

With Canada going to chip cards, will fraud migration force U.S. banks to EMV?



**Securing the campus
with contactless cards
and biometrics**

**Government ID update:
FIPS 201, ePassports,
and TWIC**

**States prepare for 'Real ID'
driver license reforms**

**Pentagon deploys
handheld ID readers**



" Trustworthy "



zero guess work. just **verified.**

INSTANT ON THE GO IDENTITY VERIFICATION.

VERIFY ID CARDS ANYWHERE FROM PARKING LOTS TO PORTS. ADD PHOTOGRAPHS OR FINGERPRINT CHECKS TO CARD SYSTEMS. GIVE LAW ENFORCEMENT OFFICERS A WAY TO SCREEN SUSPECTS AGAINST FINGERPRINT DATABASES WITHOUT RETURNING TO HEADQUARTERS.

DATASTRIP'S DSVII MOBILE CARD READER:
THE SOLUTION FOR WIRELESS IDENTITY CHECKS.

be **trusted.**



800.548.2517
www.Datastrip.com



LEGIC®
innovation in ID technology

The Choice **Today** for **Tomorrow**



Every day more than 70 million people use **LEGIC** at work and play. Learn how you can provide employees and visitors with one ID for multiple applications. Even if you only need one contactless smart card solution today, with **LEGIC** you're ready for tomorrow. Ask for **LEGIC** inside!

It's **Innovative**. It's the **Future**.

LEGIC®
innovation in ID technology

www.legic.com ph: (630) 717-5843

Spring 2007

6 | OPINION | The worldwide federation of identity

8 | BANKING | As Canada's payment cards go to EMV, will fraud migration push U.S. banks to join the smart card?

17 | DIGITAL ID | Authentication for financial services is a global goal with regional approaches

20 | MILITARY ID | Pentagon deploys handheld PIVMAN system to validate FIPS 201 IDs

22 | ISSUANCE | Tracking misprints and bad cards can be as important as tracking good ones

24 | ACCESS | Modular approach enables Lenel IdentityDefender to meet HSPD-12 needs of large and small organizations

28 | TWIC | TWIC cards hit the road in March but readers to check them remain stuck in neutral

30 | APPLICATION | No change, no problem ... with smart card-enabled parking meters

32 | INSIGHT | Secure ID submissions from our annual Expert Panel series:

- Trickle down effect of HSPD-12
- Keeping up with rapid security pace
- Internet savvy smart cards
- Securing financial transactions

34 | REGULATION | Feds may yank Regulation E's receipt requirement for small dollar transactions

38 | PASSPORTS | Machine Readable Travel Documents with biometric enhancement: The ICAO Standard

40 | INSIGHT | Contactless submissions from our annual Expert Panel series:

- 'Tap and go' payments on a roll
- The e-wallet, e-passport, e-pedigree
- Long range, driver-based vehicle ID
- Contactless trials bode well

48 | CASE STUDY | PricewaterhouseCoopers uses LEGIC technology for ID, security, print management

54 | CAMPUS ID | Philadelphia's sixty high schools issue contactless campus ID cards

55 | INNOVATION | Contactless ready to make its mark on campus

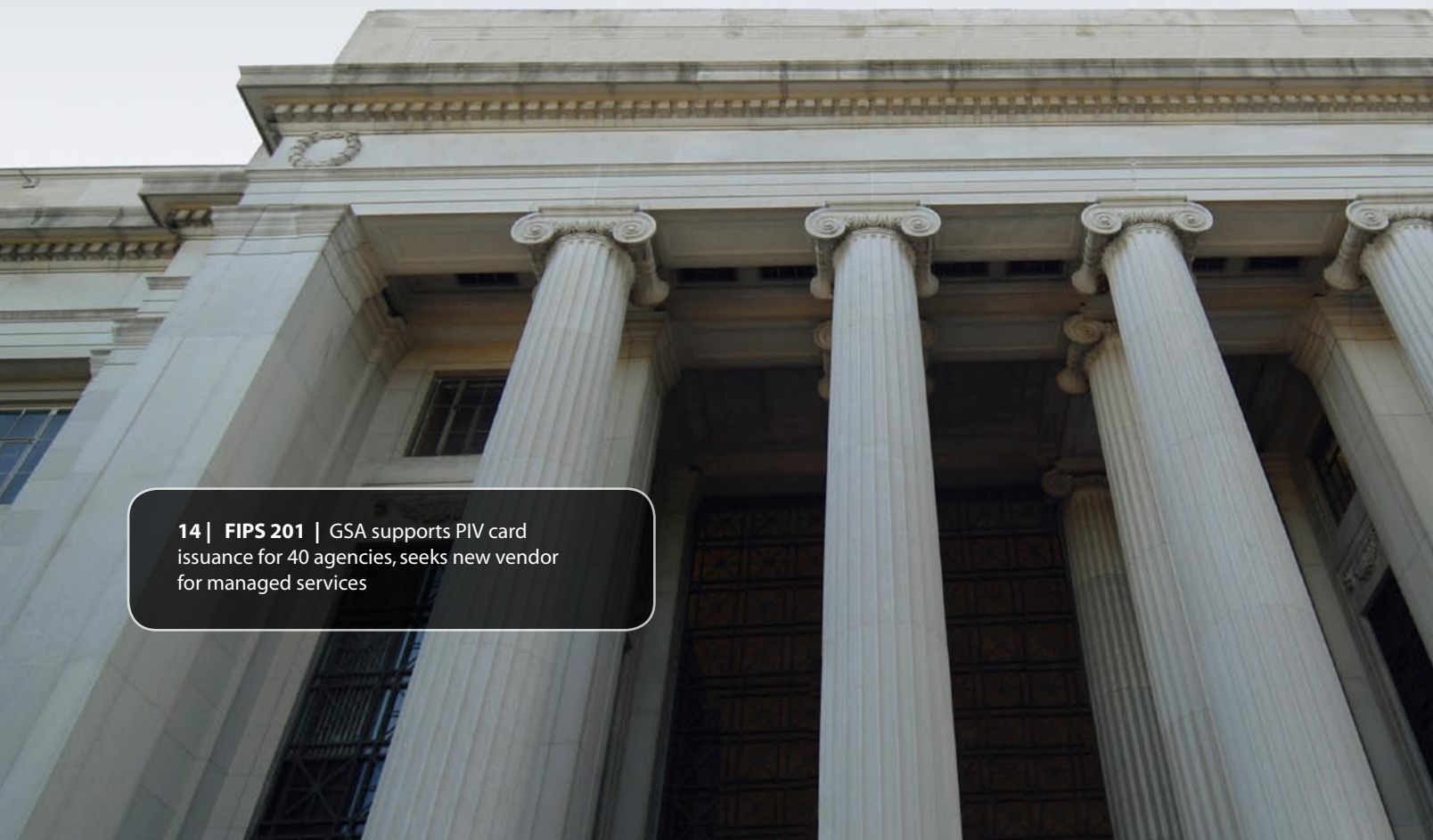
56 | BIOMETRICS | Biometrics gets its 'fingers' into school foodservice and other campus environments

62 | TECHNOLOGY | Is RuBee the next generation of RFID?

64 | RFID | The death of the 'Six Months Rule' for retail RFID strategy

66 | APPLICATION | Creating an ePedigree for sports collectibles with RFID

14 | FIPS 201 | GSA supports PIV card issuance for 40 agencies, seeks new vendor for managed services



Contents

INDEX OF ADVERTISERS

Datastrip	2
www.datastrip.com	
Legic	3
www.legic.com	
Datacard	7
www.datacard.com	
CoreStreet	9
www.corestreet.com/pivman	
Lenel Systems International	13
www.lenel.com	
Evolis	19
www.evolis.com	
Sagem Morpho	21
www.morpho.coom	
Digimarc	23
www.digimarc.com	
Muehlbauer	27
www.muehlbauer.de	
Digital Identification Solutions	29
www.edisecure.com	
Ultra Electronics	35
www.magicard.com	
XceedID	37
www.xceedid.com	
Smart Card Alliance	43
www.smartcardalliance.org	
CPI Card Group	47
www.cpicardgroup.com/contactless	
TokenWorks	51
www.tokenworks.com	
Fargo	53
www.fargo.com	
Visionbase	57
www.visionbase.com	
ASSA ABLOY ITG	67
www.assaabloyITG.com	
HID	68
www.hidcorp.com	

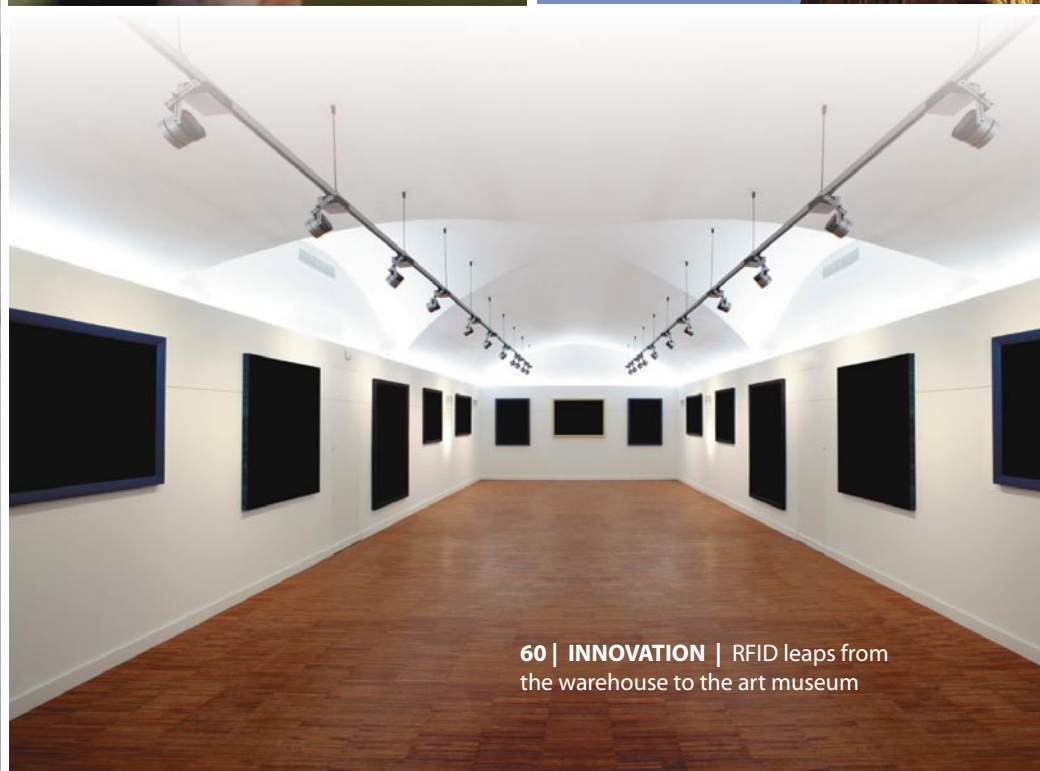


50 | FINANCIAL | Instant issuance of Visa and MasterCard directly from your card office personalization system



26 | GOVERNMENT | States prepare for Real ID in advance of pending driver license mandates

44 | PAYMENT | Contactless hits Broadway with Visa payments in leading theatres



60 | INNOVATION | RFID leaps from the warehouse to the art museum

Upending the inverse relationship between security and convenience

Chris Corum

Executive Editor, AVISIAN Publications

Security and convenience are nearly always inversely related. As one increases, the other generally decreases. Take the following example: the most convenient way to get into a home is through a wide open door, but this leaves the house extremely vulnerable. Add a number of dead bolts, post an attack dog, and electrify a fence, and you have a very secure home, but not one that is convenient for the residents. This principle holds true for technology as well as houses.

Though long considered bastions of security, identification technologies have been plagued by a lack of user convenience. They have served their intended purpose, but individuals did not want to use them because they got in the way.

This inverse relationship is beginning to change. As you will find in a number of the articles in this issue, identification technology is breaking this norm, combining security and convenience in a single package.

In his investigation of EMV chip-based payments in North America, contributing editor Andy Williams finds that the future of U.S. bank cards may meld the security of EMV with the convenience of contactless payments. It is interesting to learn how neighboring markets can be driven by these divergent forces in very different ways ... security or fraud reduction driving Canada to 'chip and PIN' while user convenience drives the U.S. to 'tap and go.'

This merging of security and convenience is also a key thread in our investigation of biometrics in our children's cafeterias, contactless credentials at both corporate and educational campuses, and even RFID tags guarding collections in art museums.

In each of these instances, the need for added security has long existed, but available technical solutions were deemed too burdensome or inconvenient. Improvement in technology, however, is enabling these environments—and countless others—to secure the 'doors to their houses' while still facilitating convenient access for residents.

I hope you enjoy this issue of re:ID.

EXECUTIVE EDITOR & PUBLISHER

Chris Corum, chris@AVISIAN.com

CONTRIBUTING EDITORS

Nate Ahearn, Daniel Butler, Ryan Kline, Marisa Torrieri, Andy Williams, David Wyld

ART DIRECTION TEAM

Darius Barnes, Ryan Kline

ADVERTISING SALES

Chris Corum, chris@AVISIAN.com
Angela Tweedie, angela@AVISIAN.com

SUBSCRIPTIONS

Regarding ID is free to qualified professionals in the U.S. For those who do not qualify for a free subscription, or those living outside the U.S., the annual rate is US\$45. Visit www.regardingID.com for subscription information. No subscription agency is authorized to solicit or take orders for subscriptions. Postmaster: Send address changes to AVISIAN Inc., 315 E. Georgia Street, Tallahassee, Florida 32301.

ABOUT REGARDING ID MAGAZINE

Regarding ID is published four times per year by AVISIAN Inc., 315 E. Georgia Street, Tallahassee, Florida 32301. Chris Corum, President and CEO. Circulation records are maintained at AVISIAN Inc., 315 E. Georgia Street, Tallahassee, Florida 32301.

Copyright 2007 by AVISIAN Inc. All material contained herein is protected by copyright laws and owned by AVISIAN Inc. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopy, recording or any information storage and retrieval system, without written permission from the publisher. The inclusion or exclusion of any does not mean that the publisher advocates or rejects its use. While considerable care is taken in the production of this and all issues, no responsibility can be accepted for any errors or omissions, unsolicited manuscripts, photographs, artwork, etc. AVISIAN Inc. is not liable for the content or representations in submitted advertisements or for transcription or reproduction errors.

EDITORIAL ADVISORY BOARD

Submissions for positions on our editorial advisory board will be accepted by email only. Please send your qualifications to info@AVISIAN.com with the message subject line "Editorial Advisory Board Submission."

STRENGTHEN SECURITY, PROTECT BUDGETS

INTEGRATED ID SOLUTIONS

DISCOVER WHY SECURITY PROFESSIONALS TURN TO DATACARD FOR A TOTAL SOLUTION

With ID card solutions from Datacard Group, you can enhance your security program without sacrificing your budget. That is why corporations, governments and other organizations make Datacard® the world's best-selling brand of photo ID solutions.

We offer everything you need to issue ID cards quickly and efficiently. We integrate and test every component for seamless compatibility. So, you can expect outstanding power, performance and value.

To learn more, call +1 800 356 3595, ext. 6623.

Or visit us at www.datacard.com/ID.



PHOTO ID
SYSTEMS



CARD
PRINTERS



ID SOFTWARE
AND CAPTURE
SOLUTIONS



SUPPLIES



As Canada's payment cards go to EMV, will fraud migration push U.S. banks to join the smart card world?

Andy Williams

Contributing Editor, AVISIAN Publications

With Canada and Mexico rapidly moving towards EMV deployment, witness the world's largest player in the credit card market, the United States, left out in the cold. Some say it's not a matter of if, but when, the U.S. will implement EMV. One reason: once its northern and southern neighbors are EMV-complaint, crooks may find much easier pickings in the U.S.

Canada began its march towards an EMV world a couple years ago when those highly secure chip cards started showing up as they were in much of Europe and the rest of the

world. Mexico began its EMV rollout in 2002, albeit slowly. In the past year implementation has picked up tremendously and the country is expected to be nearly 100% EMV compliant by next year.

EMV still stands for Europay, MasterCard, Visa even though Europay International was absorbed by MasterCard in 2002 and became MasterCard's Chip Center of Excellence. Also, Japanese credit card giant JCB has joined the network. The three also make up EMVco that was formed in 1999 to manage and maintain EMV standards. Ensuring worldwide interoperability is one of its major goals. EMV also carries the nickname "chip and pin" because every card contains a chip. The card must be inserted into the reader and left there during the transaction. And, users typically must enter a pin number before the transaction can be completed.

"The whole (Canadian) marketplace expects 100 million cards to be deployed by 2010," said Jack Jania, vice president and general manager, financial services, for card provider Gemalto. The company just recently received its Interac certification to support the personalization of contact smart cards for Canada's financial community. It has also achieved ISO/IEC 27001 MasterCard and Visa certifications.

Catherine Johnston, president and CEO of ACT Canada, the country's Advanced Card Technology Association, said, "things are progressing well (with EMV migration). It's an interesting market because the financial institutions can migrate at their own pace up until 2010, so there is not a need for all to go live at the same time." The original 2010 deadline for EMV implementation was originally set by Visa and later agreed to by MasterCard, she added.

She and her organization have been talking up EMV a lot. "We want to show stakeholders how to be involved, everyone from credit unions to regulators. We're doing a consumer research piece on Canadians' use of smart card chips and applications such as EMV ... and we're finalizing a book on the payment landscape which takes into account the complexity of introducing EMV."



PIVMAN

FIPS 201

FRAC

CAC

TWIC

MAG



Handheld device
by DAP Technologies
www.daptech.com

Is he legit? Are you sure?

Your job: securing the perimeter. Individuals are streaming in to provide critical support, but you've never seen them before.

They look right, but are they legitimate? Are they trained? Should they be there?

CoreStreet's PIVMAN™ System allows you to check any government-issued FIPS 201 credential, confirm the bearer's identity, role, associated privileges or attributes, and log all activity. Anytime. Anywhere.

