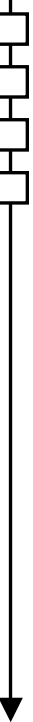
At periodic intervals, an instruction is inserted in the source code to issue a challenge to the authentication device. The response from the device is then compared to the expected response and the program continues only if the response is correct. By providing a large number of challenges and hiding or cleverly placing them in the code, the source becomes extremely difficult to reverse engineer. Finding and removing all the inserted authentication commands is a very difficult challenge.

Also, if source code is stored in flash memory, then the system designer can offer the benefit of field upgrades, but transmission of the code can expose it to copying. A hardware security device can support authentication and encryption of the code using either a common distribution model or custom images for each individual system.

- (2) **Secure Identification:** Serial numbers are useful for controlling help-center costs, identifying a system owner, managing maintenance records and many other uses. Usually, this just means putting the serial number in an EEPROM.

An authentication chip can provide numerous advantages over an EEPROM: it ships from the chip fab with a guaranteed unique serial number, and it supports an easy to use protocol that can identify any attempt at duplication.

- (3) **Encrypted Communication:** When the information transmitted over the network is sensitive (as in medical systems) or prone to fraud (whenever money is involved) it's best to encrypt the data. While





many standard microprocessors include AES encryption blocks, there's no easy way to protect the encryption key. An authentication device can be used to confidentially store these secret keys or to exchange a volatile session key with a host system.

An example of such authentication ICs is Atmel's CryptoAuthentication family of devices. These chips are designed to securely authenticate any item to which they are attached. Each device can also be used to exchange session keys with a remote entity enabling the system microprocessor to securely encrypt/decrypt data. The devices are housed in small 3-lead SOT-23 packages with footprint areas of less than 7 mm² and package heights of 1 mm, making it simple to incorporate these devices into even the tightest of spaces. The family of devices is believed to be the only low cost authentication chips which implement SHA-256, and advanced encryption algorithm. Rapid advances in crypto analysis mean that older weaker algorithms may not offer an acceptable product lifetime. Using SHA-256 ensures the designer that the obsolescence of the product will not be caused by its security system.

But using the latest algorithms doesn't matter if an attacker can microprobe the chip or attack it in other ways to get the secret out. Consequently any authentication device needs to be fully protected from such attacks. For example, Atmel's devices feature a metal shield over the entire chip, internally generated clocks, onboard voltage regulation, and a host of other defenses against all the latest attacks.

For legitimate manufacturers of embedded systems and peripherals, it is easy to justify the cost of enhancing the security of their products against the losses of add-on and replacement revenue, losses in confidence in their company's products, and damage to the company or brand reputation from inferior "clones" invading their markets. Authentication devices, like CryptoAuthentication, offer inexpensive, easily implemented solutions to accomplish this – enhanced security can be surprisingly affordable.

World News In Brief

Smart-card ID 'Virtually Dead'!

South African Home Affairs Minister Nkosazana Dlamini Zuma declared that the project to provide every South African with a 'smart-card' ID is virtually dead.

There is no longer money in her department's budget for the scheme. The idea of the 'smart-card' was launched by Home Affairs in the time when Mangosuthu Buthelezi was the minister.

The ID program aimed to take advantage of rapidly developing technologies for encrypting fingerprints, for storing the whole of the population register digitally, for computer chips embedded in bank cards and so on.

Initially the ID card was thought to be used by banks to identify customers, and security firms to allow access to employees. However, the project slowed down, and eventually the banks denied of carrying forward the plan, thus barring the chance to help fund the scheme.

'No' to NFC-enabled Mobile Phones

It was at the NFC World, that Barclaycard's Head of Innovation Marketing, Sarah Mansfield, stated that by the end of 2010 Orange customers will be able to buy an NFC-enabled handset, and use an augmented-reality application to locate nearest retail outlet offering NFC, or the nearest cashpoint for those who insist on scratch-window cash. That app will run on an iPhone, or handsets using Google's Android platform. However, neither of those

platforms supports NFC - at least not yet.

Orange and Barclaycard did launch a co-branded credit card in January 2010, so perhaps Android and iPhone users will be able to use the augmented reality app to find places that will accept their plastic cards, while those equipped with NFC-enabled handsets must rely on the traditional window stickers.

NFC is beset by chicken-and-egg problems with operators not requesting handsets and manufacturers (except Nokia) not interested in making them.

1.5 Million Americans Victims of Medical Identity Theft!

According to a recent survey conducted by The Ponemon Institute (Experian's information services company), nearly 1.5 million Americans have been victims of medical identity theft.

One of the most common instances of medical identity theft is the use of a stolen insurance ID card in order to receive medical services. According to the study, more than 50 percent of consumers didn't discover that they had been victimised until at least a year after the incident or incidents had occurred.

Of those surveyed, only 9 percent of victims reported that they have completely resolved the crimes against them and restored their identity.

As a result of the situation, 55 percent of victims lost confidence in their health care organisations.



How secure is the biometric passport?

By Tom Tainton, Smartcard & Identity News



Tom Tainton

When the biometric e-passport was introduced in the UK in 2006 the Home Office hailed the rollout as a move to ‘improve the integrity and security’ of British border control. Four years on and their prediction is in tatters. In January, a Hamas official was killed in a Dubai hotel by hired agents, six of whom had fraudulent British passports. The biometric passport’s vulnerability to forgery left one man paying the heaviest price of all. So what are the risks with the technology and what can be done to prevent it being exposed by criminals?

Well, let’s start from the beginning – August 2006 in fact. It was here when the Home Office announced the launch of hi-tech documents, with added security features such as biometric data, in a bid to combat fraud. The chip inside the passport contains detailed information about the holder’s face – including the distances between eyes, nose and mouth. Information is stored in encrypted form on an RFID tag and has an antenna that means it can be read electronically. Officials claim the data is protected in three ways:

- A ‘digital signature’ which shows that data is genuine the country where the passport was issued.
- Basic Access Control, a chip protocol that prevents the data being read without the passport holder’s knowledge.
- Public Key Infrastructure (PKI), a digital technique that confirms the data was written by officials and not been tampered with.

The UK Identity and Passport Service declare that the documents are highly secure and protected by an advanced digital encryption technique. If that’s the case, how are fraudsters still getting our information?

Since its controversial inception many studies, including one conducted by The Guardian in the UK, have proved that information on a biometric passport can be viewed using easily attainable hardware and software. Because data is stored on an RFID tag, anyone with access to the passport will be able to read the chip. The Home Office maintains that RFID tags can only be read over a distance of 2cm. A team of Dutch researchers contacted chips at 30cm. This makes cloning of the passport possible, with the holder likely to escape detection because of the biometric document’s trusted reputation.

The technology is also susceptible to brute force attack. As things stand, a computer can keep trying until it gets the encrypted pin numbers correct. Wrong this time? Have another go. And another. The Home Office is being dangerously naïve, and others agree. Several years ago, a body entitled the Future of Identity in the Information Society (FIDIS) heavily criticised the biometric e-passport. It called the technology ‘poorly conceived’ and added that the risk of identity theft had in fact been increased.

But according to AIM UK, one of Britain’s leading technology trade associations, identity theft can be prevented. Communications manager Andrew Callaway says that while we assume a passport as the ultimate proof of identity, that’s no longer the case. “As we saw in Dubai, it is possible to forge a passport if an individual is sufficiently determined. This is a clear indication that the technology is inherently flawed and not as forgery-proof as we have a right to expect.”

Callaway insists that natural feature identification – a process that takes a fingerprint of a document’s fibre would make security breaches virtually impossible. “Natural feature identification would help to prevent the risk of forgery. Because the document contains millions of fibres it has a unique pattern in the same way as a human fingerprint. A ‘fingerprint’ of the document’s fibre could be scanned at immigration control. This would stop an individual from using a different passport and greatly improve security in the process.”

Perhaps the government will accept that the biometric passport is deeply flawed, and may even consider an alternative to the vulnerable RFID chip. Until that point, the technology will continue to serve only criminals – with disastrous results for everybody else.





Smart Thinking For Local Authorities

By Stephen Beecroft, independent smart technologies consultant



Stephen Beecroft

Under the Transport Act 2000 all English and Welsh Local Authorities were required to issue a travel permit free of charge to any elderly or disabled local resident who applied for it. This permit entitled them as a minimum to half price (concessionary) bus travel within the authority's area between 9.30am and 11pm weekdays, and any time at weekends and bank-holidays.

Gordon Brown, the then Chancellor, announced in his 2005 Budget Statement that by April 2006 there would be free off-peak bus travel for the elderly and disabled within their home district. Then in 2007, Ruth Kelly unveiled the new English National Concessionary Transport Scheme that, from 1st April 2008, provided the opportunity for everyone over the age of 59, and the disabled, free off-peak bus travel across England. Some authorities provide extended concessions for local residents, for example 9.00am start and later finish.

To add yet more complexity in early September 2007 the Department for Transport (DfT) confirmed that the pass should be compliant with ITSO (Integrated Transport Smartcard Organisation) the national transport standards for smart cards. The only exception to this, and DfT have been very clear about this, is London where Transport for London (TfL) enables the London Boroughs to issue the Freedom Pass. The target date for the Freedom Pass to be ITSO compliant is set for 2010.

Whilst all this activity around transport has been taking place a number of local authorities have also issued residents cards that provide the resident access to a variety of locally delivered services such as Library Membership, Leisure Membership, Discounted Parking, Cashless Catering in Schools and e-enabled collection of revenues, such as Rent, Council Tax, Sundry Debt and Garage Rent.

How Does This Help You?

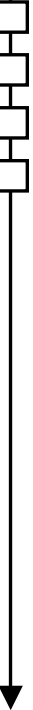
More than eight million English National Concessionary Transport Scheme (ENCTS) smart cards have been issued via every single authority in England outside of London, while London has arguably more smart card schemes than any other region of England. So, English residents are accustomed to smart cards and many of us use one daily.

Now the capability for every local authority to issue a smart card not only exists but is operational. Therefore Local Authorities can now start planning and enabling additional services, such as library and leisure centre access, on the concessionary transport smartcards they issue – but they must be aware the ENCTS cards issued before 2010 may have to be replaced for use with the additional citizen services.