No network connections. No pre-enrollment. Just grab a handheld and go!

For more information, including use case overviews and datasheets, visit www.corestreet.com/PIVMAN or send a request to info@PIVMAN.com

The PIVMAN System is covered under the following DHS grant programs:

TSGP
PSGP
IBSGP
BZPP
SHSP
UASI
LETPP
MMRS
CCP
EMPG



2007 CoreStreet, Ltd. All rights reserved. CoreStreet and the CoreStreet logo are registered trademarks of CoreStreet, Ltd. The PIVMAN System and the CoreStreet Enabled logo are trademarks of CoreStreet, Ltd. All other trademarks are property of their respective owners.

174_0207



"In Canada today and as the U.S. studies this move, there is a need for strategic visionary planning at the executive level. It's not just a technology upgrade," said Ms. Johnston.

'Fraud migration' drives the Canadian move to EMV

The major force behind EMV in Canada has been the Interac Association, the country's national ABM (automated banking machine) and POS debit sale network. Fraud prevention is reason for the revamping of Canada's financial infrastructure.

"We have seen in Canada the past few years increases in debit card fraud, skimming, etc.," said Kirkland Morris, assistant vice president, strategic policy and programs for Interac. "Our decision to commit to EMV migration is in providing for long-term security. EMV reflects the best long term solution to skimming fraud."

He added: "We do see ourselves in Canada joining a global EMV migration that's gaining momentum. The risk of international fraud migration is real. We took quite seriously the risk that the fraud could migrate to North America and Canada in particular. (It is) a decision that affects both issuers and acquirers; everybody

has something to gain from that migration, and to capitalize on new product innovation."

"It boils down to a conversation about what's happening in our market," explained William Giles, vice president, emerging technology for MasterCard International's Chip Center of Excellence in Toronto. "Some issuers make a business case based on fraud or government mandates, like Malaysia, some on the telecom costs. In Canada, it's based on fraud migration. Fraud migrates from region to region and brand to brand."

"We've been working pretty hard for more than 18 months laying the technical groundwork, the technical specifications," said Mr. Morris of Interac. "EMV provides a fairly broad menu of choices as to how you'll use certain functions. We've been completing all the work we have to do as a payment network, implementing rules, upgrading equipment; laying the groundwork. We're now looking to our members on both the implementation and acquiring sides to move forward."

First Canadian trial scheduled for later this year

While EMV cards are already in use, the first

major trial of the technology won't take place until later this year in the Kitchener/Waterloo area about 90 minutes west of Toronto.

A multilateral task force created by the issuers, the major acquiring processors and the associations, has been created to, among other things, "coordinate the activities of the (Kitchener-Waterloo) launch," said Philip Andrae, a former Europay employee who runs a consulting firm in Canada aimed at helping companies reach EMV compliance. He said all major banks would be represented in the trial, including Royal Bank of Canada, Scotia Bank and Toronto Dominion. "They've done trials there before – it's reasonably close to Toronto and there isn't a lot of inbound and outbound human traffic."

A seven to eight year horizon ...

The 2010 deadline is by no means the culmination of the EMV effort in Canada. "We're looking at a time line that spans seven to eight years," said Mr. Morris.

After Dec. 31, 2012, "Interac will no longer be able to transact business" at ABM machines unless it's through an EMV card, he explains. "After Dec. 31, 2015, (this moratorium) will take effect for POS sales. These deadlines were chosen to acknowledge the substantial work required in upgrading the card payment system."

Mr. Andrae said the Canadian EMV plan stresses backward compatibility. "The terminals will be hybrid devices (capable of reading mag stripe and chip cards)." What Canada will try to avoid is what happened in the United Kingdom during the EMV rollout.

"The store clerk (in the UK) was expecting the card to have a chip. If it didn't, the clerk refused the card. After that became well known, training documents went out to all stores telling clerks that the whole world hasn't gone to a chip card yet and you'll still get regular mag stripe cards," said Mr. Andrae. "They were able to reduce the problem, but I doubt if they were able to eliminate it."

That's one reason, that consumer education is so important to card issuers. MasterCard has already "started to educate the public on the use of the cards," said Mr. Giles. "The big-

European Union EMV Compliance Progress Assessment (2006)

Country	Debit Cards	Credit Cards	POS	ATM
Austria	100%	89%	1.5%	37%
Belgium	27%	96%	80%	100%
Denmark	100%	17%	2%	100%
Finland	44%	29%	7.2%	100%
France	83%	83%	86%	98.9%
Germany	55%	10%	0.01%	4%
Greece	2.5%	6.4%	18%	17.5%
Ireland	85%	100%	100%	89%
Italy	4.3%	2%	32.2%	1.9%
Luxembourg	100%	100%	100%	94%
Netherlands	0%	30%	0.1%	30%
Portugal	0.12%	2%	25%	95%
Spain	0.8%	0.8%	31.5%	49.29%
Sweden	73%	14%	1.09%	96.4%
United Kingdom	99%	96%	94%	100%
EU15	50.4%		39.2%	55.2%

Source: European Payments Council, 2006

gest change is the introduction of the PIN. But all our customers use Interac so they're fairly accustomed to using the PIN. The U.S. market doesn't PIN as much."

Moving south to the United States ...

While the U.S. hasn't yet committed to an EMV product, what it has done is push contactless technology.

"There is a lot of interest in the Canadian market in contactless," said Mr. Morris of Interac. "We're active in exploring the contactless space (because) we see contactless technology and EMV as complementing each other over the long term. EMV really solves the security issue. When we start to look at contactless technology, you're interested in the speed of the transaction. I think we see some different business drivers behind contactless."

He said vendors are making available chips "that include both. It will be up to the acquirer or the merchant to decide what to deploy." Parking, he added, is "well-suited for contactless. It's really about finding the business drivers that would lead you to a contactless version of EMV."



... by 2012, "fraud will migrate south. If you look at 2012 when Canada reaches critical mass, that's about the time when fraud will begin to migrate to a significant degree."

Is this how the U.S. will eventually join the rest of the EMV world?

"I really do see this (EMV) as a global phenomenon; regardless whether it's in contactless form," said Mr. Morris. "I do think the U.S. will be going the chip migration route at some point."

EMV consultant Andreae says two things must happen. "Debit fraud is beginning to become an issue in the U.S. with people skimming the

password and details at ATMs. The numbers aren't big, but the rate of increase is alarming."

Second, as equipment is replaced, the new readers are likely to be EMV-compliant which erases some of the infrastructure costs which may be holding back the U.S. market, he said.

Also, with the "deployment of PayPass (and other contactless programs), the next evolution of the (EMV) card (may have) contact and contactless using the same chip. The prices for those cards are expected to drop to the \$1.50 level in the next 18 months. As contactless grows, the U.S. has the opportunity for deploying the right infrastructure over an extended period of time ... As the price of (dual interface) cards comes down to the price of the contactless card, you take away the financial burden of EMV."

He thinks that by 2012, "fraud will migrate south. If you look at 2012 when Canada reaches critical mass, that's about the time when fraud will begin to migrate to a significant degree," he added. "That's when it will begin, not when it will end."

Gemalto's Jania sees the contactless/EMV convergence scenario as about the only way EMV will come to the U.S. "If you're looking from a technology perspective; when will it come to the U.S., that will be determined by the amount of risk the financial institutions in the U.S. are willing to bear," said Mr. Jania. "In North America, the contactless deployment is well underway. Contactless will lead in North America, followed by EMV. Right now it appears convenience is driving North American products and security is driving the Canadian market; do I see those markets converging? Yes."

Regarding that convergence, he said it's "more about how you want to use the card. EMV can be used to secure online payments. Contactless is really more for payments under \$25. I can see, moving forward, a card (with both capabilities) would be very valuable."

Others are more definitive regarding an eventual U.S. migration to EMV. Matt Landrock, managing director at Cryptomathic, a Germany-based security solution provider involved with EMV migrations in Europe, said categorically that the U.S. will switch over to EMV sooner or later. "The market internationally is quite

ripe. It's like a set of dominoes. What we're seeing in Canada, it wouldn't surprise me if it doesn't spill into the U.S. since many of the providers in Canada are American companies. I'm quite confident this will begin in 2007 even if slowly."

He said there are challenges holding EMV back. "Many banks and credit card providers have been saying they don't want to upgrade their infrastructure right now (because) the costs are higher." There's also the "cultural difference. Chip cards haven't been that widely used in the states as compared to Europe. People (in Europe) are used to working with chip cards for about 10 years; whereas in the U.S. it hasn't been a thing the consumer would think about."

"They haven't gone there (to EMV) yet, but the operative word is 'yet,'" said Ms. Johnston of ACT Canada. "It's inevitable they'll go for two reasons: the richness of the opportunity exists equally for American stakeholders, so you'll want to play in that arena. Second, fraud will play a factor in two ways. Companies that have converted will ultimately want to eliminate mag stripes from their cards; so pressure will be brought to bear in terms of higher fees where mag stripes still exist and, additionally, fraud will continue to migrate to those countries which haven't gone to chip. Consumers will start to ask for it and bring pressure on issuers."

Real-time authorization works against EMV in the U.S.

But—and it's a big 'but'—even though it appears that convenience seems to trump security in the U.S., there is another more overarching reason that the U.S. may be dragging its EMV heels.

As Visa's Brian Triplett explained it, the U.S. is ahead of many other countries in "real time authorization" of credit card transactions. "We can provide in-flight real time analysis of each and every authorization of a transaction. Telecommunications capabilities (in other countries) aren't the same as in the U.S. Not all regions can support this type of real time authentication, so they were pushed to authenticating it at the terminal. That's fundamentally why some regions were pushing hard for EMV chips."

Patrick Gautier, senior vice president of New Product Development at Visa USA, emphasized this point in a prior interview with *SecureIDNews*: "The traditional driver (for EMV implementation) is fraud and the U.S. doesn't have a fraud problem. So the reason to go to chip here are different and centered around differentiation and value add services. Fraud in the U.S. is just 5 cents per \$100 spent. That is a historic low at a time when usage is expanding. The reason is that we have great authorization systems that make use of information and customer data to combat fraud."

In the same interview, he reiterated what Mr. Triplett said: "The U.S. telecom infrastructure is cost-effective and expansive to the point that over 99.5% of transactions are authorized. And it is only getting better. With DSL at the point of sale ... we have achieved round-trip authorization times of 1.4 seconds in the United States."

But while fraud levels in the U.S. may be acceptable today, an EMV-protected world could leave the country as an unprotected island.

Fraud migration is real, not just anecdotal, said Dr. Toni Merschen, head of MasterCard International's Chip Center of Excellence in Waterloo, Belgium. "Malaysia migrated to EMV in a very short period of time because fraud was going through the roof. It proved that EMV works because fraud was reduced by more than 90%. However, neighboring countries like Thailand and Indonesia took the hits. We're seeing increased (fraud) activity there. So, fraud migration is real. We've seen it in other regions."

While he can't say when, or if, the U.S. will become EMV-compliant, he does see fraud migrating there from other regions, "When the rest of the world has migrated to EMV."

Right now, real time online credit card authorizations are keeping fraud low in the U.S. But, he added, crooks are becoming more savvy in their use of stolen cards. Banks can usually shut down a card once it detects supposedly fraudulent transactions after the card is used two or three times. But of late, it appears that "stolen or compromised cards are being used just once. They (the crooks) make a big enough hit one time, then walk away," he said.

Another scenario, explained Dr. Merschen, is that a bank's high-end users are usually the ones who frequently travel abroad. If they start experiencing problems with their mag stripe cards being accepted overseas, as happened in the U.K. case, a bank may decide to issue chip cards to those customers.



Could contactless be the driver for EMV in the U.S.?

Another EMV-foot-in-the-door scenario is possible now with a convergence between contactless and EMV. But any change to the U.S. payment infrastructure takes time due the sheer mass of cards and terminals.

"The U.S. has about 1 billion payment cards in circulation," said Mr. Gautier. "5.6 million merchants accept Visa payments and over 13 million POS terminals are deployed. Compare this to the U.K., which has just 70 million cards in market and took over 10 years to make the transition to EMV."

"We see the EMV chip and other chip programs like contactless and NFC (near field communication) to have interoperability," said Mr. Triplett of Visa. "We're working on that right now. When we first launched contactless, we did it for local programs for small dollar transactions. Given the success and adoption of contactless, even in markets that have implemented EMV, we have adopted a global standard for contactless and EMV cards. At that

level, we're taking both the speed and convenience to the next generation level of performance and security. By doing that, we're not going to the lowest common denominator (which is, everything working from the same basic infrastructure)."

Will there be an EMV card in the U.S.? "I can't answer that, but the contactless chip will be EMV-compliant," said Mr. Triplett.

Contactless/EMV convergence is a reality today, Dr. Merschen agreed. "We've developed an EMV-based contactless card in Europe for PayPass and this is something that could make its way into the U.S."

Unlike in the U.S., where the card is online authorized, "the authorization is taken over by the chip in an offline mode. That opens up offline scenarios like parking meters and vending stations in a more secure way. These cards are interoperable, so the U.S. PayPass card will work in the contactless (mode)," said Dr. Merschen.

"There is still a cost associated with migrating a huge market like the U.S. But if you look at the trend on the cost side, it's going the right way. Card costs have come down dramatically and (some) readers installed in the U.S. already have the chip reading hardware integrated," said Dr. Merschen.

"A couple years ago, (banks and acquirers) didn't know how to spell chip or EMV. But they've had to implement EMV now. They had to support chips in Europe and Asia specifically. Even if it is not on the same system platform, they have the knowledge and experience to do it," he added.

As to a full-fledged EMV implementation in the U.S., Dr. Merschen said it is strictly "a business decision to be made by U.S. banks. They're not sleeping. They're looking at all the various aspects and will make a decision when they feel it's time."

Added Ms. Johnston, ACT Canada: "Sometimes, it (EMV migration) is very straightforward. For others it can be very complex. But it offers rich opportunities for stakeholders if they understand their options."

HSPD-12

in one neat package.

ISC West
Booth 15087

[We know the requirements.
So does our software.]

IdentityDefender, a new identity management product suite from Lenel, was built from the ground up to be in total compliance with all FIPS 201 requirements. Using a single streamlined interface, IdentityDefender performs all PIV I and PIV II processes with an emphasis on data integrity and security.

The modular IdentityDefender suite includes the IdentityDirector IDMS, the IdentityCollector enrollment system, the IdentityProducer card production system, the IdentityActivator card issuance system, and the IdentityEnforcer logical access solution.

Each module can seamlessly integrate into an organization's existing infrastructure, such as a human resources or physical access control system. Best of all, IdentityDefender can be purchased as either a complete end-to-end HSPD-12 solution, or piece by piece to fit within any ongoing implementation.

Check out the complete IdentityDefender® suite at www.lenel.com

Access Control • Digital Video Surveillance & Recording • Identity Management
Integrated Alarm Management • Smart Card & Biometrics • Logical Security
Enterprise Architecture • Intelligent Video • Visitor Management • APIs & Integration Tools
Building Automation • Intrusion Detection • Fire Alarm Integration • Asset Management



GSA supports PIV card issuance for 40 agencies, seeks new vendor for managed services

Chris Corum

Executive Editor, AVISIAN Publications

The Government Services Administration (GSA) was instrumental in the federal agencies' successful compliance with last year's October 27 deadline for PIV card issuance. That is because the GSA's HSPD-12 Managed Services Office (MSO) actually issued the cards for 39 contracted agencies. It is outsourcing at the federal level—agencies heads not wishing to handle their card issuance and HSPD-12 compliance internally can hire an outside entity to do it for them. And that is precisely what the MSO is there for.

"We (now) have 40 customer agencies on board and we have a current user count of 420,000," said Steve Duncan, GSA.

Back in August 2006, GSA awarded a contract to BearingPoint to service the MSO in its efforts to provide PIV card planning, enrollment, issuance, and service to agency clients. The option to continue the contract, however, was not exercised when it came up for review on January 7.

"We made an initial procurement of cards back in August ... for our 39 client agencies," explained Mr. Duncan. "We decided not to exercise the option for that procurement (but rather) to do another one." (Lockheed Martin, EDS, and Xtec had filed protest against the BearingPoint award with the Government Accountability Office but it became moot when the MSO decided to voluntarily end the contract.)

The new request for quotation (RFQ) was released on January 12. "We have defined 141 requirements ... and 61 are critical, and the vendors are going to have to show them to us in an operational capabilities demonstration. These demonstrations will begin two weeks after the February 2 due date for price proposals.

This demonstration will be no small task for the selected vendor. It will require a virtually complete HSPD-12 environment including sponsorship, enrollment, adjudication, issuance, activation, and credential use. Mr. Duncan adds, "the card they give us prior to award will go through the GSA test lab to make sure it passes all the (tests) that NIST provided."

There are 18 companies listed on Schedule 70 SIN 132-62, the GSA approved list from which the winning bidder must come. These companies include: Accenture LLP, Accenture National Security Service, ADT, Anteon, BearingPoint, Centech Group, Communications Resource (CRI), CondorTech Services, EDS, ElectroSoft, Jacob & Sundstrom, Lockheed Martin, Maximus, Open System Sciences of Virginia, Operational Research Consultants, Probaris Technologies, SI International, and XTEC.

Issuance is key

The MSO will begin deploying issuance stations in Washington D.C.—two stations per week for four weeks. The national rollout will eventually result in 225 enrollment stations across the country—200 fixed stations and 25 mobile stations.

"We use a centralized printing approach," says Mr. Duncan, "so we are looking for someone who really understands pre-issuance and post-issuance security."

With a significant percentage of agencies relying on this single source for PIV cards and services, this is an understatement.



**Take 30 seconds and sign-up
for a free subscription to this magazine
[turn page for details]**



FREE SUBSCRIPTION

The following questions must be answered to complete your subscription.

My job title is:

- ☐ CEO/President ☐ EVP/VP
☐ Director ☐ Manager
☐ Other _____

My primary job function is:

- ☐ Management
☐ Sales/marketing
☐ Operations/development
☐ Administration

My relationship to ID technology is:

- ☐ End user ☐ Manufacturer
☐ Reseller ☐ Consultant
☐ Solution Provider/Integrator
☐ Other _____

My primary market focus is:

- ☐ Government ☐ Corporate
☐ Financial ☐ Transportation
☐ Education ☐ Retail
☐ Other _____

My primary application focus is:

- ☐ Physical security ☐ Computer security
☐ Payments ☐ Transit
☐ ID issuance ☐ Logistics
☐ Other _____

Number of employees in company:

- ☐ Under 25 ☐ 25 to 99
☐ 100 to 499 ☐ 500 to 999
☐ 1000 to 4999 ☐ 5000 to 9999
☐ More than 10,000

Annual sales volume:

- ☐ Under \$1 million ☐ \$1-10 million
☐ \$1-25 million ☐ \$25-100 million
☐ More than \$100 million

In the next 24 months, I expect to be involved in a decision to purchase:

- ☐ Physical security products
☐ Logical/computer security products
☐ Biometric products
☐ ID issuance hardware and/or software
☐ Smart cards (contact or contactless)
☐ RFID systems/components

Subscribe for FREE to Regarding ID magazine and keep up-to-date with the latest news and insight from the world of identity management, biometric, and advanced ID technology. (Free subscriptions available to U.S. addresses only. *International subscribers pay US\$45 per year to cover postage and handling costs.)

FAX this form to 850-222-4477
or subscribe ONLINE at www.RegardingID.com/subscribe

- ☐ Please send me/continue to send me Regarding ID magazine FREE.
☐ My address has changed. Please send Regarding ID to this address instead.

Name _____

Job title _____

Company _____

Address _____

City _____

State/Province _____ Zip/Postal Code _____

Country: ☐ U.S. (FREE) ☐ *Other (U.S.\$45) _____

Phone _____

Email _____

Signature _____ Date _____

* Non-U.S. subscribers: Fax this form and we will send you an invoice for US\$45 to the Email address you provide. Your subscription will begin when payment is received. To begin immediately, visit www.RegardingID.com/subscribe.

I would also like to receive a FREE subscription to the following AVISIAN online publications sent to my email address (check all that apply):

- ☐ SecureIDNews ☐ ContactlessNews ☐ CR80News ☐ RFIDNews

FAX this form to 850-222-4477
or subscribe ONLINE at www.RegardingID.com/subscribe

Have a colleague that would like to receive Regarding ID for free as well?
Send them a link to RegardingID.com/subscribe

Authentication for financial services is a global goal with regional approaches

Jose Diaz, US director of technical and strategic business development, Thales e-Security, and
Nesic Dragoljub, UK head of professional services, Thales e-Security

The current needs and demands for authentication and identity management show huge variations around the world. One thing that is common across all regions, however, is the ever-increasing requirement to prove that you are who you say you are in the face of rising security threats, such as fraud and phishing. According to CIFAS, the UK's Fraud Prevention Service, the number of victims of identity theft was up by 19.91% (at 67,406) compared to 2005. To combat this crime and secure against wider identity theft threats, there are several technologies that strengthen authentication security, some of which have already been deployed and are showing signs of success in the fight against fraud.

Perhaps one of the most successful schemes to date is the UK's Chip and PIN initiative which uses the EMV standard to secure cardholder-present transactions. Almost a year on from its mandatory introduction, APACS, the UK

payments association, reported that thanks to Chip and PIN, there was a reduction of nearly £60 million in counterfeit and fraud on lost and stolen cards in 2005 compared to 2004 (a drop of 24%). To date, two-factor authentication is only implemented for face-to-face transactions and there is still much progress to be made securing cardholder-not-present banking and transaction channels in the UK.

Contrary to the compulsory approach the UK has taken, the US is regarded to have responded with a softer solution that is aligned to customer demand. Currently, introduction of EMV cards is only being considered for international customers who are finding it increasingly difficult to make payments in countries like the UK that require a secondary factor, over and above magstripe and signature authentication. Strengthening Internet transactions, on the other hand, has become a priority in the US and in 2005, the Federal Financial Institutions Examination Council (FFIEC) issued guidance stating that US banks should undertake a risk-based assessment of the processes in place to manage and authenticate identities by the end of 2006. Following FFIEC concerns that single-factor authentication was no longer sufficient, banks must satisfy the FFIEC that the security adequately protects customers, not only on their Internet banking but also telephone banking channel.

A further example of the diverse approaches to security can be found in the Far East and Eastern Europe, where banks are incorporating mobile authentication into online transaction security. Mobile communication via SMS is highly popular in these regions and is therefore considered an extremely viable option for securing online transactions.

Taking a snapshot of the current identity management marketplace, it is clear that there is no one accepted standard of strong authentication. Rather, there are a variety of different approaches implemented by financial bodies around the world, each with their own pros

Perhaps one of the most successful schemes to date is the UK's Chip and PIN initiative which uses the EMV standard to secure cardholder-present transactions.



and cons. In this current climate of identity theft, how will emerging challenges in 2007 threaten the efforts and current technologies in place to combat identity crimes, and how can the industry respond?

The trend for conducting online transactions around the world is unrelenting, proving consumers are not yet deterred by the risks associated with Internet banking. Whilst the direct cost of fraud for banks is not great enough to justify the cost of investing in the technology required to combat it, banks also need to protect themselves against the knock-on effects of this crime, such as damage to brand, reputation and customer satisfaction. Loss of confidence would also result in customers reverting to more expensive means to conduct business, such as through the branch or writing cheques. These factors will prove to be an important driving force for the adoption of two-factor authentication by banks in 2007.

... in the Far East and Eastern Europe ... mobile communication via SMS is highly popular and is considered an extremely viable option for securing online transactions.



In addition to concerns related to brand equity, 2007 will also see legislation driving banks' identity management solutions. In the Far East, governments already have or are currently introducing legislation to force banks to provide strong, two-factor authentication to their customers – Thailand, India and Hong Kong are good examples. Elsewhere, regulation could force banks to consider the need to address the security levels they currently have in place.

The faster payments initiative in the UK is one such example and could prove to be the tipping point for mass roll-out of two-factor authentication the industry requires. Due to come into force in the UK in November 2007, faster payments has been designed to speed up the processing of low value, person-to-person transactions, from the current three-day period to same-day transactions. This near real-time transaction processing approach by banks is aimed at improving customer satisfaction and acknowledges the growing use of alternative payment channels such as the Internet and telephone. However, this will pose severe challenges to banks' authentication techniques. Put simply, banks' current risk modeling systems are not up to the challenge of receiving a payment instruction from a variety of different channels and strongly au-

... the trend in the US is to supplement Internet transactions with layered security, as opposed to the more expensive solution such as a smart card reader or another challenge-response token.



thenticating that person within the 15-second transaction processing time limit that faster payments will enable.

The solid business case for investing in two-factor authentication that faster payments has provided is an unexpected knock-on effect of the initiative. While always generally supportive of the benefits two-factor authentication can bring, especially in the battle to fight cardholder-not-present fraud, banks have lacked any immediate incentive until now. Faster payments fundamentally changes this as when it goes live in the UK in November 2007, the member banks will be instantly vulnerable.

Banks in the US are also faced with the security implications of new legislation. The risk assessments imposed by the FFIEC will mean that banks face a number of compliance checks in 2007, subsequent to the December 2006 deadline. The FFIEC will need to establish whether banks have correlated the risk of certain transaction types with the security they require to conduct them.

Akin to the majority of the world's regulatory bodies, the FFIEC has not pinpointed how stronger security must be achieved for Internet and telephone banking, citing two-factor authentication as just one of several possibilities. Combining this flexible approach with US consumers' desire for simple, convenient banking, the current trend in the US is to supplement Internet and telephone-based transactions with layered security, as opposed to the more expensive solution of hardware such as a smart card reader or another challenge-response token. Layered security is achieved through answering pre-registered personal questions. This can also be complemented with behaviour-orientated security, such as banks authorising only one IP address to prove the transaction is originating from your personal computer.

By using methods that require customers to submit additional personal data to banks, as opposed to issuing hardware such as smart card readers, banks are increasing their duty to safeguard and protect this information from fraudulent use. Management of risk is driving the process to strongly authenticate, yet ironically the introduction of layered security poses a greater threat to risk models, particularly concerning internal fraud. 2007 will witness US banks' close adherence to the PCI

(Payment Card Industry) standards for data security and will require them to carefully examine their internal information management infrastructure to insure this highly confidential information is sufficiently protected.

... starting Nov. 2007, the UK's faster payments initiative is designed to speed up the processing of low value, person-to-person transactions, from the current three-days to same-day transactions.



The reluctance of banks in the US to issue security hardware to their customer is not only a cost consideration. The trend the world over is for simple and accessible banking, and this is particularly acute in North America. Current consumer demand for quick and easy payments is clear from the success of contactless card uptake across the continent. In the same way banks yielded to this consumer pressure, they do not wish to burden their customers with a physical item that must be present as well as their bank card to make a payment, yet they are acutely aware of the risk that must be managed.

One option for the North American market that may show promise in 2007 is the use of mobile phones as an authenticating device, as seen in the Far East and Europe. There are features that make it an attractive option for banks as well as convenient for consumers including its ubiquitous use and penetration in the market, convenient handling and zero distribution costs. SIM cards are the largest appli-

cation of smart card technology in the world so there is value for banks in harnessing their growing processing power to perform other tasks such as identity authentication. There are many trials currently being undertaken in the US that could lead to the implementation of such solutions in the near future. A barrier to the adoption of this technology to date has been the need to foster partnerships across the banking and telecom sectors. However, with mounting pressure to address heightened security in a straight-forward manner, mobile authentication has the right criteria to satisfy both banks and consumers in the near future.

Contrary to the US, the success of EMV in the UK has resulted in positive consumer opinion towards smart card readers and the concept of utilising a token to authenticate payments. As industry chatter about two-factor authentication continues to build momentum this year, providing each customer with a smart

card reader is an avenue that is proving to be popular. With the support of APACS, 2007 will see the highest commitment from banks to providing their customers with two-factor authentication. Barclays appears to be leading its competitors by stating it will begin to offer on-line banking customers handheld card readers this year. As these trials proliferate in the UK, it is likely that a wave of implementation will emerge as banks strive to at least keep up with their peers.

Although the banking industry the world over is facing the same challenges, the marked differences in approach prove as strong as ever before. The demands made on identity management solutions will continue to rise in line with the problems that are driving banks to seek stronger authentication, ultimately forcing banks to deliver more secure systems that protect consumers across all banking channels.

SIM cards are the largest application of smart card technology in the world, so there is value for banks in harnessing their growing processing power to perform other tasks such as identity authentication.



Because We All Need Recognition



DOUBLE YOU



tattoo



PEBBLE



dualys



SECURIION



QUANTUM

Evolis printers:
A complete range for card personalization



evolis
printer innovator

www.evolis.com

evolisinc@evolis.com

Pentagon deploys handheld computers to validate FIPS 201 IDs

PIVMAN solution from CoreStreet to authenticate cardholders at key Department of Defense locations in Washington, D.C. area

Security at the Pentagon is in the capable hands of the Pentagon Force Protection Agency (PFPA) but now there is something else in their capable hands ... CoreStreet's PIVMAN. The PFPA officers will use the handheld identity verification units to authenticate individuals via their FIPS 201 compliant ID cards.

"The first order was for 90,000 privileges under management and 100 (handheld) units," said Chris Broderick, CoreStreet CEO. "This represents the largest transaction to date and the first flagship installation."

The solution will be used to secure access to Pentagon grounds as well as some of the leased grounds controlled by the Department of Defense in the National Capital Region. "We have been working collaboratively with the Department of Homeland Security's (DHS) National Capital Region throughout development of the product," adds Mr. Broderick.

The PIVMAN solution consists of three main components:

- A handheld device: The unit purchased by the PFPA is a ruggedized handheld manufactured for CoreStreet by DAP.
- Device software: The software powering the handheld enables secure reading of data on PIV credential, biometric capture and verification, as well as revocation checking.
- Backend software: The backend system monitors the FIPS 201 revocation lists and consolidates data for upload to the handhelds. It also collects privilege data from various data sources and ties that to the credential.

The Pentagon deployment is not the first for the PIVMAN. The system is in use with the City of Los Angeles, in pilot deployment in the state of Maryland, and other pilot locations as well.

"We have seen a significant uptick in the first responder community," says Mr. Broderick. "The issuance has accelerated in local governments

and it is increasing the number of municipalities that can become PIVMAN customers."

At CoreStreet, hopes are high that many of these municipalities will elect to utilize the PIVMAN solution. Such hopes are empowered by the fact that under the DHS Grants Management Program, state and local governments are eligible for reimbursements for the system, suggests Mr. Broderick.

An alternative to the GSA's Approved Products List?

The PIVMAN, like many applications that have and will emerge to capitalize on the PIV credentials, is not on the frequently referenced GSA Approved Product List. Yet this does not mean it shouldn't be used. Rather, it means it did not fit into a defined category for evaluation by GSA.

According to the GSA FAQ: "The list created represents the technical data that has been defined. If a product doesn't have a category, GSA felt that there wasn't enough information to support that category. However, this doesn't mean that agencies cannot purchase that specific product. It means that the agency has to determine how to make that product meet the HSPD-12 goals."

It is this broader schedule of products, applications, and services where you will find the PIVMAN solution. According to Mr. Broderick, "PIVMAN is the only compliant system for this use case in the First Responder Community."

This "other" list is called SIN 132-62: HSPD-12 Product and Service Components and it is where you will find the PIVMAN and many other products related to HSPD-12.

The government's IDManagement.gov site describes 132-62 as follows:

"(It) is established for products and services to implement the requirements of HSPD-12, FIPS

201 and associated NIST special publications. Qualification requirements are established for the following HSPD-12 system components and categories on SIN 132-62:

1. PIV Enrollment and Registration Services and Products
2. PIV Systems Infrastructure Services and Products
3. PIV Card Management and Production Services and Products
4. PIV Card Activation and Finalization Services and Products
5. PIV System Integration Services and Products

About the PFPA

The PFPA was created in the wake of the 9-11 attacks to provide law enforcement and force protection for the Pentagon and other DoD building and facilities within the National Capital Region. And now it has 100 new agents on its team—more accurately 100 new PIVMEN—to help in this important mission.



ID Solutions

LOGICAL ACCESS CONTROL

PHYSICAL ACCESS CONTROL

ALL FIPS 201 COMPLIANT

MINEX CERTIFIED MATCH-ON-CARD

FIPS 201 DUAL INTERFACE CARDS



Biometrics in Action

MA120 PIV

MS0350 PIV

MA220 PIV

RapID

Outdoor MA

For more information: info@morpho.com
1.800.326.2674
www.morpho.com

 **Sagem Morpho Inc.**
SAFRAN Group

Imaging Corner

Sponsored by:

FARGO

Tracking misprints and bad cards can be as important as tracking good ones

Keeping track of the bad cards—those that were printed but never issued—is just as important as tracking the good cards when managing your ID card system.

For John Ekers, Fargo Electronics' director of product marketing for software and services, it has become something of an evangelization issue.

"One of the things we've been trying to promote, which comes from working with security bureaus, is that it's not just about your cards, but about your duplicates as well, your bad cards and how you are managing those," said Mr. Ekers.

"...particularly in the ID market with desktop printers, you see a huge gap. No one is managing the bad cards, the ones that had to be remade," he stresses. "Not many have software in place to tell you we made four copies of Jane's ID badge and the fifth is what we sent out."

What's needed is something that will help organizations to do a reconciliation to match bad cards against the inventory and produce an audit trail. "The bad cards don't necessarily have to be kept on file, but a supervisor needs to look at them, check them off (that they actually reviewed them) and then the cards can be destroyed," said Mr. Ekers.

It's all about hardening your security. The card may not have been encoded yet, but the picture is still there, the name is on the card and it could still be used fraudulently.

Fargo and others have tools that can secure the issuance process. "We're trying to manage the issuance of both good cards and bad cards," explained Mr. Ekers.

A presentation at a National Association of Campus Card Users (NACCU) conference on the issuance process ended, "with most of (the

40 college attendees) wanting to get back to their offices as soon as possible," said Mr. Ekers. "These were people who initially felt their offices were pretty secure," he said. "You need to know who has access to your card issuance system. Can someone come in over the weekend and produce fraudulent cards? And what is your liability if that happens? Fear drives a lot of this."

If you're providing a system to manage access, but you're not managing the security of the issuance process, you could still be liable for any breakdown that occurs, he said. For example, someone could print out a fraudulent card that allows him to gain access to a secure building.

One preventative measure organizations can take is to utilize a tool that can lock down their printers. "If you have an application running on your PC, the only way the printer will work is if you present the printer password. That's more widely accepted in the education market. In a lot of cases," said Mr. Ekers, "you have students doing the badging process. At least over the weekend no one can come in and access the printer."

Complementing that system, he added, would be a notification application. "An individual who comes in over the weekend who wanted to print badges and if the printer wasn't locked up, the printer would send out a message over the network or cell phone and let the manager know that someone is trying to print something," said Mr. Ekers.

Another possible security gap is the data itself that's used to print the badges. "We recommend that you don't maintain that data any longer than you need it. If you look at Visa or MasterCard, they're not allowed to maintain account information for more than seven days. You don't have to maintain a local database," said Mr. Ekers.

Computer advancements have also led to more security holes. The simple USB port provides quick access to data on the computer. "A lot of corporations are not buying computers with USB ports," he said.

Even if you don't have the means to implement a sophisticated issuance security and card inventory system, "you can at least have an Excel spreadsheet where you log in the number of cards, cards you've printed, and so forth," said Mr. Ekers. "You really need to manage that inventory." Or, you could go low-tech with a simple pencil and paper method, he added.