A group of Local Authorities along with LASSeO (Local Authority Smartcard Standards e-Organisation) and SCNF (Smart Card Networking Forum) met in September 2009 at a conference in Cambridge and ratified a specification for the NXP DESFire card type that most Local Authorities are intending to issue from January 2010. LASSeO has published their specification and guidance for encoding multiple applications on a transport card. The specification includes basic cardholder information, cash collection, parking, identity and entitlement.

In November 2009 at an SCNF workshop in London, transport representatives from Local Authorities across England unanimously agreed that including other services on their ENCTS cards was an efficient way of delivering some services and indeed included in their future plans. And a study undertaken by an independent consultancy commissioned by the London Councils to provide guidance for Local Authorities in London, found that there was a positive business case for a multi-application smart card at borough level and more so at a pan-London level.

In 2010, concessionary card holders could be using their transport smart card to access services at their library, leisure centre, community centre and Town Hall.





Many of the ENCTS schemes were deployed on simple card production only systems, which are perfectly suitable for issuing a card with only one application on the chip and a static print design. This is exactly what the ENCTS card requires for public transport use. However once more applications are included, many schemes will need to be migrated to more comprehensive Card Management Systems (CMS) so that the Local Authorities or scheme operators can efficiently manage applications. Clearly Local Authorities will need guidance and advice from smart card consultants on timing and approach of any decision to migrate. There promises to be a real need for very flexible solutions and therefore CMS providers will have opportunities to consider.

Local Authorities are in the main keen to exploit their existing ENCTS scheme as an additional channel for delivering services to their residents but may well be deterred from pursuing that if it is expensive to do so. Card technology providers will need to nurture this as a long term opportunity, as if a quick return is sought experience shows that the Local Authorities will simply walk away especially given the current financial climate.

So to answer the original question:-

- The residents are comfortable with the use of smartcards and indeed embrace them for their convenience.
- The capability for Local Authorities to issue smart cards not only exists but is operational today and has been for almost 18 months.
- The appropriate smart card technology has been identified and agreed upon to enable uniformity without being anti-competitive.
- The Standards for encoding the smart card have been ratified.
- The Local Authority Business Case for most blends of application is positive and in many cases provided ROI within two years.
- CMS and Card Production suppliers have greater experience gained during the ENCTS launch and also from a number of other multi-application schemes launched in the last 12 months.

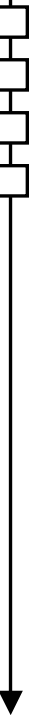
In addition, the analysis work required to complete the Business Case will identify how, by implementing a borough wide residents card, the authority will be contributing to National Indicators (NI's), Best Value Performance Indicators (BVPI's) and individual service plans which grab the attention of the Chief Executive right through to Service Managers. Whilst this may not be an easily calculated cashable benefit, the significance for the senior stakeholders should not be underestimated.

Why Didn't Local Authorities Take This Approach Sooner?

Before the concessionary transport cards were launched in England in April 2008, authorities had little time to consider other applications and today very few cards are used for more than bus travel. Although many of the cards were configured so other applications could be added, the announcement from ITSO that Mifare Classic® cards may not be issued after December 2009 put any additional application plans on hold – local authorities did not know what mix of cards they would have in 2010.

Now we are well into 2010, confidence is returning and most councils are opting for DESFire as the replacement and can expect this card family to meet their needs for several years to come – it is more secure, has 4K or 8K storage and additional security features which can be invoked in the future. This makes it possible to plan additional applications with reduced risk of technology change but does require a replacement of the Mifare Classic® cards, so card suppliers should see orders from clients that they sold Mifare Classic® cards to in the last 18 months.

SCNF is working with LASSeO to ensure the encoding specification for the DESFire cards is publicised to Local Authorities, implementation guidance is available, configuration options are understood and support can be provided if required. The specifications have been published on the LASSeO and SCNF websites.





The Death of the Token

By Dave Abraham, Signify



Dave Abraham

These days, it is widely accepted that two-factor authentication (2FA) is essential to secure remote access to sensitive information on the corporate network. And with the increase in remote and home working for greater flexibility, a better work/life balance and cost savings, the demand for 2FA is on the increase.

Once the decision has been made to deploy 2FA, the next question is whether to go for a solution based on hardware tokens or opt for a tokenless approach that makes use of mobile phones. Vendors that offer only a tokenless solution would have us believe that tokens will soon be replaced by tokenless authentication, which has led to much debate about the pros and cons of each. But is it really a case of one or the other?

Dedicated tokens - such as those produced by market leaders RSA - provide a one-time passcode, typically every 60 seconds, and have been the traditional approach to 2FA for many years. However, more recently, the introduction of tokenless solutions has been hyped, mainly due to their ability to deliver one time passcodes on demand to a standard mobile phone or smartphone such as the popular Blackberry. After all, most people already carry one of these devices with them, most of the time.

A tokenless solution therefore eliminates the need to carry a separate piece of hardware – albeit usually attached to a key fob - and reduces the costs and time associated with provisioning new and replacement tokens. Sounds ideal; but it's not the full picture and the simple truth is that tokens remain the best solution for frequent users who rely on getting secure remote access to systems and information from any computer at any time.