"So many colleges today seem to be overwhelmed with operational requirements. Historically, they've let a lot of these things go just to get the cards out the door. But I think they're starting to understand that there's a lot more at stake," said Mr. Ekers.





27 countries
60 million citizens per year
50 years of service
One universal feeling: **Trust**

Governments around the world trust Digimarc to provide them with the secure ID solutions they need to deter counterfeiting, enhance traffic safety and national security, protect their citizens from identity theft and fraud, and facilitate the effectiveness of voter ID programs. Custom solutions. Proven, tested products. Standard technology platforms.

From expert project management to the hardware, software, system integration, installation and ongoing support you need to ensure reliable ID issuance systems, Digimarc is the internationally trusted solution.

DIGIMARC



Modular approach enables Lenel IdentityDefender to meet HSPD-12 needs of large and small organizations

In 2004, a significant challenge faced the physical security industry. An important government directive was signed by President George W. Bush requiring all government agencies to comply with a strict identification standard. That mandate, HSPD-12, required the use of smart card technologies that were still under development.

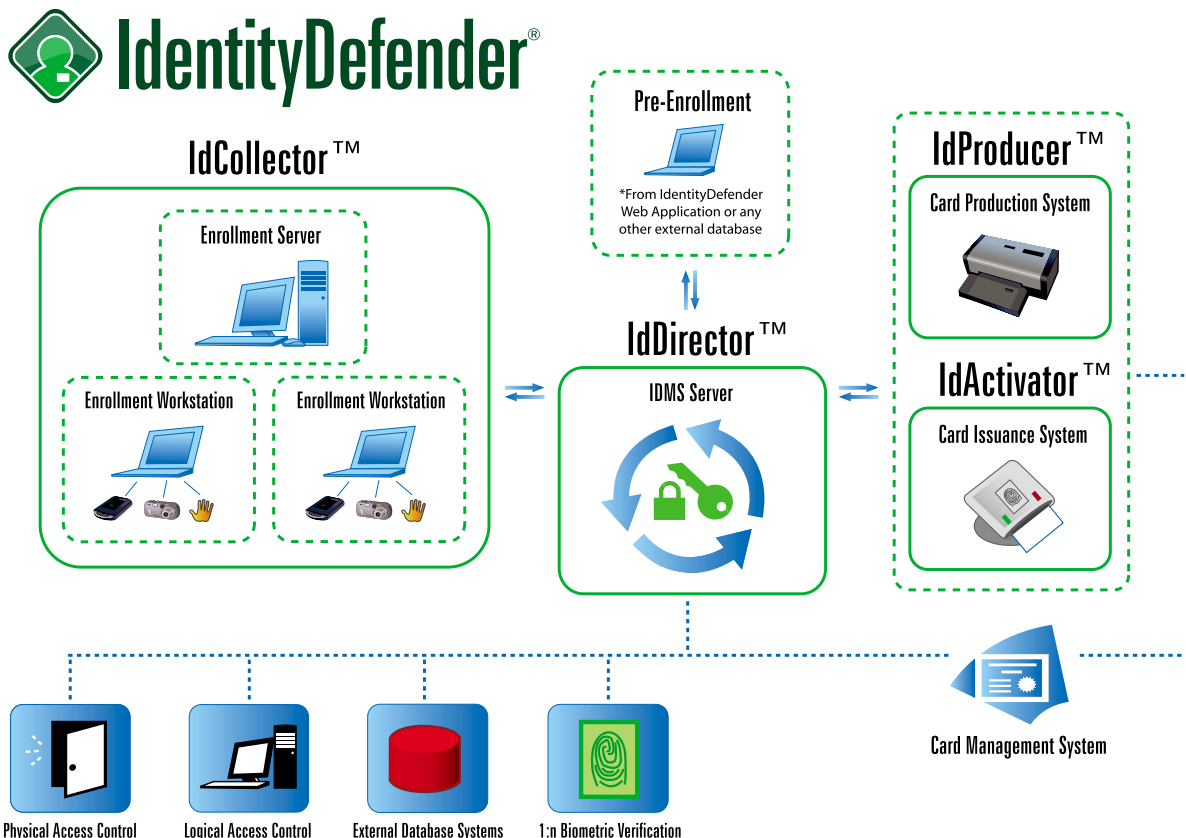
As significant as the challenge was for hardware manufacturers, software designers faced an even greater struggle. They had little upon which to build their solutions, especially considering that such software is usually shaped by the hardware with which it interfaces. The team of engineers and product managers at Lenel Systems International met the challenge head-on, working despite the lack of hardware reference points. Two years later, Lenel released IdentityDefender, an innovative software solution to achieve the government's HSPD-12 directive.

"The HSPD-12 marketplace created extensive opportunities for the smart card industry to push its standards of security and innovation farther than ever before. With a strong set of very specific security requirements in place, organizations gained concrete development reference points to build upon," said Randy Vanderhoof, executive director of the Smart Card Alliance.

But these reference points were a work in progress. Most agree that developing software solutions is challenging when all variables are defined, but when key elements (e.g. cards, readers, data formats) remain in flux, it can be daunting. With the IdentityDefender software relying so heavily on the progress of the smart card hardware that HSPD-12 requires, Lenel found itself in an interesting position. As the release timeline was announced, it became clear that the software development would have to press forward in spite of the lag in development of industry technologies.

Lenel relentlessly studied HSPD-12 requirements to create a vision of what a total software and hardware solution would encompass. From the beginning, this vision included four essential components:

- A dedicated identity management database to securely route all data through each product module: the IdCollector enrollment system, the IdProducer production system, and the IdActivator issuance system
- A web-based architecture to ensure total flexibility of the product
- Partnerships with vendors of key system components required for HSPD-12 compliance
- A product designed with strict adherence to HSPD-12 requirements, yet flexible enough for both government and commercial applications



The product architecture gives IdentityDefender the flexibility to adapt to any changes in HSPD-12 requirements. Key partners in the government market quickly recognized Lenel's achievements in the identity space.

"We have passed the rigorous testing process applied by the General Services Administration to be listed on the GSA Approved Product List," said Paul Russell, marketing and government program relations for Lenel. As a result, he added, government and commercial entities have already begun pilot programs for the software.

Building on the success of prior solutions

"We introduced several different foundational elements in both the security and infrastructure of IdentityDefender," said Erik Larsen, Lenel's product manager of identity solutions. "We created IdentityDefender using the same open architecture development philosophy that has been a hallmark of OnGuard, our physical access control system." OnGuard was first released by Lenel 12 years ago, and now has an installed base of around 13,000 systems worldwide.

IdentityDefender is the first totally new product line Lenel has developed outside of the OnGuard brand. This not only expands the company's presence in the physical access control and government markets, it also allows Lenel to enter both the logical access control and "physical/logical convergence" markets with a proven platform.

Modular, flexible design fits both government and commercial demands for converged solutions

"A series of checks and balances is built into each component to ensure that the first and foremost concern is a secure workflow," said Patrick Rodwell, marketing and government program analyst for Lenel. "A truly intelligent identity solution must create a smart card ID that is fully utilized in both the physical and logical security environments."

"The workflow is provided through templates that are fully-configurable around FIPS 201 and the requirements of the government agency," Mr. Rodwell added. "The selected template will dictate the workflow of the other modules." Because of this modular approach,

IdentityDefender is designed to integrate into any existing infrastructure, whether it's a small, basic configuration or a large-scale enterprise installation.

"IdentityDefender delivers all capabilities required for a turnkey system," Mr. Rodwell said. Each IdentityDefender module is a self-contained application that meets a very specific need in an identity management implementation. "So whether an organization needs to create a system from the ground up, or requires only a few pieces of the puzzle, IdentityDefender can help the customer achieve a total identity management solution."

"We've had an overwhelmingly positive reaction to IdentityDefender," concludes Erik Larsen. "Although we developed it as a workflow solution based on FIPS 201, the product has emerged not only as a one-stop HSPD-12 solution, but also as a complete, commercially-viable entity all its own."



"We have passed the rigorous testing process applied by the General Services Administration to be listed on the GSA Approved Product List."

— Paul Russell

*Marketing and government program relations,
Lenel*



"We introduced several different foundational elements in both the security and infrastructure of IdentityDefender."

— Erik Larsen

*Product manager of identity solutions,
Lenel*



"A truly intelligent identity solution must create a smart card ID that is fully utilized in both the physical and logical security environments."

— Patrick Rodwell

*Marketing and government program analyst,
Lenel*

States prepare for Real ID in advance of pending driver license mandates

Central and distributed issuance options, facial recognition, and secure ID management has led 32 states to solutions from Digimarc

Andy Williams

Contributing Editor, AVISIAN Publications

With Real ID Act regulations lurking somewhere around the corner, secure ID management provider, Digimarc, is well-positioned to help states comply with the new requirements. The fact that the Oregon-based company is already in more than two-thirds of U.S. state driver license offices certainly gives it a leg up as well.

"We're in 32 U.S. driver license programs, five Canadian provinces and Mexico with its voter ID project," said Scott Carr, Digimarc's executive vice president.



Since the Real ID Act is supposed to standardize driver licenses from state to state, it's no surprise that Digimarc has been heavily involved in Washington, D.C., as well. "We've spent a lot of time working with our states in helping them understand the law and anticipating what's required," said Mr. Carr. "We've also been called on to testify to a U.S. Senate committee about border crossings and security."

The Real ID Act of 2005, which passed Congress in May of that year, prohibits federal agencies (and airlines) from accepting state-issued driver licenses or identification cards unless they meet minimum security requirements – such as including common machine-readable technology and certain anti-fraud security features. It also requires verification of information presented by the license applicant, who must also supply evidence that he is a citizen or a legal immigrant. The act requires standardized driver licenses by May 11, 2008.

One of Digimarc's assets is its facial recognition software which guards against a state issuing a duplicate license and also verifies the person renewing his license.

Many states are implementing software that concentrates on facial characteristics that can help them weed out duplicate—and possibly fraudulently produced—licenses. Regardless of what Real ID may mandate, states now are trying to better secure the license issuance process, said Mr. Carr.

Securing the license issuance process with facial recognition

When Digimarc sets up a facial recognition process in a driver license office, the company delivers "a high quality camera that makes for a better driver license and provides for more effective facial recognition. We'll deliver the computers and cameras and everything else that's needed. From an operator's perspective there is no impact."

This is how Digimarc's facial recognition software works: "First," explained Mr. Carr, "if I'm going back in to renew my driver license and you take my picture, the clerk can pull up my prior picture and do a one-to-one comparison to make sure I am me. This happens in the office and is just a way of confirming my identity."

Next up in the facial recognition process is to make sure that person doesn't have another driver license under another name. "Instead of checking against your previous photo, I check it against every face in my database," said Mr. Carr. That's more prevalent with states doing a central issuance, where the license is produced in a factory, then mailed to the recipient. "There's a two-day delay and I can use that time to do that check." About a dozen states centrally-issue their licenses and Digimarc handles all of them except New York.

This "one-to-many" check could also produce several matches. If that happens, "I probably want an investigator to make a judgment on whether a possible fraud is involved," said Mr. Carr. "Investigators love the software because they can do things now in six hours that used to take months."

Central vs. distributed issuance: Each poses unique challenges for Real ID

He cites Kansas as an example of the central issuance model. "I go through the enrollment process and give them all my (identity) information. They take my picture and when I leave the office, I have a temporary license. Overnight, they run a one-to-many comparison and an investigator gets a list of all potential fraud cases. The valid ones are sent to a secure factory, which we operate, the license is produced and mailed."

Added Mr. Carr: "It will be easier to implement a Real ID workflow in a central issuance model particularly if the Department of Homeland Security regulations require a whole host of data checks and other security procedures."

In the last five years, a number of states have moved towards a central issuance process, said Mr. Carr. A new system costs the state money, "but it reduces fraud so there's a quick pay back," he added.

The downside, obviously, is that it sacrifices convenience. Digimarc has five central issuance factories at undisclosed locations in North America. At these driver license factories, all employees have background checks and production processes are managed.

"It's hard to do that when you're issuing driver licenses over the counter," said Mr. Carr. "But a number of states continue to use over-the-counter." Digimarc is the only vendor, he added, that offers both over-the-counter and central issuance processes. "It is up to the customer to decide which workflow to choose and it is our job to make them successful."

Progress in advance of Real ID

Many states are "innovating in advance of Real ID. We're finding improvements in the security of the driver license itself such as extended data verification steps" where the information

itself is checked to verify identity, added Mr. Carr.

So, states aren't slowing down in their attempts to harden driver license security. But they would like to know what will be required under Real ID, particularly since they must implement the act 15 months from now.

The National Council of State Legislatures even has a web site counting down, by second, the time left that states have to implement Real ID. The organization, in a survey of its members, estimated it would cost about \$11 billion to meet Real ID regulations over the next five years. Most of that cost will come if states have to reissue every license. The survey was based on the law itself, not DHS regulations which haven't been issued yet.

Real ID remains controversial. Proposed legislation to repeal the Real ID Act is very much alive. Sen. Daniel Akaka, D-Hawaii, and Sen. John Sununu, R-New Hampshire, want more privacy protections and lower state costs. While the bill was introduced during last year's congressional term, it's likely it will again be taken up during the 110th Congress.

"We've been involved with regulations associated with driver licenses for many years. Our solutions have been designed to anticipate Real ID and to help our customers get compliant," said Mr. Carr.

But even before Real ID becomes a reality, states along the Canadian or Mexican borders, must deal with PASS (People Access Security Service). This proposed card is designed to meet the Western Hemisphere Travel Initiative (WHTI) requirements, which mandates that by Jan. 1, 2008, anyone entering the United States, including U.S. citizens, have travel documents that prove their identity and citizenship. Canadians claim the PASS card would severely hinder their country's commerce, particularly tourism, making it more difficult for Americans to visit Canada and vice versa.

"We are involved in the PASS card because a few states are trying to determine how to intersect Real ID with PASS," said Mr. Carr.

PASS? Real ID? Merging a more secure driver license with the two? It's enough to give state driver license administrators heartburn ... and enough to keep Digimarc very, very busy.

Trust in more than 50 successfully handled ID projects

A complete solution from one source



Mühlbauer
High Tech International



Data Enrollment & Data Management



IDENTIFIER 5000
ePassport Laser & Inkjet Personalization



ID Document Production & Personalization



Access Control & Supervision



Border Crossing & Verification

Issuing high secure ID documents needs special technology, market know-how and experience. is your competent solution partner along the complete value chain of the TECURITY market.

From data enrollment over inlay and ID document production as well as laser, inkjet or re-transfer personalization you will get modular and flexible machine concepts to produce fully ICAO compliant fraud resistant documents in best quality.

The latest solution is the ePassport Personalization System IDENTIFIER 5000 that can be configured for inkjet, laser or re-transfer personalization. Due to the modular structure the combination of all technologies within this innovative equipment is also possible. Additional to the ePassport Personalization portfolio Mühlbauer is able to provide a full range of card personalization systems for all kind of technologies and throughput ranges.

Combined with the latest production management software Mühlbauer INCAPE and the border crossing solutions Mühlbauer SIMPLE and FAST the turnkey solutions for every demand in the Smart Card and ePassport area is round off.



Mühlbauer AG
Josef-Mühlbauer-Platz 1
93426 Roding, Germany
Phone: +49 9461 952-0
Fax: +49 9461 952-1101
Email: info@muehlbauer.de
Internet: www.muehlbauer.de

TECURITY® - Complete Solutions setting the new Standards

TWIC cards hit the road in March but readers to check them remain stuck in neutral

Transportation workers will soon be carrying the first TWIC cards and they will not be delayed getting into transport facilities by a contact chip and PIN number. That is because TSA officials have decided that contactless is the only way to go for everyday TWIC use. But the readers have not yet been defined ... so while a new working group does its thing, use of the new cards will be limited.

Contactless was the original plan since the project was announced after 9-11 and the initial prototype phase contract was awarded to BearingPoint back in August 2004. But contactless temporarily got bumped in the spring of 2006 when TWIC officials deter-

mined that they needed to more closely follow HSPD-12 and its decision to require a PIN to unlock the biometric.

Industry rallied against this decision citing that it would make the access control process a bottleneck to rapid entry into secured facilities. Additionally, many stressed that the encapsulated nature of contactless readers makes them less susceptible to damage resulting from the elements and vandalism. The cries were heard and the mandate for reader deployment was postponed so that appropriate contactless biometric readers could be identified for TWIC operation.

A bit of background

TWIC is based on the Maritime Transportation Security Act (MTSA) that pertains to individuals that need unescorted access to secure areas of MTSA regulated vessels, facilities, and Outer Continental Shelf (OCS) facilities, which includes but is not limited to longshoremen, truck drivers, vendors, facility/vessel employees, maintenance personnel, train crews, etc.

The cards, planned for issuance beginning in March, are compliant with the FIPS 201 specification and contain a dual interface chip and biometric templates.

A recent TSA announcement details the issuance process in the following way: "TWIC enrollment will begin in March of 2007, initially at a small number of ports. Additional TWIC deployments will increase and continue throughout the year at ports nationwide on a phased basis. Workers will be notified of when and where to apply prior to the start of the enrollment period in their given area. After issuance of TWIC cards to a port's workers has been accomplished, DHS will at each port establish and publish a deadline by which all port workers at that port will thereafter be required to possess a TWIC for unescorted access.

"The total population is around 750,000," says John Schwartz, TWIC project manager, TSA, "but it is a transient population so we think during rollout it will approach 850,000 or more." With a rollout goal of just 18-months to issue all cards, the project is a significant undertaking.

"We will have enrollment centers at population nodes ... at a minimum of 120 locations throughout the US," says Mr. Schwartz.

At these enrollment centers, the applicant's ID documents are scanned, 10 fingerprints are captured, and a facial photo is taken. This information is encrypted and transferred into the central TWIC system. A security threat assessment for the applicant is conducted by TSA. If the applicant is approved, the card is printed and the individual is notified to return to the

What does the first TWIC rule specify?

Security threat assessment – All applicants will undergo a comprehensive background check of criminal history records, terrorist watch lists, immigration status, and outstanding warrants. If no adverse information is found, the threat assessment takes less than ten days.

Technology – The credential will be a smart card containing the applicant's photograph and name, expiration date, serial number, the holder's fingerprint template, a PIN chosen by the individual, and a card holder unique identifier.

Use – During the initial rollout of TWIC workers will present their cards to authorized personnel as a flash pass (visual inspection only). The Coast Guard will verify TWIC cards when conducting vessel and facility inspections and through spot checks using handheld readers to ensure credentials are valid (reading the chip via the contact interface). Until contactless card reader technology is tested and specified, facility owners and operators will not be required to utilize TWIC readers for facility access.

Cost – The fee for TWIC will be between \$139 and \$159 and the TWIC cards will be valid for 5 years. Workers with current, comparable background checks including a HAZMAT endorsement to a commercial drivers license, merchant mariner document or Free and Secure Trade (FAST) credential will pay a discounted fee, between \$107 and \$127.

Biometric data – Applicants will provide a complete set of fingerprints and sit for a digital photograph. Fingerprint checks will be used as part of the security threat assessment and biometric templates will be stored on the card.

Privacy and information security – The entire enrollment record (including all fingerprints collected) will be stored in the TSA system, which is protected through role-based entry, encryption and segmentation. Vendor employees will undergo a TSA security threat assessment prior to collecting biometric and biographic data. All enrollee personal data is deleted from the enrollment center workstations.

enrollment center where, following biometric verification, he or she obtains the card.

Contactless is coming but not for a while

Industry, led by the International Biometrics Association, helped convince TSA that it would be a mistake to launch TWIC using a contact chip for everyday access control decisions. But from the outset TWIC officials knew they needed a secure reader that could be deployed in offline as well as online environments. The two approaches, it was determined, needed to be reconciled.

"We have a working group that is building a contactless biometric reader specification (for TWIC)," says to Mr. Schwartz. The group's report is due on Feb. 28. "Then we will test the new spec in five geographically-dispersed locations," he adds.

Because this new development will take some time, the TWIC rulemaking process was split into two parts: card issuance and reader deployment.

"On Jan. 1 we posted the text of the implementing rule to kick-off the program," says Mr. Schwartz. It will actually be in effect on the 25 of March following the required waiting period.

The requirement to acquire and use TWIC readers is postponed and will be in a follow-on rule. Thus, for a window of time, TWIC cards will be in the field but there will not be readers at access points.

"We will be using it as flash pass (in the interim)," according to Mr. Schwartz. "We are not going to be using the (contact) chip on a routine basis because ... we feel it will slow up commerce too much for everyday in and out access verification."

But, he stresses that the contact chip will be used for spot verification and in cases where there is reason to suspect an individual may be doing something wrong. The Coast Guard will be validating TWICs with handheld contact chip readers as part of regular security checks, suggests Mr. Schwartz.

Vendors and prices to be determined "in the coming weeks"

The cost for the TWIC card will be a direct pass-through to the user. Because the bid has not been awarded, however, the final cost is not known. Figures released by TWIC suggest that each cardholder will pay between \$139 and \$159 for the initial card and between \$36 and \$60 for replacement cards. TWIC cards will be valid for five years.

While the final award has not been made for the project, Mr. Schwartz said that the field had been narrowed to eight qualified vendors from the pool of respondents. TSA spokesperson, Darrin Kayser, told *SecureIDNews*, "we expect to make an award in the coming weeks."

It looks like this time the TWIC is really on track and we will see cards, readers, and usage in 2007.



We're not just another pretty face...

We not only give you beautifully printed cards on the longest lasting and most durable ID card printers on the planet, but we are also the single source for all of your secure credential solutions...

NEW for 2007! Contact us or your local **EDISecure®** reseller about our unique trade-in program where you could get up to \$3,000 in real cash for each of your current ID card printers.* **Ask about our 3 year standard warranties!**

*Most re-transfer and direct ID card printers qualify. Contact us for details!

EDISecure®
PROVEN WORLDWIDE.

1-888-DIS-USA-1 • www.edisecure.com • sales@dis-usa.com



Re-transfer Card Printers

Direct Card Printers

Card Management Software

No change, no problem ... with smart card enabled parking meters

Solutions like Parcxmart can save municipalities cash and boost user convenience

Ryan Kline

Contributing Editor, AVISIAN Publications

Since the conception of the on-street single-space parking meter in Oklahoma City, OK by Carl C. Magee in 1935, people have been reaching deeper into their pockets to feed the meter. But in a world where non-cash payments have become the norm, many believe the time has come for parking meters to dispense with the coins. There are nearly 500 million in the United States alone, so the challenge is great, but so too is the opportunity. If every parking meter in the U.S. collected just \$2 per day, the gross revenues for a single day would reach a staggering \$1 billion.

Parcxmart creates smart card-based payment solutions for municipal parking. It offers a multi-application smart card platform that integrates with existing electronic funds transfer (EFT) networks. The company's parking payment solutions are deployed in Bridgeport, CT, New Haven, CT, and Truckee, CA.

Parcxmart is launching several new city parking solutions throughout 2007, including first quarter pilots in Ft. Lauderdale, FL, Newark, NJ, Baltimore, MD, and an undisclosed number of smaller cities in the north-east primarily in Connecticut and Massachusetts.

How the Parcxmart system works

In the Parcxmart programs, customers receive the smart card at no cost. They load the card with a set amount of money to be used for parking at all participating meters and garages. The card can also be used for payment at participating merchants. The smart card is viewed the same as cash: if it is lost, there is no replacement. A benefit, according to Mr. Regan, "it is not linked to their name, address, or social security number so they will never experience identity theft or fraud when using our card to buy time at a meter or purchase small dollar goods in our local merchant community."

To pay for parking, the card is inserted into the meter and the desired amount of time is selected. The meter adds time in fifteen-minute intervals on the screen. When the desired duration appears, the smart card is removed. But just like most meters that have a maximum time limit, the meter can still regulate the space and only allow people to park there for a finite duration. According to Parcxmart, the average purchase in a parking meter is \$1.39.

To encourage stores to sell the smart cards for the municipalities, loyalty programs and in-store payment acceptance are offered. Stores that distribute the smart cards can also accept them as a means of payment. Customers who use the smart cards at the stores can receive coupons

to be used in conjunction with the card. In Truckee, CA, customers who pay for parking with the Parcxmart Card receive a 15% discount. The average purchase, according to Parcxmart, in a retail store or coffee shop is \$6.93.

The movement of money between parties in the system

Electronic value is loaded onto the Parcxmart card's electronic purse (e-purse) using a debit or credit card at point of sale (POS) terminal. The terminal, which includes a smart card reader and runs the Parcxmart load application, is made available to local merchants in the communities served by the parking system. The transactions are processed via the existing EFT networks, just like any other over-the-counter debit or credit card purchase.

Transaction data is sent to the Parcxmart host for processing. The host processes this data and prepares a settlement advice that is sent to the municipality's chosen bank to transfer funds from the cardholder's bank account. Parcxmart never touches the money—it only passes through their system.

Commissions associated with the sale of Parcxmart cards are settled with the merchant, and value associated with the load volume is moved to the Parcxmart Trust Account. The money from the trust account is then used by Parcxmart to reimburse the parking authority for revenue spent at city parking locations. All monetary movement is managed by a bank triggered by settlement advices and timeframes established between Parcxmart, its merchants, and the parking authority.



The Parxmart system is even fully auditable. Parxmart can provide full reports, even encompassing risk management for the program. Parking authorities are granted access into the Parxmart Host so that transactions and other related data associated with the program can be viewed.

Advantages of smart card-based parking solutions

The primary driver to switch from a traditional meter system to a smart card capable system is to increase revenue and decrease operating costs. Obviously, the fewer times a city has to physically visit each meter to collect coins, the less expensive it is to operate the system. "All of the cities want to collect less coin and cash and believe our system will enable that to happen once we reach about a 20 percent market penetration rate," said John Regan, President of Parxmart. After the first 90 days of operation in New Haven, Parxmart was at a ten percent penetration with a steady trend upwards, he suggested. "We believe we will be over 20 percent end of first quarter (2007)," continued Mr. Regan.

According to Parxmart, "With a secure smart card payment option, you minimize the use of coins and cash, and in the process the possibility of fraud is decreased, and the reasons for vandalism are diminished."

The Smart Card Alliance Transportation Council also acknowledges advantages in implementation of a smart card application for collecting payment at meters: "If implemented properly, a smart card system can allow a city to increase revenues dramatically. The city can increase rates on existing meters without incurring the high initial replacement costs associated with implementing a completely new system."

Customer convenience through interoperability

With an independent card distributor and back-end-operator like Parxmart, the potential for an interoperable, multi-city system emerges. One day, consumers might be able to use their card at any meter or garage nationwide that is part of the network.

"We have just begun our first interoperable city program between Bridgeport, CT and New Haven, CT. Bridgeport will not finish rolling out until end of February, so it is too early to tell (how

many people actually use the cards in an interoperable fashion.) We will see this happen in southern Florida and northern New Jersey soon. Anecdotal information from lawyers who work in both courthouses in Bridgeport and New Haven have stated to staff they use their cards in both cities all the time."

But when individual municipalities distribute their own card and manage their own system, consumers might need different cards to park in neighboring cities.


Many municipalities, in the U.S. and around the world, issue their own smart cards as a parking solution for their city. According to the report, "Smart Cards in Parking" by the Smart Card Alliance Transportation Council, "in New York City, the Department of Transportation has been issuing contact smart cards to pay for parking since the summer of 1998. The cards are prepaid and sold as disposable cards. As of late 2005, over one million cards have been circulated at a rate of about 25,000 cards per month."

Because these systems are created for use in the one locality, they are not interoperable with other smart card parking systems. The report continues: "Historically, adoption rates for these smart card systems have been low. Many cities record usage rates in single-figure percentages. Low usage rates have been attributed to the lack of an effective card distribution and reload infrastructure, the lack of an effective card marketing plan (for which cities typically lack budget and expertise), and the fact that the cards can only be used to pay for agency-specific parking (unless otherwise negotiated)."

The elimination of change in the parking sector is certainly not an easy task, nor is it one that is certain to occur. Using smart cards does enable municipalities to lessen the amount of change they must collect, but until usage reaches significant levels, it is simply an alternative method of payment that requires additional effort and cost to support.

The ideal scenario would likely involve an online, networked meter infrastructure much like the global point of sale networks. But that is unrealistic due to the high costs, unsecured environments, and lack of power at on-street parking locations. Off-line payment platforms, like the one offered by Parxmart, are much cheaper to initiate and hold the promise of operational cost savings and user convenience.

Parxmart has roughly 5,000 cards in circulation, mostly in New Haven. There are more than 3,000 metered spaces accepting Parxmart cards. 2007 is the first year of post pilot operations in New Haven. Parxmart is predicting to have about 100,000 cards in circulation by 2008.



City	Cards Issued	Single or Multi-space	Multi-application	Reloadable
NEW YORK	1,000,000	64,200 (SS) 1,850 (MS)	NO	NO
PARIS	3,000,000+	13,000 (MS)	NO	NO
NEW HAVEN	5,000 Combined	2,500 (SS)+GARGES	YES	YES
BRIDGEPORT		1,000 (SS)	YES	YES
TRUCKEE		500 (SS)	YES	YES

Trickle-down effect of HSPD-12

Kathleen Phillips, Vice President, Sales and Marketing
Fargo Electronics



While the implementation of HSPD-12 has been the card-related news to watch in 2006, its effects will be felt in other areas as well throughout 2007. HSPD-12 mandates the badging of all federal employees and contractors under guidelines formed by the National Institute of Standards and Testing. While this is a landmark move for the federal government, the impact of established standards for smart card

credentials on state government, university and corporate markets will have a more far-reaching effect.

For the first time, mid- to large-card program managers have a comprehensive template to guide them in designing and implementing a secure smart card credential program. While not every feature of the NIST standard may fit individual programs, the standard provides a thorough checklist for consideration. Two highlights of the NIST standard are important for other markets:

- A detailed vetting process that includes background checks and the authentication of 'breeder' documents
- A credential that is difficult to counterfeit and a structure to prevent the creation of unauthorized credentials.

The impact of the NIST standard, in combination with more readily available, off-the-shelf smart card software applications and overall lower technology card prices will make a higher-security smart card program more reachable. And while HSPD-12 was conceived to address security issues, the impact of productivity and efficiency will be seen in applications such as local area network logon, email signature, Web portal usage, etc. Market leaders who demonstrate a return on investment to private sector customers will see a higher adoption rate of their smart card solutions.

Keeping up with rapid security pace paramount in '07

Dave Ella, VP of Products,
AMAG Technology

The world of security is always changing. Below are five trends we've noticed that are moving at a rapid speed.

Trend #1

Large organizations are maintaining all of their identity information in a single place – whether it is an ERP application like SAP, an LDAP identity management directory or Microsoft Active Directory. In this

new environment, the integration to the physical access control and badging systems needs to be real time and flexible to take into account changing organizational requirements.

Trend #2

AMAG is finding that schools and universities are tightening up the access privileges of their students down to specific doors at certain times. Lab time, for example, is assigned and students are allowed access at their assigned time only. In this environment, you need a powerful capability to amend student access rights in bulk at the start of a new school year or when they transition from class to class.

Trend #3

Today almost all new physical access control systems incorporate integrated digital video management. This allows a security guard to compare the person at the door to the photo of the person whose badge he or she is using. This can provide a considerable increase in security at the perimeter without the need for biometrics or other additional security measures.

Trend #4

Throughput of visitors is important, and we find that many customers who process several hundred visitors a day—for example military bases or prisons—are using driver license scanning techniques to populate their ID management systems. The driver license scanner populates visitors' details in seconds, including their photos, and therefore allows visitors to be processed much more quickly, keeping delays to a minimum.

Trend #5

The federal government and transportation workers ID card projects have been moving forward quickly and one of the key issues as we see it is the inter-agency interoperability of the cards and making sure that credential revocation databases are freely available. If an employee of Agency A visits Agency B carrying his credential, Agency B needs to be able to check that Agency A has not revoked the credential. In other words, is the credential still valid?

Next generation smart card will be Internet savvy

Gil Bernabeu, GlobalPlatform Technical Director
and Gemalto Technical Advisor, Standardization & Technology

The year 2007 will witness the integration of smart cards into the Internet world. The next generation smart card, referred to by GlobalPlatform as "connected smart card," has been initiated by the dynamic advancements of the telecom sector, and its increasing desire to offer end users innovative services. However, all sectors deploying smart cards will benefit from connected smart card functionality.

Simplifying the language

Current technology requires the host of a smart card, such as the mobile handset or a computer, to be a key element in the communication process that allows an application provider access to an existing ap-

plication on the token. Connected smart cards, however, will authorize smart card integration into all general IT infrastructures.

Server to server connectivity

Connected smart cards interfacing with IT infrastructures take advantage of industry developments such as improved communication speed (HSP) and processing power enhancements proposed by new chips. The improved architecture enables next generation tokens to be securely connected to an IT network.

End user interaction

Connected smart cards will also provide a web interface, encouraging end users on their handset to use a standard Internet browser to interact with their personal smart card tokens.

The technology

The release of Java Card 3.0 in 2007 will be one of the most significant developments in this area. Java Card Forum, which promotes and develops Java technology, and Sun Microsystems in collaboration with GlobalPlatform, have integrated these new features into a completely new platform; not as an extension of current technology. This new standard also proposes a migration path for the numerous issuers of Java Card 2.2 to transition to Java Card 3.0 technology.

Although the new Java Card 3.0 environment is increasing functionality, it will simplify the development of a smart card implementation by using standard Internet knowledge familiar with IT developers. It is envisaged that this will encourage industry sectors currently not engaged with smart cards to adopt and benefit from the technology, and increase cross-industry collaborations.

Based on 2007 advancements of Java Card 3.0, GlobalPlatform plans to develop an application management framework to facilitate the deployment of this technology, which it aims to release in early 2008. This will facilitate other technology standardization bodies currently using GlobalPlatform technology, such as the European Telecommunications Standards Institute, to smoothly move into this new environment.

Securing financial transactions a high priority for '07

Matt Landrock, *Managing Director*
Cryptomathic, Germany



Decreasing fraud through security will continue to be a high priority for the financial sector in 2007. The ability of criminals to continually infiltrate financial systems has resulted in the realization from the market that investing in high security technology now will achieve long term benefits—from reduced fraud to customer assurances that their investments and transactions are protected.

The high-level adoption of EMV technology throughout many global regions, such as Europe, Asia and South America, has intensified over the past 12 months, demonstrating the commitment of many countries to implement new and more sophisticated systems to increase financial transaction security. In some countries, legislation has played a key role in encouraging adoption by the financial institutions. In other regions, the liability shift deadlines imposed by the international payment systems has been the key driving factor.

Canada will be a major focus in 2007 as it continues the transition to EMV payments, with an EMV migration deadline of 2010. It is predicted that EMV adoption in this market will impact the U.S. payment industry's reluctance to migrate to EMV, as the business security benefits of implementing chip and PIN will become ever more apparent and necessary in such an evolving and sophisticated marketplace.

The migration of EMV within adopting regions has another key advantage: it provides the infrastructure and tools for the financial sector to implement ever increasing robust security measures. Over the past year this has been witnessed by the significant acceptance and deployment globally of two-factor authentication (2FA) methods. These are based on the Chip Authentication Program (also known as OneSmart from MasterCard) which allows issuers to leverage the chip card roll-out for strong user and message authentication for online banking. The adoption of the technology, particularly in Europe, demonstrates the increased awareness among issuers, who now understand the security advantages of authenticating an online customer based on what he has and what he knows.

Although Europe has, and will continue to implement, 2FA widely across many markets, the global rise of 2FA has in part been contributed to the U.S. Federal Financial Institutions Examination Council's (FFIEC) guidelines, which requires all U.S. banks and financial institutions to implement 2FA mechanisms in the transfer of money to a third party account.