Road warriors, home workers or systems engineers, for example, often log into many different portals every day and requesting or obtaining passcodes from a mobile phone or PDA is far too much hassle.

What's more, tokens are not limited to a particular platform such as Windows and are not reliant on how secure a mobile phone network is, good network coverage or the battery life of the phone. They are also more robust. RSA tokens will work even if dropped from a great height or if they fall in a glass of water. The same is not true of the mobile phone.

It is much easier and reliable for frequent users to carry a token that automatically and continuously generates passcodes for immediate access.

And when it comes to cost; frequent users can quickly run up SMS charges for requesting passcodes from a mobile phone or PDA.

But this is not to say there isn't a place for tokenless authentication; it is ideal for infrequent or temporary users and for those that simply do not want to carry a separate device. As it requires an additional request stage, tokenless authentication is best suited to occasional users, contractors, part-time staff and those checking email from home, for example. It can also provide temporary extranet access to other departments, professionals and partners or for sensitive online services such as HR, e-commerce or access to health information. Having short term remote access to the corporate network is also valuable in emergency scenarios as a result of bad weather, strikes or terrorist threats, for instance.

The reality is that it's a case of 'horses for courses', depending on the organisations, the user's working requirements and the data and applications they are accessing. In fact, for most organisations the question shouldn't be which option to go for, but what combination of token and tokenless 2FA they need.

The ability to mix both token-based and tokenless two-factor authentication within an organisation means that authentication can be tailored to meet specific needs, budgets and working patterns. But, having realised the benefits of deploying both token and tokenless 2FA, the problem organisations will face is that most two-factor authentication vendors will only offer one or the other.

By deploying two-factor authentication as a hosted service, this hurdle is eliminated by removing all the hassle of setting up, deploying and managing both a flexible token and tokenless two-factor authentication solution. Using a cloud-based service means that organisations can reap the benefits of both options and choose the right authentication based on specific users' needs. In addition, a hosted authentication service delivers proven





security and guaranteed reliability along with a lower total cost of ownership. And when it comes to tokens, it removes any of the complexities and logistics of deploying the tokens, ensuring fast, reliable and flexible service delivery.

So yes, the death of the token is greatly exaggerated. Through the delivery of 2FA as a service in the cloud, tokens will always remain the most reliable choice for many users. While the battle between the token or tokenless vendors suggests that customers have to choose one or the other, the simple truth is that organisations need to take a flexible 'best of both' approach that meets the requirements of different types of user.

Signify is exhibiting at Infosecurity Europe 2010, the No. 1 industry event in Europe held on 27th – 29th April in its new venue Earl's Court, London. The event provides an unrivalled free education programme, exhibitors showcasing new and emerging technologies and offering practical and professional expertise. For further information please visit www.infosec.co.uk

World News In Brief

LaserCard Wins \$850,000 Vehicle Registration Card Program in Middle East

LaserCard Corporation, one of world's leading providers of secure ID solutions, has been selected to manufacture and supply vehicle registration cards for the Middle Eastern nation - Saudi Arabia. A recent \$850,000 purchase order follows an initial order valued at approximately \$560,000 shipped earlier this fiscal year.

This new program expands LaserCard's footprint in the Middle East, where the Company supplies multi-technology, highly secure national ID cards to the Kingdom of Saudi Arabia to address the varied needs of the government ID market, regardless of application and the technologies required. The program also marks LaserCard's fourth vehicle registration program win, following three successful, on-going programs for the state authorities in India. The new cards are high quality, durable documents incorporating high-resolution security printing and other innovative features.

Barclays revamps Mobile Phone Banking Service

British financial services provider Barclays has added a new feature to its mobile phone banking service, which is set to allow customers to make payments to third parties.

Through the provision of this service, Barclays allows customers to pay funds to existing or new beneficiaries that have been set up on online banking. An interface has also been developed for mobile phone viewing.

Launch of New Dual-Interface EEPROM Enabling Remote Access

STMicroelectronics, a world leader in RF Memory and EEPROM ICs, has announced sample availability of the first in a new family of products that provide the flexibility to remotely program or

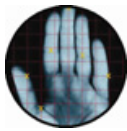
update electronic products, anytime during their lifetime, and anywhere in the supply chain. The new devices enable manufacturers to update parameters, regionalise or activate software without connecting a programmer, or even opening the retail packaging. This pioneering way to access the memory will allow businesses to add new functions and capabilities to their products, but also reduce manufacturing costs, simplify inventory management, and respond more quickly to changing market demands.

The M24LR64 is an EEPROM memory with a standard I2C serial interface, providing communication with most microcontrollers or ASICs, and also a standard ISO15693 RF (radio frequency) interface for wireless communications with RFID readers. The ISO15693 standard is passive RFID technology, which gathers both the energy and the data from the RF system. No power is required to operate the M24LR64 in RF mode, which enables on-board energy savings and provides easy and convenient remote access to electronic product parameters.

ARM to Reshape the Smartcard Market with SC000 Processor

ARM announced at the Cartes-Asia conference in Hong Kong, the launch of the highly compact and energy-efficient ARM SecurCore SC000 processor (pronounced SC triple zero), designed specifically for the highest volume smartcard and embedded security applications.

The SC000 processor is the latest addition to the successful ARM SecurCore family of processors, greatly expanding the range of target applications into tamper-resistant contact and contactless Smartcards such as SIM, government, banking, transport, ID and conditional access. Delivering unprecedented feature-rich 32-bit performance in competitive 8/16-bit cost, area and power footprints, the SC000 processor is ideally suited for the next-generation devices in the highest volume smartcard markets.



Biometric Data Protection in the Education Sector

By Peter Hodgson, Founder and CEO of Brightfilter Limited



Peter Hodgson

Although many of us use portable storage devices to conveniently transfer data from one location to another, most of us will freely admit that these devices are not encrypted, allowing anyone to access the data if lost or stolen. In many instances, losing information is merely an inconvenience. But if the lost device contains private data left open to be accessed by anyone, the consequences can be remarkably serious, especially if the personal records of children fall into the wrong hands. Despite this, many child-centred organisations continue to use unencrypted data devices that are misplaced on a frequent basis. Two years ago, Leeds City Council lost a USB stick that contained the names, ages and addresses of 80 children, a significant breach of the DPA (Data Protection Act.) The Chief Executive of the council was told that personal information should not have been uploaded to the

drive as it was not encrypted, providing anyone with access to the details. A year later, a USB stick from a Vale of Glamorgan council that contained confidential child protection information including medical records and details of court cases was found in the street, neither encrypted nor password protected.

A large number of school staff also uses USB drives to carry around private student records and information. However, a study conducted in 2008¹ revealed that nearly half of England's primary school teachers back up pupil data on portable storage devices and take them out of school without encrypting them first. The consequences of losing an unencrypted device can range from internal issues such as pupils gaining access to peer records, to much graver circumstances if the names and addresses of schoolchildren fall into the hands of a paedophile.

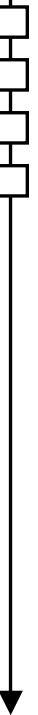
It is also in the school's interest to encrypt its data, as section 7 of the DPA requires that "appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."² Non-compliant schools can receive serious legal penalties, not to mention a severely damaged reputation. Such potential risks reflect the need for schools to adopt a highly secure method of transporting data. BECTA (The British Educational Communications and Technology Agency), the Government's lead agency for ICT in education recommends that, "as well as protecting data on devices and media, organisations should also encrypt personal data that is transmitted between systems, applications or locations."³

One effective, compliant solution is biometric encrypted USB drives. Many schools have already implemented biometrics for registration, locker access and school dinner payments, although this method has yet to be extended on a wider scale to data protection, despite the numerous benefits. Biometric encrypted USB keys provide a high level of security as accessibility can only be achieved by one authorised user. Access cannot be shared as biometric properties are unique to each person, making it extremely difficult to duplicate a copy of a fingerprint. Biometric systems have been developed around the unique characteristics of individuals, therefore making the probability of two people sharing the same biometric data virtually nil. Losing a biometric property is also a rare incident, often only occurring in the case of a serious accident.

Further benefits schools can receive from biometrically encrypting data include:

- Powerful protection using two-factor authentication; 'something you have' (your fingerprint) and 'something you know,' (a password)
- Teachers and IT staff no longer needing passwords that may be hard to remember, shared or seen by unauthorised individuals
- An exceedingly high level of security at a relatively low cost
- Convenient data mobility whilst also complying with DPA legalities
- Management of all USBs on a school network from a centralised administrative system

The benefits to this last point also extend beyond data protection. Students plugging their own USB drives into computers are a common cause of viruses in school IT infrastructure, as seen with the Conficker virus. Conficker started near the end of 2008, developing into a sophisticated and resilient infection that spread rapidly to shut down computer defences. The virus is thought to have entered school networks via USB sticks





and is estimated to have spread to over 7,500 school computers since its launch. Preventing widespread virus infections is an ongoing challenge, with IT staff often resorting to gluing up USB ports to restrict access. However, by installing a centralised management system, staff can control access to any USB stick on the network and block unencrypted drives.

If schools were able to give each member of staff a biometric encrypted USB drive, the results would be hugely beneficial. Lost or stolen devices would no longer threaten privacy, as even if one fell into the wrong hands, the unauthorised individual would not have the ability or correct biometric characteristic to gain access. It would also protect schools from legal penalties, as they would be able to prove that responsible measures had been followed to ensure data was safely protected. The future of biometric school data protection would lead to a highly protected, impenetrable network that offers the convenience of data transportation whilst ensuring that children's private details remain safely locked down.