FFIEC's recommendations requested implementation of 2FA by the end of 2006. However, as it implicitly excludes many existing U.S. 2FA solutions because they do not focus on something the user has in their possession, but what they know—such as static passwords and images—the market is still open to increasingly sophisticated criminals who are continually creating new methods to access financial information. Subsequently, to ensure the highest possible security, U.S. banks will need to upgrade their 2FA systems in 2007 to reflect those used in international markets.

As the payment scheme providers and payment card industry advance their agenda on decreasing fraud through tightened security measures, emphasis has also been placed on devices. One final area of continued growth in 2007 is the ever-increasing demand for automated Advanced Key Management Systems to secure keys between issuing and acquiring networks. The new technology reduces the cost and time of manually installing and managing the life-cycle of keys on devices at regular intervals by removing the need to have key custodians present locally. This is an important development as it allows the keys to be updated more frequently, at no extra cost to the financial market and its customers, thus preventing the increasing number of fraudulent attacks on ATMs and similar transaction points.



Feds may yank Regulation E's receipt requirement for small dollar transactions

Change could open floodgates for contactless and other payment cards in vending, transit, unattended locations

Chris Corum

Executive Editor, AVISIAN Publications

Regulation E, the rule outlining consumer rights with regard to electronic financial transactions, can make things tough on new payment offerings – but many argue that is its mission. Electronic payment providers have to make a slew of disclosures, they have to guarantee against fraudulent usage, they have to provide periodic statements, and they have to provide receipts for transactions. But this receipt requirement may be loosening. The Federal Reserve (Fed) is considering a change that would exempt transactions under \$15 from the need to provide a receipt. Big deal you say? Read on.

Here is the Fed's summary description:

"The Board is proposing to amend Regulation E, which implements the Electronic Fund Transfer Act ... The proposed amendments would create an exception for certain small-dollar transactions from the requirement that terminal receipts be made available to consumers at the time of the transaction."

NEW
from Magicard

Finally, a tough printer for tough laminated cards.

With the unique UltraCoverPlus 2 year warranty.



Tango +L

NEW

Integrated ID Card
Printer + Laminator



The **Tango +L** prints and laminates your card for increased visual security, and to protect cards against physical wear for a longer lifetime.

With a Plug and Play Windows driver, standard Ethernet and USB for flexible interfacing, and both hardware and software printer locking facilities, the Tango +L is the professional's choice.

Double Cover

UltraCoverPlus® 2 year warranty and support



Double Strength

Robust metal design with lockable security



Double Security

Both HoloKote® watermark and Holographic lamination available



Ultra Electronics Card Systems
6711 - 176th Avenue, NE Redmond, WA 98052
Tel: (425) 556 9708
email: USSales@UltraMagicard.com
www.Magicard.com

MAGICARD
secure ID card printers

What was some of the justification suggested for the change?

Consumers are using electronic payments where they used to use cash as the dollar value 'threshold' for card payments has been lowering in consumer eyes. The idea is that consumers *want* to use cards to pay for things that, in the past, would have required cash. Examples include vending machines, transit tickets, parking facilities, and other small ticket items and unattended locations.

According to the proposed rule change:

"Merchants, financial institutions and payment card associations have responded to the shift in consumer preferences towards non-cash methods of payment for small-dollar transactions in various ways. Payment card associations have changed their rules to enable quicker processing of transactions for both debit and credit cards. For example, these associations have waived the signature and personal identification number (PIN) authorization requirements for certain types of purchases under \$25. Moreover, to encourage merchant acceptance of payment cards, these associations have also reduced their debit and credit card interchange rates for certain small-dollar transactions. In addition, some card issuers have integrated new technologies into their products which allow consumers to swipe or wave radio frequency-enabled cards or other devices to authorize payment in "contactless" transactions. These initiatives have reduced the amount of time consumers spend at checkout, which has in turn allowed merchants to process more transactions in the same amount of time."

- The proposed changes would benefit industry but have no real value for consumers, so this is no longer a consumer protection regulation but rather an industry expansion effort.
- Arguments in favor of the change centered around the fact that this could help to open up the use of the payment cards at new locations and venues, to the benefit of the modern consumer.
- Additionally, many industry comments suggest that the threshold for the receipt exception be raised from \$15 to \$25.
- Keep the amount consistent with the payment card association's dollar value for no-signature requirements.
- Keep the amount consistent with common corporate travel policies for no receipt required for expense reporting purposes.

David DeMedio, commented as a representative of USA Technologies, a leading manufacturer of payment readers for unattended devices. He explained the potentially insurmountable challenges to providing receipts at many unattended devices:

"Deploying a credit/debit payment option, with the requirement to provide a receipt, would be a major, if not insurmountable impediment to industry-wide acceptance. In vending, for example, many of the makes and models of the estimated 8 million vending machines installed in the U.S. do not have the required space to accommodate the additional receipt printer and paper roll. Also, since the newly introduced contactless credit/debit readers utilize the existing, available power from the host vending machine, adding a receipt printer would now require an additional power source to power the printer."

He also addressed the service challenges that we have all likely experienced when trying to get a receipt from unattended gas pumps, stating:

"Significant servicing issues arise with offering receipts because of the unattended, distributed nature of these machines and the infrequency in which they are serviced. Malfunctioning printers, empty paper rolls and litter from discarded receipts, which could go uncorrected for the reasons above, could actually cause the consumer to have a negative experience while purchasing from the machine, thereby negating the purpose to install the printers in the first place."

What happens next?

According to a spokesperson for the Federal Reserve, the proposed change will follow an established process. Staff will review the comments and consider them as they prepare a final recommendation. This will be presented to a Board committee for consideration and, if approved, will be presented to the Board of Governors for final consideration.

Though a timeline is not available, other proposed changes have taken as long as eighteen months from start to finish. Several things, however, work in favor of this change being accepted or rejected in a more rapid period. First, it is the only proposed change to Regulation E currently under consideration. Second, it is fairly straightforward issue for consideration and does not possess the degree of complexity of many other proposals. Stay tuned.



Arguments for and against the change ...

The comment period on the proposed change ended on January 30, 2007, and more than 30 comments were received in response to the proposed changes. As one might expect, consumers submitting comments tended to react negatively to the proposed change, while industry came down in favor of the change. Of course, this should in no way be deemed a true representation of either group's opinion as only those with a vested interest or extremely strong opinions are likely to take the time to comment.

The arguments against the proposed change centered on the following themes:

- Consumers need receipts to keep track of expenditures, dispute incorrect charges, and reimburse expenses with employers.

The Original **Multi-Technology Readers**



**125 kHz
PROX**



**13.56 MHz
SMART**



**FIPS 201
PIV II
US GSA APL**

The Most Versatile, Secure Readers in the Industry



XceedID®
Xceeding The Ordinary

To learn more please visit: www.xceedid.com

Machine Readable Travel Documents

with biometric enhancement: the ICAO Standard

Mary K. McMunn

Former Chief, ICAO Specifications and Guidance Material Section

This article reviews briefly the work ICAO has been doing over the past nine years to specify how to make use of biometric technology to enhance the security of travel documents and to facilitate inspection of international travelers at border control points.

The Convention on International Civil Aviation and Annex 9 (Facilitation) together provide a framework of obligations of member States and Standards and Recommended Practices pertaining to the immigration and customs inspection and clearance of persons in airports. In this context ICAO, since 1980, has been publishing specifications for standard formats for machine readable passports, visas and official travel documents. Document 9303, Machine Readable Travel Documents, is now a suite with three parts. Part 1 (Volume 1 and 2), Machine Readable Passports, was published in its sixth edition in September 2006.

Most readers and administrations are by now very familiar with the basic machine readable passport, which is now being issued by at least 110 States and territories, a number that is steadily increasing. The standardized format is comprised of two parts – a visual inspection zone or VIZ, containing mandatory and optional data elements in a prescribed layout, and a machine readable zone or MRZ, containing mandatory data elements in a form and position that are absolutely mandatory.

The two machine readable lines of OCR-B typeface, with their standard format, data elements, field lengths, and check digits, comprise the first security measure that ICAO invented for a passport.

Another security measure inherent in the document and in the inspection procedure is the use of a mandatory photo image to link the holder of the document to the document itself, in order to confirm identity. In recent editions of Doc 9303 ICAO has been tightening up the specifications for the photo, to insist on high-quality images of adequate size, preferably digital images printed directly onto the data page, in order both to prevent photo substitution and to offer more confidence to the inspector or airline agent making a visual comparison between the photo and the person presenting the passport.

But over the years—and well before 9/11—member States identified the need to confirm identity of travelers more effectively, due to the myriad cross-border social, political and criminal problems that emanate from identity theft. So in 1997 the ICAO TAG/MRTD asked its New Technologies Working Group (NTWG) to begin a systematic study of biometrics and their potential to enhance identity confirmation with passports and other travel documents.

In search of the “right biometric” for travel documents, the chosen approach was to first identify requirements instead of just reviewing industry-based technology studies. This set ICAO apart from mainstream

thinking at the time, and incidentally invited criticism from purveyors and users. But we felt that to choose the “best-performing” biometric based on laboratory tests and then try to adjust our requirements to it would not be the right approach. Instead we chose to evaluate the different biometrics against the unique requirements of travel document issuance and inspection.

And what are these requirements? Briefly, they are: compatibility with travel document issuance and renewal; compatibility with machine-assisted identity verification requirements in the issuance and inspection

The technology that met all of ... requirements was the contactless integrated circuit, and the NTWG decided that of the two ISO-standard options, the “proximity” type (ISO/IEC 14443) should be specified.

ICAO has been tightening up the specifications for the photo, to insist on high-quality ... preferably digital images printed directly onto the data page, in order both to prevent photo substitution.

The two machine readable lines of OCR-B typeface, with their standard format, data elements, field lengths, and check digits, comprise the first security measure that ICAO invented for a passport.



processes; redundancy; global public perception of the biometric and its capture procedure; storage requirements; and performance. Considering all of these factors and using a quantitative scoring methodology, the group found that face came out on top with an 85% compatibility rating, while finger and iris were tied in second place with a 60-65% compatibility rating. Therefore face was recommended as the primary biometric, mandatory for global interoperability, and finger and iris were recommended as secondary biometrics to be used at the discretion of the passport-issuing State.

The face as primary biometric addresses numerous identity-related requirements. It supports lookout identification, as prior enrollment and cooperation of the subject are not required for successful image

... because data written to a chip can be written over, a public key infrastructure (PKI) scheme was required, in order to give the reader of the chip assurance that the data had been placed there by the authorized issuer ...

... face was recommended as the primary biometric, mandatory for global interoperability, and finger and iris were recommended as secondary biometrics to be used at the discretion of the passport-issuing State.

Under Basic Access Control (BAC) the inspection system uses a "key" derived from numeric data elements in the MRZ to "unlock" the chip ... Thus the passport must be open in order for the chip to be read ...

capture, and facial images are available on virtually every person in the world. Face also permits 100% identity confirmation in the inspection process, as the travel document photo of quality specified by ICAO could be used for machine assisted checks in the absence of an electronically stored image. Moreover, with the photo, facial recognition can be done visually, even when the equipment malfunctions!

After deciding that the face would be the primary biometric, the NTWG looked for an appropriate storage medium. The medium chosen would have to offer enough data storage space for images of the face and possibly other biometrics, as the concept of using templates had been abandoned due to the fact that templates and their readers are not internationally standard. The technology had to be non-proprietary, available in the public domain worldwide, in the interests of global interoperability. And of course the technology had to be compatible with book-style (paper and cloth) documents. Ease of use, without a requirement to position or fit the document into a reading device, was also a factor. The technology that met all of these requirements was the contactless integrated circuit, and the NTWG decided that of the two ISO-standard options, the "proximity" type (ISO/IEC 14443) should be specified.

Next, a standardized "logical data structure" for programming the chip was specified to ensure that chips programmed in any country could be read in any other country. And because data written to a chip can be written over, a public key infrastructure (PKI) scheme was required, in order to give the reader of the chip assurance that the data had been placed there by the authorized issuer and that it had not been altered in any way since then. Thus an expert group within the NTWG developed specifications for a specialized PKI for application to travel document issuance and inspection.

Finally, during the testing of chips and readers there arose issues of skimming and eavesdropping. The physical possibility of skimming – the surreptitious reading of the data in the passport chip by means of a concealed device and unnoticed by the holder – is considered to be extremely remote, but nevertheless it is a concern. Eavesdropping – illegally listening in on a communication between the chip and the reader – though unlikely, is feasible. To address these concerns a scheme for "basic access control" (BAC) was developed and recommended for use by issuing States. Under BAC the inspection system uses a "key" derived from numeric data elements in the MRZ to "unlock" the chip so that the system can read it. Thus the passport must be open in order for the chip to be read, and the holder is assured that his data can be read only when he hands over his passport.

So there you have it – what ICAO calls its biometric blueprint, consisting of four parts – the facial image, the contactless proximity chip, the logical data structure, and the ICAO PKI. These "four pillars" are each essential to the ePassport, and are inseparable from one another. Technical details about the blueprint and the ePassport standard and other aspects of ICAO work in MRTDs can be found on our dedicated web site: mrttd.icao.int.

This article originally appearing in the ICAO MRTD Report 2006, and is reprinted with permission.

'Tap and go' contactless payments on a roll

Trevor Pavey, *Manager of Contactless Payments*
Texas Instruments



The era of 'tap and go' payments fueled by contactless technology has arrived. In the past year, issuers have released more than 14 million contactless credit cards in the U.S. under the American Express, MasterCard, and Visa brands. Driven by the revenue potential and greater customer convenience of contactless payment, retailers, including 7-Eleven, CVS and McDonald's, announced nationwide roll-outs.

In 2006, the market trials proved the value of the technology. With research that demonstrated faster transactions, shorter lines and increased spending, issuers put even more 'tap and go' payment devices in their customers' hands and equipped close to 200,000 POS locations.

Contactless technology has also had a liberating effect on payment form factors. While traditional plastic cards dominate in the non-contactless world, increasingly companies such as MasterCard, American Express and Citibank are experimenting with alternative forms like key fobs. Advances in performance and the increasingly smaller size of radio frequency chips and antennas are making these new forms possible, while ensuring the optimum consumer experience at the checkout.

What does the future hold for contactless payment? Our top three predictions for 2007 are:

Increase in Retailer Roll-outs: In the coming year, we expect more retailers to follow the lead of early adopters. POS locations will rise more than 33% from 2006, reaching 300,000. New applications will proliferate for micropayment transactions under \$25 where speed and convenience are crucial, such as in taxicabs and vending machines. We may even see more retailers, like Jack-in-The-Box, that opt to forego trials and move straight to chain-wide roll-outs.

Cool New Form Factors: The inherent coolness factor of new 'tap and go' forms will help drive consumer acceptance. Among the potential new form factors are 2-D fobs resembling grocery store loyalty cards, and 3-D key fobs which can be fashioned into just about any shape imaginable, such as a football helmet or medallion in the shape of a company logo. Mobile phones, watches and portable music players enabled with contactless payment are also on the horizon.

Greater Consumer Acceptance: Contactless payment will gain more traction with consumers. To win their confidence, card issuers must communicate that this new technology does, in fact, offer a secure payment transaction, and that the liability policies in place for traditional credit and debit accounts also apply to contactless transactions. Issuers will also continue to tout the speed and convenience value propositions of contactless in their marketing to increase consumer perception about the technology's benefits.

Retail payment is being transformed with the maturation of contactless technology. 'Tap and go' payment convenience for everyday purchases has reached major retail chains, attracting new retailers and consumers alike. As customers continue to learn about this new form of payment, we'll see the continued growth of secure contactless payment, available in a number of new locations and in new types of devices.

E-nnovation in 2007: The e-wallet, e-passport, e-pedigree bring greater security and convenience

Manuel Albers
NXP Semiconductors



From ultra thin smart card ICs that are finer than a human hair, to infusing an extra layer of patient safety to pharmaceutical products, 2007 will bring the development of contactless and RFID technologies closer to the consumer.

We have long been familiar with the fact that customer adoption is key, and the goal of our technologies is to deliver simplicity, security and the most innovative designs to our customers. In 2007, I think the focus will be on three key technologies that will change the way consumers go about their everyday lives.

Consider the mobile wallet. With more than 225 million mobile phone users in the United States alone, it's only natural for consumer payments to extend to this device. Once adopted, the benefits for contactless payment are obvious: speed of transaction for merchants, convenience for consumers and the use of smart objects instead of traditional cards as a marketing tool for banks.

NXP believes that, as we move forward, credit cards and mobile payments will coexist. Online banking and traditional credit card payments will reinforce the trend of contactless payments, creating an environment where credit cards and mobile payments will fortify the habits of the connected consumer. The tap of a phone to pay for transport or the ability to scan an advertising poster for more product information will change the way we transact digitally.

I think we will increasingly see cities in the U.S. adapting mobile payments for public transportation, offering speed and convenience to the rider. Atlanta, Boston and Houston are already planning to adopt mobile payments for public transportation in the coming year via NXP MIFARE technology, which is also being used in several Latin American countries for public transport installations.

Fueling the growth of contactless payment is Near Field Communication (NFC). I believe 2007 will be the year that sees NFC specifications made available on high- to medium-end phones. NXP is working with handset and consumer electronics manufacturers, carriers, financial institutions and service providers to build the ecosystem for NFC.

Educating the industry and value chain players about NFC and how it can drive value to consumers, merchants, and issuers will be a key challenge in the coming months.

Another trend to watch is the compliance-driven market for RFID in the supply chain, compelling the healthcare industry to seek advancements in tracking technology. One prime example of this is the electronic pedigree, an electronic quality seal for drugs to authenticate product origin as mandated by various government entities.

The World Health Organization estimates that counterfeit drugs cost the industry more than \$35 billion a year. In response, RFID technology provided by NXP and others is being used by healthcare, pharmaceuticals, and medical equipment providers in attempts to eliminate counterfeit drugs.