¹ <http://news.bbc.co.uk/1/hi/education/7171740.stm>

² http://www.ico.gov.uk/for_organisations/data_protection_guide/list_of_the_data_protection_principles.aspx (no. 7)

³ http://schools.becta.org.uk/upload-dir/downloads/information_handling.pdf (section 4.2.3)

World News In Brief

Software Sniffs out Criminals by the Shape of their Nose

With worries about illegal immigration and identity theft, Dr Adrian Evans and Adrian Moorhouse, (University of Bath's Dept of Electronic & Electrical Engineering) and Professor Melvyn Smith and Dr Gary Atkinson from University of the West of England (UWE's) Machine Vision Laboratory decided to investigate whether images of people's noses could be used to recognise individuals. They used a photographic system called PhotoFace, developed at UWE, to scan the 3D shape of volunteers' noses and used computer software to analyse them according to six main nose shapes: Roman, Greek, Nubian, Hawk, Snub and Turn-up. Instead of using the whole shape of the nose, the researchers used three characteristics in their analysis: the ridge profile, the nose tip, and the nasion or section between the eyes at the top of the nose. Whilst the researchers used a relatively small sample, they found that nose scanning showed good potential for use as a biometric, with a good recognition rate and a faster rate of image processing than with conventional biometric techniques such as whole face recognition.

FT to use PayPal for Daily, Weekly Payments

Financial Times (FT) CEO John Ridding has announced that the day and weekly pass will be powered by PayPal (the e-commerce business owned by eBay) and will begin in the next few months. The move is different from FT.com's regular annual subscription, which appears as a direct payment.

News of the FT's collaboration with PayPal underscores the newspaper's emphasis on digital subscriptions amid an increasingly difficult climate for print media. While Pearson, the parent company of the FT, recently posted a 13% increase in profits from last year, the FT Group, which includes FT Publishing and Interactive Data, reported that revenues dropped by 12% in the last year.

Verayo Launches Next Generation of Unclonable RFID Chips

Verayo, a security and authentication solutions provider has launched its next generation of RFID ICs based on the company's innovative Physical Unclonable Functions (PUF) technology. The first chip of the new product family, the Vera M4H, delivers authentication and security to mass transit tickets, secure IDs and access cards and consumer product anti-counterfeiting, where cost has been an impediment for adoption.

DarkMarket Mastermind Jailed

The mastermind behind one of the most pernicious online criminal forums in the world has been jailed for four years and eight months (26 Feb, 2010). The site, DarkMarket, was a sophisticated, invitation-only service for buying and selling compromised credit card data and other information and equipment for committing financial fraud. It allowed criminals to collaborate on deals which caused global losses worth tens of millions of pounds.

In the dock alongside Renukanth Subramaniam was 66 year old John McHugh, known online as 'Devilman'. McHugh was sentenced to two years. The trial is the latest stage in an international investigation by SOCA, the FBI and the USSS.



G&D Wins CIT Golden Card Award for Cell Phone Sticker

Convego(r) Air Mobile, the sticker for contactless payment from Giesecke & Devrient (G&D), was a winner at this year's CIT Golden Card awards in the category of "most innovative payment card". Organised since 2002 by IIR, the Institute for International Research, the Golden Card awards set out to recognize excellence in the smart card industry. The awards are given in conjunction with the CIT Congress, Spain's leading smart card event, held annually in Madrid.

Next-Generation Powered Display Card Released

NagraID Security, with over 1 million display cards deployed in 29 countries, is the world leader in Display Card manufacturing. NagraID Security further extends its technological leadership with the introduction of a 12-button Touch-Keypad Display Card. The new open platform enables NagraID Security and their partners to develop and implement multi-function applications on a single card.

STORK One Step Closer to eID Pilot Projects across the European Union

STORK, a pilot scheme co-funded by the EU that aims to implement EU-wide interoperability of electronic identities (eIDs), announced the availability of the latest approved and public project deliverables. Deliverables of note that are now fully accessible to stakeholders, include reports on process flows, the recently defined pilot-specific and eID common specifications together with draft planning for the forthcoming pilots.

Gemalto Receives "2009 SmartGrid Product of the Year" Award

Gemalto's MASSIM solution has received a 2009 SmartGrid Product of the Year Award from Technology Marketing Corporation (TMC) and Intelligent Communications Partners.

Gemalto has developed a unique technological advancement aimed at meeting smart grid service needs. The MASSIM concept is an M2M solution specifically designed to detect if a machine-to-machine wireless network subscriber identification module has been removed from a utility meter and placed illegally within another device. This detection ensures the essential connectivity element within the smart grid ecosystem is tamper proof, protecting the utility and wireless operator from fraud. MASSIM is highly customisable with multiple environmental sensing parameters and sends a service provider alert in the event of unexpected change.

Now start Tweeting with your Voice

Viva, the fastest growing mobile carrier in Dominican Republic announced that it has launched TwitVoz (Call-n-Tweet) service on its mobile network. The solution has been sourced from Kirusa, the world's leading vendor of Voice SMS and a leading developer of mobile value added services.

With this launch, Viva DR mobile subscribers can update their status on Twitter through voice tweets. This provides a very convenient alternative to texting. The service is available to all Viva DR GSM and CDMA subscribers across Dominican Republic, whatever the mobile handset model is, they do not need a smart phone.

STMicroelectronics Delivers 90nm STM32 MCU with Unique Flash Accelerator

STMicroelectronics has announced two significant advances that further improve the performance and power consumption of its successful STM32 family - availability of production devices featuring embedded Flash at 90nm process technology; and industry's first Adaptive Real-Time (ART) memory accelerator optimised for the STM32's industry-standard ARM Cortex-M3 processor.

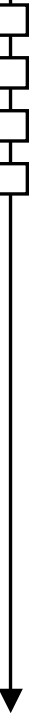
The first production STM32 microcontrollers leveraging ST's 90nm embedded Flash technology, deliver faster operation, increased peripheral integration, lower power consumption, and increased on-chip memory densities.

The proprietary ART memory accelerator balances the inherent performance advantage of the ARM Cortex-M3 over Flash memory technologies, which normally requires the processor to wait for the Flash at higher operating frequencies. The CPU can now operate up to 120MHz without waiting, thereby increasing overall system speed and efficiency.

Release of World's First WiFi-enabled SIM

One of the world's leading smart card manufacturers, Sagem Orga (Safran group), will be presenting the world's first Wireless LAN SIM card at the international CTIA Wireless show to be held on March 23 – 25, Las Vegas, Nevada, USA.

The flexibility of a Wireless LAN connection can now be enjoyed with any mobile phone, combined with the high security of a SIM card. World's first WiFi-enabled SIM (ConnectSIM™) can be used in any mobile phone to enable fixed-mobile convergence, proximity transactions, trusted peer-to-peer operations between two SIM cards, strong authentication services, WEB security, etc.





Beyond Conferences

By Peter Tomlinson and Pamela Bells



Peter Tomlinson

In last year's clutch of conferences about public transport, organisers understood that key components of providing good service to the public are ticketing systems and associated service management. By the end of the year, both DfT and local government were making new plans in this area, and the 2010 Transport Ticketing Conference tried to update us.

Day 1 of the Conference was like a meeting of old friends - a re-acquaintance with some things old, combined with the latest news of progress both in the UK and from abroad. The day consisted of a series of varied presentations including practical experiences from the Netherlands: the OV Chipkaart project illuminated by Thomas Osinga of TransLink Systems. Nationally recurring themes appeared, with a number of 'positive' ITSO messages throughout the

day and a general feeling that 'plans' were being made, starting with Chris Lewis of Transport for London who spoke about the integration challenges for the Oystercard and future plans. Key in these plans is ITSO and EMV acceptance, being progressively rolled out between 2011 and 2015. Details were given of their new card reader capable of producing ITSO, EMV and Oyster transactions - all of which must have been welcome news to Professor Brian Collins from the Department for Transport (DfT), who spoke about embracing new technology and the need for 'integration'. Prof Collins went into some detail on recent developments including the DfT ticketing strategy (published Dec 2009) and the appointment of a new CEO of ITSO to provide added leadership on the commercial aspects of ITSO. The DfT are developing a 5 year plan, with funding already going into 9 major urban areas, combined with an assessment of where they want to be in 2015 and how they can make ITSO more important in the context of smart and integrated ticketing. Questions addressed first the business case in the strategy, in particular for rail, and then about addressing what passengers need.

Of interest to the PTEs on the topic of settlement was Lewis Nolan of Visa Europe who spoke about Visa payWave technology in the transport market, and Visa Europe's plans to accelerate the market rollout of payWave. Visa payWave is designed to penetrate the low value transaction segment, and Visa Europe views their pay@gate contactless ticketing as an alternative to or replacement for the Oystercard. To be fair about fares, MasterCard is equally active in this space. The day ended with a thought provoking panel discussion on new fare media, with a promise of a 'Day 2' with more of a focus on NFC and case studies.

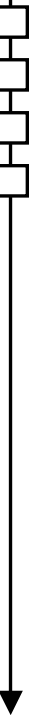
Day 2 was even more of a re-acquaintance experience. It started with further international case studies and then moved on to technology: ITSO, bar codes, NFC and work on pan-European through ticketing and the passenger.

Six weeks later, at the March Transport Card Forum (operated by Smartex in collaboration with DfT), it once again became clear that, in improving public transport, the challenge continues to be to respond to the unique demography of the UK: many urban centres quite close together, with rail and bus and coach services connecting them. At the TCF we heard of long running research that looks at why public transport in many dense urban environments (including London) works well. London's Oyster scheme is not scalable to cover the whole country, yet we need interoperability within and between the various urban areas, and also through ticketing. From the very beginning (12 years ago) of the discussions that led to ITSO, we addressed that, working with the UK demography, setting out three principles for a set of interoperable schemes linked by a data network:

- Smart Media ticketing
- Automated journey management
- Reporting all transactions and related management information

That was based on the assumption that the costs of data communications, data storage and processing power would fall dramatically – and they have done just that. But ticketing and associated management technology are just tools for public and private sector to use.

¹ <http://www.dft.gov.uk/pgr/regional/smart-integrated-ticketing/>





World News In Brief

Rs 25 Crore Spent On Global Credit Cards!

Who paid Pakistani-American terrorist David Coleman Headley's international credit card bills is at the heart of a widening probe which has revealed that at least Rs 20 (₹3 million) to 25 crore (₹3.7 million) was spent by terror suspects across India in the recent past through such credit cards.