Finally, e-government solutions, such as e-passports or ID cards, will focus on providing scalable and secure platforms for designers. The significance of innovative design in smart card ICs that are finer than a human hair or a sheet of paper underscores the response to key security agendas from global governments. NXP is playing a critical role in this area and currently powers 30 out of 36 e-passport programs around the world, including the U.S.

Critical to 2007 is for the industry to focus on innovation surrounding its key strengths. It must also meet the market demands for effortless transactions while creating more secure government ID programs.

Need will grow for long range, driver-based vehicle ID systems

Gorm Tuxen

NEDAP/Tuxen & Associates, Inc.



The market acceptance for driver identification to be a fundamental requirement of any AVI (Automatic Vehicle Identification) system—one that is truly considered a security system—will continue to grow in 2007. It is no longer enough to just identify the vehicle, which could easily become an automated “Trojan Horse” in anyone’s security operation.

Systems presently offered, including the so-called booster tags—which are in-vehicle reader/transmitter devices—are able to read a common building access card such as a prox card.

As the trend towards smart cards continues, so will the development of these types of technologies that will allow the newer, higher level security cards to become an active component in identifying the “employee” as a driver—at long range and in real time.

These new booster devices expand the functionality to include compatibility with both 125 KHz and 13.56 MHz cards. These devices are also fully compatible with ISO 15693 and ISO 14443.

A driver-based AVI tag is made up of two components: the in-vehicle card reader/transmitter and a personnel credential, such as a contactless building access card. The in-vehicle reader will identify the building access card and “boost” the signal to an external reader at ranges up to 33 feet (11 meters), which allows plenty of time for the back end security controller to activate the barrier or gate prior to the arrival of the vehicle.

This booster device will, in effect, act as the lock and the building access card as the key. In some cases the booster will contain its own embedded vehicle ID, which allows the back end the ability to immediately match the right driver with the right vehicle. The driver must take his ID with him when he exits the vehicle, as he will need the card to gain access to the building. Only the booster will remain in the vehicle and that, alone, cannot be used to activate the barrier.

Long range driver-based AVI systems are rapidly finding their way into applications where positive driver identification must be established without bringing the vehicle to a stop. Such applications can be used at military bases, airports, utility companies, corporate and educational campuses, police, fire and other installations where vehicles must be assigned to a specific driver, such as company service vehicles.

More contactless project trials bode well for the technology

Stephen Neff, *VP Sales and Business Development*
LEGIC Identisystems Ltd.



The CARTES show held recently in Paris confirmed my feeling that the year 2007 will be a great one for the whole contactless smart card industry. The almost overwhelming number of new and innovative applications being presented by exhibitors and speakers alike bode well for the next few years.

What's impressive is the fact that a large number of public projects are in the trial phase and if successful could

be the engine for the real growth that the business needs. For instance new applications schemes such as e-payment, NFC, e-passport and the like will have a continued effect on educating the market place. That means the traditional areas of contactless smart cards, such as ticketing, access control and campus cards will continue to grow strongly.

However, what I also believe will be a trend is the demand for stricter regulation and technological ingenuity to ensure that data cannot be skimmed or gathered unknowingly. It will be a challenge for the industry to address these concerns, be they justified (in some cases) or unjustified (in other cases).

The success of many new applications for contactless smart card technology will depend on providing defenses and mechanisms that safeguard user data and privacy even if this means higher initial investment costs for system operators and system providers. This implies that solid technological security mechanisms should have priority over marketing statements that are very often written by unknowing corporate PR people who have a different—or little—understanding of the potential issues at hand.

Granted no system or technology is, or will be, secure forever, but as the market becomes more educated about RFID and contactless smart cards, it's important that everything is done to ensure that the industry does not end up with egg on its face as a result of misinformation, misinterpretation, or—as in most cases—misunderstanding. This would be a shame as we all know that contactless smart card technology can offer security features on par, or in most cases, beyond what is used today.

I think that the above two trends alone will make 2007 a challenging and interesting year. It may be the year that could lay the growth cornerstone for many years to come. We as a company expect overall growth, like this year, to be double digit again and look forward to another successful year.

The smart ID card: eventually everyone will need one

Ernie Berger, *President*,
Gemalto North America

Every individual on every network will increasingly use microprocessor-based personal security devices to identify themselves and access services. Here's the how and why of this digital security phenomenon.

Today, 2.8 billion microprocessor-based smart cards already securely identify individuals and provide them with access to services on networks. This addresses the way individuals conduct their daily life, wanting and expecting more freedom to communicate, travel or buy anytime and anywhere in a secured way. In a world of 4.5 billion people aged 14 years or older, approximately half use a smart card for some type of network identity. Some even have two or more smart cards.

We are thinking beyond the card itself to how we are connected to the bigger world of digital security for information technology. At Gemalto, we are thinking and talking about our industry in a different way.

If you think about it broadly, what we are really providing is a personal form of digital security within a networked IT infrastructure. In each of our three biggest current markets — payment, mobile communications, and identity and security — we are protecting individuals' identities and access to services over networks. And protection of digital identity, assets and transactions are vital to individuals as well as to governments and business.

In these examples, what is the role of the microprocessor card? It is a trusted, convenient and really portable computing platform with its own secure operating system and applications. It is ideally suited to identify someone and his/her privileges when connected to network-based systems.

Secure devices such as smart cards carry applications from one place to another, from one device to another. And they deliver the highest levels of security, up to full mutual authentication with private/public key pairs and encryption. But they always represent someone. A unique individual and his/her unique privileges are securely identified among hundreds of millions of others.

What started as a technology for the unconnected has found that its role is also at the network's edge as a small, portable highly secure and connected device. Eventually, these secure personal devices will be used by everyone to identify themselves, protect their identities and access services over networks.



Smart Card
Alliance

The single industry voice for smart cards ...

The Smart Card Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology. The Alliance is the single industry voice for smart cards, leading discussion on the impact and value of the technology in the U.S. and Latin America.

Through specific projects such as education programs, market research, advocacy, industry relations and open forums, the Alliance keeps its members connected to industry leaders and innovative thought.

Worldwide outreach - A primary mission of the Alliance is to show the world the benefits of smart card technology. We accomplish this through an array of outreach efforts including an informative web site, published industry reports and papers, active press relations campaigns, our Smart Card Talk electronic newsletter, and an international calendar of speaking engagements and exhibitions.

Unrivaled education - At Alliance-sponsored events and leading industry conferences, top quality smart card education is offered to the benefit of both members and leaders from industries impacted by the technology.

Task forces and reports - Active participation from representatives of member organizations feeds a vibrant network of industry-specific councils and focused task forces. Highly regarded white papers, reports, and other deliverables flow from groups focused on payments, secure identity, health care, transportation, and more.

Conferences - Alliance conferences feature informative programs and speakers who provide insight and knowledge on smart card technology and applications, coupled with exhibitions that showcase leading edge products. These events provide exhibitors with invaluable access to true decision makers and enables participants to see the technology in action.

Networking - The best and brightest from the smart card industry and the key markets it serves participate in the Alliance, attend Alliance functions, and share a camaraderie that extends beyond the Alliance organization to the worldwide network of industry activities.

Join the Alliance. It will pay dividends for your industry, your company, and your career. For more information, visit www.smartcardalliance.org.

Smart Cards in Government 2007

Ronald Reagan Building ITC • Washington, D.C. • April 10-13, 2007

Including pre-conference HSPD-12 workshop, 3 day conference, and over 50 exhibits

Each year, the Smart Cards in Government Conference highlights the exciting new advances in market adoption and technology innovation for smart cards in the government sector. **Don't miss this event!**

For details, visit www.smartcardalliance.org

WORLDWIDE OUTREACH



UNRIVALED EDUCATION



TASK FORCES & REPORTS



CONFERENCES



NETWORKING



Contactless hits Broadway with Visa payments in leading theatres

Andy Williams

Contributing Editor, AVISIAN Publications

Convenience continues to be redefined when it comes to contactless payments. The latest innovation: using wireless readers/terminals to take—and pay for—concession orders at a group of Broadway theaters in New York City.

Sandbar Concessions is one of the leading in-theater refreshment services companies on Broadway. The company is concessionaire for The Nederlander Organization, which serves the Brooks Atkinson, Gershwin, Lunt-Fontanne, Marquis, Minskoff, Nederlander, Neil Simon and Richard Rodgers theaters. It is also the first refreshment service company to accept Visa credit, debit and, now, contactless payments.

At the Minskoff Theater, home of Disney's *The Lion King*, Sandbar introduced "The Lobby Bar" on the main floor of the theater overlooking Times Square. The Lobby Bar staff is being equipped with wireless terminals that can accept both magnetic stripe and contactless transactions. This program is scheduled for introduction at other Nederlander theaters later this year.

"Concessions had previously been cash only. Now, with wireless terminals and readers, the consumer speeds through the whole process," commented Brian Triplett, Visa's senior vice president for emerging product development.

Theatergoers simply place, and pay for, their concession orders with clerks wandering the concession area utilizing wireless point-of-sale terminals from ExaDigm that accept contact and contactless cards. The paid-for order is then picked up at the concession stand, explained Mr. Triplett. As with most contactless

payments, no signature is required for orders under \$25. Regardless, customers can still request a receipt if they want one, he added.

"This brings whole lot of new things together for us. We're excited about our relationship with Broadway theaters, which we've had since 1999. We continue to look for unique and innovative places where we can put this (contactless) technology to work to drive value. Here, we're taking a cash-only environment and making it easier for the customers. It's a combination of a whole lot of things coming together, and it makes a lot of sense for both consumer and merchant."

For The Nederlander Organization, it means faster concession lines during the short intermissions and, of course, customer convenience.

Electronic payments also increase throughput and spending, and add to collection efficiency, inventory management and reporting processes associated with cash handling, Mr. Triplett stressed. Probably most important, shorter concession lines means more purchases since theaters have only a limited time to sell concessions, typically before the show and during the short intermissions.

While ticketing is a different operation, that may be something for Visa down the road. "At this point we're just focusing on this first launch at Sandbar," said Mr. Triplett.

Using Visa contactless at the theaters is just part of the "hospitality upgrades the theater has put together. They've opened a new bar area where patrons can watch the performance on plasma screens."

While Visa has a half-billion cards in use in the U.S., just seven million are contactless, said Mr. Triplett. "But well over 50% of consumers are starting to understand what's out there. (Contactless) is beginning to penetrate the consumer mind set."

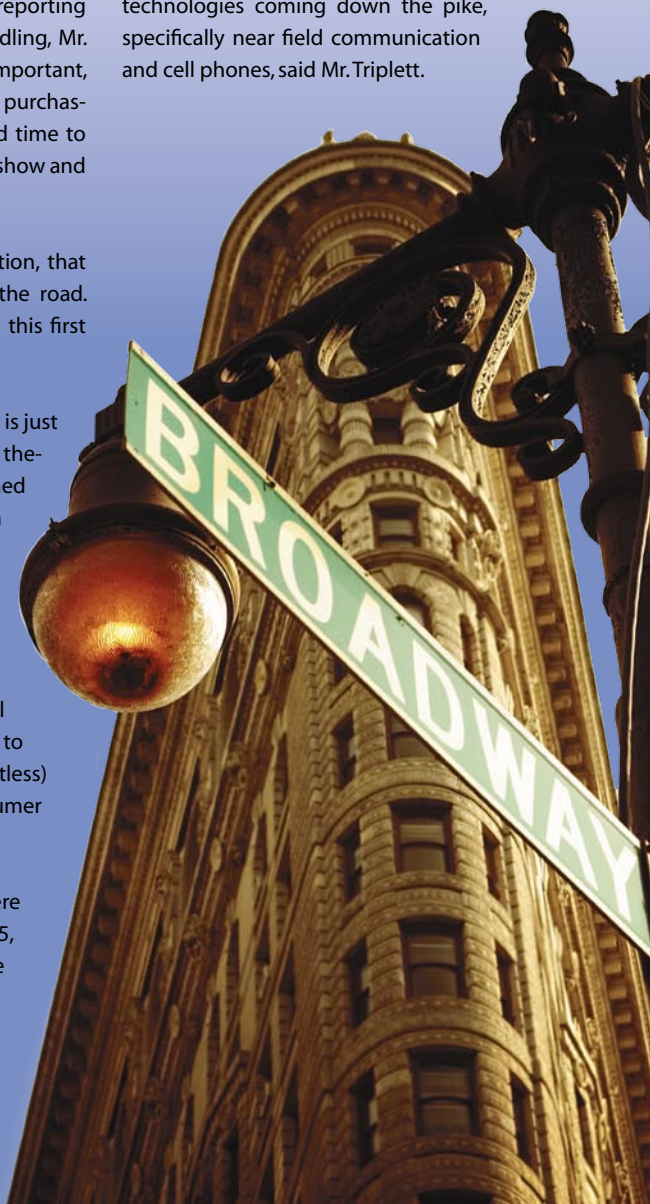
He added: "Two years ago, there were zero (contactless) cards. In June 2005, the first Visa contactless card hit the market in Atlanta." Before moving on, "we wanted to make sure we had a solid base of acceptance." It

helped with Chase, Visa's biggest issuer, "dropping" Visa cards in major markets, such as Denver, Colorado, New York, Dallas, Texas. "At the end of '05, we had 3,000 merchant locations. At the end of '06 we had just over 25,000. Now we're up to 30,000," he said.

And other issuers are coming online, such as U.S. Bank, Wells Fargo, "and quite a few more who are in the process of coming aboard," said Mr. Triplett. "Adoption by large scale issuers will drive the growth," he said.

Driving the contactless model specifically is recent Visa research that shows more and more consumers want to use a payment card for purchases under \$25 for convenience (73%), efficiency (44%) and speed (39%).

What 2007 holds "is continued growth," including adding cards and merchant locations, continuing to promote consumer adoption, and getting more involved in some of the new technologies coming down the pike, specifically near field communication and cell phones, said Mr. Triplett.



On Your Desk



On Your Desktop



The best ID technology resources are from AVISIAN Publishing and they are **FREE**.

Sign up today and get the up-to-the-minute news and insight you need to make informed business decisions. Visit www.regardingID.com/subscribe to get started.

AVISIAN

Sesames Award winners honored as year's best in smart card and ID technology

In its eleventh year, the Sesames Awards has become a key part of the industry's leading event, the annual CARTES smart card and identification conference. Sesames honors innovations and application achievements within the chip card industry. As 2006 was coming to a close, an international panel of judges active in the industry selected the individual recipients from 203 companies that applied for the ten Awards.

Software

Gemalto's IPv6 embedded stack took the Software category honors. The product provides enhancements in areas such as auto-configuration and built-in security for data protection and integrates the smart card into the network world via a high-speed protocol communication interface.

The winning product beat out another Gemalto product, the PC-Link. sim. It allows a Windows PC and the SIM card in a mobile phone to communicate with each other. It also bested Oberthur Card Systems' AngellC, a winner in the Mobile category.

Hardware

Infineon Technologies received top honors for its CC EAL 5+ certified Flash Chipcard Microcontroller that enables data to be stored on the card in flash-like EEPROM in a secure manner that is usually considered possible only via ROM.

Runners up in the Hardware category were Gemalto's GemBorder Inlay designed to increase the power yield between chip and reader for passports and ID cards, and INSIDE Contactless' Micropass L4, a chip designed from the ground up for contactless optimization and use as a multi-payment brand offering.

IT Security

The winner was SIM Strong from Gemalto, a product that leverages SIM-equipped mobile devices to provide secure access to online content and services. According to Gemalto, a user with a valid Identity Provider account and SIM-enabled mobile phone or dongle can securely log on to a host of online services such as e-commerce or the Intranet.

The other two finalists in the IT Security category were Ingenico with IngeTrust that secures communications between a terminal and its host computer, and Page International's ICS 2 Invisible Code System for securely sending PIN codes via the mail.

Banking/Retail/Finance

ASK took top honors here with its shielding media designed to protect data on contactless cards from fraudulent RF readings. The shielding also works with contactless paper tickets and e-ID documents such as e-passports.

Runners up in the Banking category were Gemalto's GemInstant Sticker containing a contactless chip and antenna that can be affixed to any device; MasterCard Worldwide PayPass M/Chip Flex allowing the issuance of OneSmart PayPass cards without updating the EMV infrastructure; and Way Systems' MTT5000 mobile POS device (a winner in the e-Transactions category).

Transport

French-based Let It Wave's CodeCID Transport won for its compression software that reduces the storage of high quality ID photos to as few as 500 bytes, taking up to three times less space on the ID card. It is intended for low capacity multi-application cards such as those used in transport, parking, access, etc.

Runners up were Ingenico's iPod-compatible payment terminal that allows users with a plug-in module to use their iPod to download tickets, etc., that can be read by a terminal and China-based Watchdata System's SIMPass, a mobile payment application that includes a contactless interface allowing for credit and debit payments and an e-purse.

Identification

Smart Packaging Solutions, France, and its E-Pastille with E-Booster, designed for passports, won this category. It includes a contactless module (the E-Pastille) made with a die and a small antenna that is embedded in the cover page of the passport but cannot work directly with the reader. Communication is done through a passive larger antenna, called the E-Booster, located on the data page.



Runners up included Adobe Systems' Adobe Acrobat 7.07 for Smart-Cards, which offers digital signing; Cross Match Technologies' L Scan Guardian that captures an individual's fingerprints, evaluates them and displays them on screen; and Datacard Group's Artista VHD retransfer color printing module.

Health Care

Actividentity and InterComponentWare Card Management System took this award for their German eHealth card solution, which includes a smart card to provide German citizens with a secure e-prescription service, allowing authenticated card holders to store and then reproduce their digitally-signed doctor's prescriptions.

Runners up in the Health category included: Dallas Semiconductor's Maxim Integrated Products/DS3600, a battery backup for POS terminals; Page International's ICS 2-Invisible Code System; and SCM Microsystems' eHealth 100, a smart card reader designed for the German health system.