Intelligence agencies, tracking economic footprints and wide network of jihadis (Islamic terrorists) and their sleeper cells in different cities, have found that of late, terror suspects have been using international credit cards issued in the US, Canada, the UK, Dubai, Nepal and Bangladesh and bills are picked up by their handlers based in these countries.

Further investigation has revealed that Rs 20-25 crore was withdrawn in all parts of the country, including Delhi, Mumbai, Bangalore, Hyderabad and Kashmir, indicating the wide spread of terror networks and the ease with which they manage to dupe the surveillance system.

Latest Software Application to Personalise NFC-enabled Devices for the Payment Industry

NBS Technologies Inc., a leading provider of hardware and software solutions for card personalisation, smart card and semiconductor equipment solutions, has announced the addition of a Near Field Communications (NFC) application to its tried and tested suite of personalisation software, UbiQPersoMaster.

NBS's UbiQPersoMaster software application is aimed at the personalisation of NFC devices to enable secure financial transactions. Financial institutions utilising this application can effectively personalise a customer's NFC-enabled mobile phone with their credit card information, similar to the current contactless credit card. A customer's mobile phone needs to be waved in front of the NFC-enabled POS terminal only to get the purchase registered on the customer's account.

Loss of 46,000 individuals' Personal Financial Information by Zurich Insurance

The Information Commissioner's Office (ICO) has found Zurich Insurance plc in breach of the Data Protection Act after it lost an unencrypted back-up tape containing financial personal information belonging to 46,000 policy holders of Zurich Private Client, Zurich Special Risk and Zurich Business Client, which are all part of Zurich Insurance plc.

The back-up tape, which also included personal

details of 1,800 third parties, was lost by a sister company, Zurich Insurance Company South Africa, during a routine transfer to a data storage centre in South Africa. The data loss occurred on 11 August 2008 although the sister company did not inform Zurich Insurance plc until over a year later.

UK Branch Manager of Zurich Insurance plc, Stephen Lewis, has now signed an Undertaking to ensure that where any future movement of back-up tapes is required appropriate data security procedures including the use of encryption where appropriate, are in place.

Mobile Banking App for Blackberry and iPhone in Canada

ING Direct is the first Canadian bank to offer mobile banking apps for both the BlackBerry and iPhone. Canadians will now be able to save anywhere, transfer funds, check balances, and review transactions with the new apps. Customers simply use their current online Client number and PIN to login.

ID Cards for the Homeless

The Calgary Herald has reported that the province is working on ways to provide ID cards to homeless people that could include biometric samples of fingerprints or facial scans.

In a meeting with the Herald editorial board, Housing Minister Jonathan Denis said his department is in discussions with Service Alberta about creating an Alberta ID card for the homeless. According to Mr. Denis, "Identification does have value on the street and we have to make sure we have those adequate controls in place". The ID cards would help them get on their feet with a bank account, things that one can't get without identification.

Read more here: <http://www.calgaryherald.com/>

L-1 Identity Solutions Unveils Latest Biometric Access Control Device

L-1 Identity Solutions, Inc., announced a new access control solution based on finger vein recognition technology, the 4G Finger Vein Station. This is the first L-1 solution to incorporate vein recognition and the Company's line of access control devices now support vein, finger and face recognition.

Very dry, dirty or worn fingers pose a challenge for standard fingerprint readers and the 4G FingerVein Station offers an alternative for these conditions found commonly in industrial and manufacturing environments. The use of near-infrared light to gather biometric data means that the condition of the skin surface does not affect accurate processing.

The most comprehensive examination of Retail Cards
and Payments on the market

SMi Present...

Retail Cards and Payments

12th & 13th May 2010, Crowne Plaza Hotel – St James, London

Gift, Loyalty &
Open-Loop Prepaid

Our Key speakers include:

- **Will Shuckburgh**, New Business Development Director, Nectar
- **Arun Glendinning**, Business Services Manager, B&Q
- **Michael Birchall**, Payments Product Manager, Post Office
- **Andrew Sellers**, Development Manager, Commercial, John Lewis
- **Jon Levenson**, Director of Commercial Partnerships, Trafford Centre
- **David Cabreza**, Director Financial Services, Hilton Hotel Group
- **Bede Feltham**, Marketing Director, Squid Card
- **Fiona Duncan**, Head of Prepaid, VISA Europe
- **Julian Bonnett**, Sales and Marketing Manager, Marriott Hotels
- **Brian Dunne**, CEO, Action Solutions

An in-depth focus on every aspect of the Retail Payments Market; Loyalty Cards, Gift Cards, Voucher Schemes, Open-Loop Prepaid Cards, Mobile & Contactless Technology and much more...

HALF DAY POST-CONFERENCE WORKSHOP

Setting up a Gift Card Program – Defining the Benefits and Pitfalls

In association with Action Solutions

14th May 2010, Crowne Plaza Hotel – St James, London

Please quote Smart Card News and receive £150 off the delegate place

REGISTER ONLINE AT:

www.smi-online.co.uk/retailcard16.asp

Alternatively contact Marta Szymaniak on +44 (0) 20 7827 6180 or
mszymaniak@smi-online.co.uk