Mobile

Oberthur Card Systems won for its AngellC solution that enables a mobile subscriber to plug a SIM USB key into his PC or laptop to place and receive calls from a PC soft-phone using the subscriber's mobile phone number. The product bridges mobile services with VoIP and messaging services and can be used by virtually any broadband connected PC.

Runners up in the Mobile category were Banksys' Pay2me, a mobile phone to mobile phone payment system; Sagem Orga's Phonebook New Generation which manages phonebook applications; and Watchdata System's SIMPass.

e-Transactions

Way Systems won for its MTT5000, the latest EMV/PCI certified mobile phone payment terminal with contactless capabilities. Its 32-bit processor allows it to meet the needs of individual merchants as well as larger companies in a wholly mobile way.

Runners up were Gemalto's ChipSwipe, a pocket handheld reader that protects against skimming by encoding a unique key generated by the chip onto the mag stripe prior to a transaction; Xiring's Xi-Sign 4500, an EMV authentication device for the visually-impaired; and Innovative Card Technologies' ICT DisplayCard that helps with online authentication by generating a random number.

Loyalty

Xiring of Suresnes, France, won for its Xi-Card Vida Bancomer, a smart card reader associated with the "Vida Bancomer" marketing program in Mexico. The reader allows each cardholder to check the number of coupons, loyalty points or cash bonuses earned while using his or her EMV payment

card at participating merchants. The Xi-Card is aimed at accelerating the adoption of the EMV payment card in Mexico.

Runners up included YesPay International's Real Time Service for Business Intelligence, which helps manage a retailer's POS, inventory and other business systems; and Gemalto's FireFly, which provides an on-card light source that is powered by the reader's RF field and can be used to add special effects to cards (e.g. the issuer's logo lighting up).

The 12th edition of the Sesames awards will be presented this year at CARTES, November 13-15, 2007, in Paris, France.

Over 10 Years Experience in Contactless Card Manufacturing



cpi card group™

1.800.446.5036

contactless@cpicardgroup.com

www.cpicardgroup.com / contactless

An ISO 9001:2000 registered manufacturer

PricewaterhouseCoopers uses multifunction LEGIC technology for security, print management, and more

Andy Williams

Contributing Editor, AVISIAN Publications

When PricewaterhouseCoopers (PwC) went from 13 different buildings down to one at its Zurich, Switzerland office, many of its 1,200 employees were using different ID cards providing only limited uses. So why not switch to one multi-function card?

That's what the company went searching for. "We've always tried to look for state-of-the-art systems and we found this card," explains Corina Gerber, facility management, senior manager, for PwC Switzerland.

This card Ms. Gerber refers to contains a chip manufactured by fellow Switzerland-based LEGIC Ident systems that handles everything the company needs with room for expansion.

Called an "all-in-one" card, it's not new. Actually, it has been around about 10 years, said Bob Fee, general manager, Business Unit, for LEGIC in North America. But with the demand for more applications on one card, a multi-function type card is starting to come into its own.

PwC's applications include building access, print management, an e-purse for cafeteria usage, garage and elevator access, and more, said Ms. Gerber.

For the time being just the Zurich office has the new card. "We moved into the new building about a year ago. Before that we had 13 different buildings. Just from a logistics (point of view) it was not working out correctly. We all moved under one roof in November, 2005, and had to design our own solutions for our cards," said Ms. Gerber.

Secure document management provides a key application

PwC is a professional services firm best known for its auditing and accounting capabilities. One of the biggest demands the company had for its card is what Ms. Gerber calls "follow me" or "follow&secure" printing. Obviously a company dealing with tax returns and other sensitive data doesn't want documents spit out by one of the company's 60-plus multi-function printers/faxes/scanners just lying around until the person who sent the documents to the printer shows up to claim them.

"Secure means you have to physically go to the machine and, using your badge, release your documents," said Ms. Gerber. "You always have things you don't want lying around. You have the whole Human Resources department that prints out things such as salary schedules. This was one functionality we needed."

With "follow&secure," the job is sent to the printer, but it's not printed until the document's owner shows up at one of the company printers



and flashes his card to the machine. That unlocks the printer and the job, which has been stored in a queue. Once the printing is finished, the person puts in his card again, which locks the printer.

The "follow" aspect of the solution is that the print job can follow wherever you happen to be.

"We have about 62 machines in the building and I can use any of these machines. I have my office on the first floor and I may have meeting on the fifth floor. That makes it very convenient. I don't have to go to a particular printer. I can use the one on the fifth floor," said Ms. Gerber.

"It's also a cost factor," she added. "We used to have printers and copying machines. Printers aren't that expensive, but maintenance of copiers can be quite high. With the multi-function devices, costs are quite lower. We can print, scan, copy, and fax. Scanning is really great. You go there with your badge, and once the device knows it is you, you put in the papers to be scanned and within one minute it's in your mailbox."

Access control via contactless and biometrics

Physical access control is another key component of the card. During normal business hours, only the employee's ID badge is needed to gain access. "But after hours and on weekends, we go to biometrics," specifically a fingerprint, said Ms. Gerber. The fingerprint template, added Mr. Fee, is stored on the 1 kb contactless chip.

Employees have to use a separate entrance in this case, where they have to produce both their badge and their finger. They then enter through a turnstile-like door that allows just one person in at a time. That, of course, prevents one employee from letting in several others with his badge and fingerprint.

Nothing's perfect, however, so PwC also has 24-hour security in place as well, she said.

"When biometrics was first introduced, we thought maybe employees wouldn't want to give us their fingerprint. But it's just to gain access and it only covers five points. It's not like the fingerprints police take. It's the lowest type of fingerprint," she added. "So nearly all of our employees gave us their fingerprint."

The smoothness of the transition to the new system was brought about by "all the communication we did with our employees before we moved into the new building. We showed them what we intended to do with biometrics and how it works and how the multifunction devices would work," she said.

PwC has offices in 149 countries; and some 140,000 employees. "In Switzerland, we have about 2,500 employees in 14 offices and 1,200 employees at the Zurich office," she said.

Different vendors, different applications, but a single card ...

"What we're trying to make people understand," said Mr. Fee, "is that different applications from different vendors doing different things can be stored on the card and be totally independent of each other. We have 50,000 customers. About half of them use more than just one application, usually two or three on average," he added. The applications, like PwC, include access control, cashless payment, time and attendance, and the follow and secure print concept.

"About five LEGIC partners offer the 'follow me print' application. This particular application is being sought after more and more," he said.



What PwC is utilizing on its all-in-one card is just the tip of the iceberg. German automaker BMW, serviced by LEGIC, "has 17 applications on their ID card. Airbus has 12," said Mr. Fee. "They're actually saving money because they're using one card and it gives them more flexibility."

The 13.56 MHz frequency LEGIC contactless smart card uses encryption in the transmission. Data from the different vendors are encrypted from reader to the card and also on the card itself. "It provides a higher level of security. If a person loses the card there is nothing that can be accessed," said Mr. Fee.

In fact, added Ms. Gerber, anyone finding a lost card won't even know that it's from PwC. There is a separate company name (Interlock) on the back of the card, and a telephone number. People can use that as a means of returning the card.

"We chose the name of the company which makes the card," she added. "It's a card maker here in Switzerland that we use." When the card is lost, she said, it's locked out of the system, but the money in the e-purse portion of the card is gone. Employees can load about 100 Swiss francs on the card that is usable in the company's cafeterias or vending machines.

Originally, PwC had an ID card with no functions on it. "It was just a card that showed you were working at PricewaterhouseCoopers," said Ms. Gerber.

While the Zurich office was the first with this type of card, other PwC offices are starting to come on line. "Geneva is starting up with the multi-function machines. We have to provide a card so an employee in Geneva, when he comes to the Zurich office, can still use the same card. Geneva is the first that has started doing this, but we're working slowly with other (PwC) locations," she said.

However, these cards carry only building access capabilities and aren't yet all-in-one cards, she added.

From Zurich to the PwC world?

Ms. Gerber estimates that each card produced by PwC costs about 10 Swiss francs, but that includes the cost of the machine as well. "We produce our own cards for obvious security reasons," she added.

Added Mr. Fee about the all-in-one card installation: "We relied on our partner network who did the installation and integration. We acted as a consultant and helped them understand how best to use the technology. We provided the oversight, the RF module and the transponder."

He cited the PwC installation as "an excellent example of how an organization can utilize an all-in-one card. It reduces costs, increases security and gives them the flexibility to do more down the road ... to use technology to enhance the organization. They can easily add or remove applications a year from now or five years from now. We've had customers using the technology for the last 15 years. It's very secure and very flexible.



Visa and MasterCard on your campus ID

Instant issuance solutions like CardWizard let campuses produce branded plastic

Chris Corum

Executive Editor, AVISIAN Publications

If you have a bank-issued debit card in your wallet, chances are that it has a MasterCard or Visa logo on it. But if you have a campus card with a bank account attached, odds are it does not. More likely you will see ATM network logos like Pulse, Cirrus, or Maestro. A major reason for this is that students need the ID card the day they get to campus but you can't just print a MasterCard or Visa card from your card office ... or can you? A growing number of campuses are doing just that and it may well be the wave of the future.

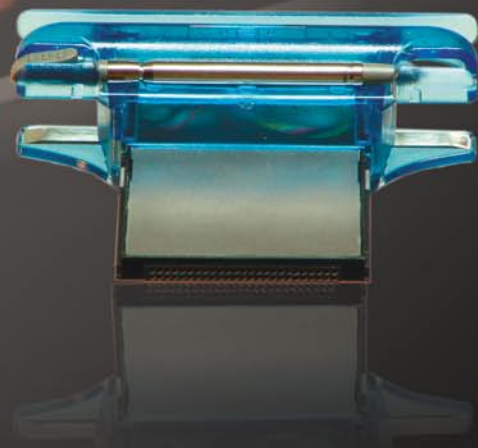
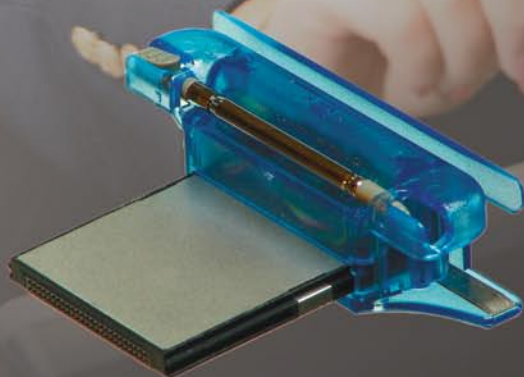
One of the long-standing "truths" of the campus card market was that campus card programs require instant issuance but the card associations, specifically Visa and MasterCard, prevent instant issuance of their branded products in an effort to combat fraud. The association requirements dictated high security printing environments and strict blank plastic management processes that made it all but impossible to print cards on campus or even within a bank branch. Branded cards came from fortress-like printing facilities with clean rooms, man traps, and armed guards.

But something changed a few years back and that change is rippling through the campus card industry. The rules governing card issuance eased enabling branded cards to be produced under less stringent conditions.

Today, many bank branches are issuing debit cards to their new customers and replacing lost or stolen cards for existing cardholders on the spot ... and some campus card programs with bank partnerships are along for the ride. Campuses in North Carolina, Wisconsin, Michigan and Colorado are paving the way, providing library and mealplan functions on the same piece of plastic as global branded debit card services.

A solution called CardWizard from Englewood, Colorado-based Digital Card Solutions has been a key player helping financial institutions and campuses make it happen. According to the company's Vice President of Sales, Ron Zanotti, it can be done with very little disruption to the current student badging processes.

'Look Ma, No Wires'



The DigiSwipe™

The DigiSwipe™ 3-Track CompactFlash Magnetic Card Reader transforms a Pocket PC or Windows XP Tablet into a mobile Point of Sale or ID Security terminal. Create applications which read credit cards, student IDs and drivers licenses for Pocket PCs, Laptops or tablet PCs.



Affordable. Portable. Flexible.
Solutions by TokenWorks®.

For more information please visit us at:
www.tokenworks.com/digiswipe.htm

How does instant issuance typically work on campus?

"Our implementations follow the same process flow through badging," he says. "The only difference is that when (the student) engages with the banking representative they get a different card selected in the system and it is routed to a different printer."

That different printer is stocked with blank plastic cards with the Visa or MasterCard logos and embedded security elements.

The card is printed with the elements sent from the normal campus card production system. This can include elements such as digital photo, cardholder name, ID number, library number, etc. The magnetic stripe is also encoded with the same data as the normal (non-branded) campus card.

At this point, the card is really just a campus card printed on branded card stock. But from here, the process changes for the branded version. The card is transferred from the standard card printer and fed into the embossing unit.

It reads the data encoded in the magnetic stripe and uses the ID number to call for information from the bank's card issuance system. From the bank system, the data elements required to make the card a compliant, readable, branded debit card is obtained. The magnetic stripe is then rewritten with the new data – or a combination of the old and new data.

The cardholder name, account number, and expiration date are embossed on the card and it is ready to go.

The offset PIN, an encrypted version of the cardholder PIN, is written to the magnetic stripe during the final encoding process or in a subsequent customer self-selection.

Security remains a major focus

Mr. Zanotti stresses that the instant issuance rules still require extreme caution and strict control over blank card stock and system access. "Dual control procedure that are currently used for other cash like conditions" are required when dealing with card stock. Two people must count and sign for the stock when it is received and locked up, when it is moved from inventory to the printer, etc.

Pioneering campuses instant issue Visa / MasterCard

The first implementation of instant issuance on campus occurred in 2002 at the University of North Carolina Chapel Hill. Wachovia Bank is the financial partner for the UNC One Card Plus, combining campus card functions and Visa check card offering.

In 2005, Wachovia made the same program available for the University of North Carolina Greensboro and Mercer University.

Oakland University in Rochester, Michigan, partnered with Credit Union One to issue the MasterCard-branded version of its campus ID card beginning in 2005. The 18,000-student campus selected Credit Union One.

In the Fall semester of 2006, Ent Federal Credit Union began issuing Visa branded cards for the University of Colorado at Colorado Springs' campus card program and the university's 7,800 students and 1,000 faculty and staff.

This spring, U.S. Bank will launch its first instant issuance program offering Visa-branded cards at the University of Wisconsin Eau Claire.

But this responsibility falls not with campus staff but with bank staff. "When we send it to the printer that has the Visa/MasterCard stock," says Mr. Zanotti, "(that printer) is located in the bank branch." Indeed all the processes associated with the branded card issuance and account setup are typically handled by bank personnel.

But while the personnel remain bank employees, the facility where production occurs may not always be the on-campus branch. U.S. Bank will begin issuing a Visa card at the University of Wisconsin Eau Claire campus this spring but the bank does not have an on-campus branch.

According to a U.S. Bank representative, with prior instant issuance campus programs, the student is instantly issued the card, but still has to go to the branch to have the card activated before being able to use it. "With the U.S. Bank program, the account and card are instantly issued and activated at the card office and in the U.S. Bank card system so the customer can walk out of the card office and go right to the ATM or a merchant and begin using it."

Campus cards using instant issuance

While only a handful of campuses have made the leap to instant issuance to date, Mr. Zanotti stresses that his company's solution is very well established. "We have just landed our 300th financial institution customer." On campus, at

least six campuses are on board with instant issuance and, to date, all campus projects are relying on the CardWizard solution from DSI.

The wave of the future?

CardWizard has already worked alongside many of the major campus card systems. "We have done the major ones out there," adds Mr. Zanotti, "CBORD, Blackboard, General Meters."

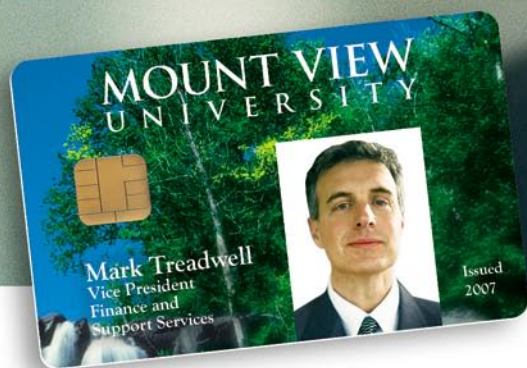
Costs for the solution, while not insignificant, seem reasonable when the total cost of a financial partnership is weighed. The additional hardware required consists of a separate photo ID printer, the embossing unit, and some peripheral devices (e.g. PIN pad, standalone PIN encoder). Mr. Zanotti estimates the hardware investment at \$15,000. Software fees are largely determined by the amount of customization required to integrate the instant issuance solution with the campus and bank issuance systems. He estimates \$25,000 as the upper end of a typical installation.

The investment makes sense for the financial institution, he suggests, because "the money in ATM transactions is largely gone. Banks make money on signature-based Visa/MasterCard transactions."

"It's the only way to go," says Mr. Zanotti, commenting on the future of branded campus cards, "because it really adds more functionality to the card."

I want a campus
card program that:

*ENHANCES
OUR REPUTATION*



Mark, Campus Card Programs Director

Fargo High Definition Cards™ reflect your school's outstanding public image.

Whether you issue photo IDs or multi-function smart cards, Fargo Card Identity Systems deliver.

Our exclusive **High Definition Printing™** technology produces campus cards with the highest image quality available. You get cards that enhance your school's reputation by looking great and lasting for years. Plus, you get reliable, affordable and efficient card issuance.

Contact us today and get your FREE guide that shows you how to unlock the potential of your ID cards. Visit www.fargo.com/freeguide or e-mail us at freeguide@fargo.com.



*Only Fargo Card Identity Systems produce the
High Definition Cards that your school deserves.*

FARGO®

The World's Most Secure
Card Identity Systems



Philadelphia's sixty high schools issue contactless campus ID cards

Access, attendance tracking, lunch programs drive the implementation provided by ScholarChip

Andy Williams

Contributing Editor, AVISIAN Publications

Colleges have been using campus card ID systems for years. But with increasing security concerns, similar products are moving into public schools. One example: Philadelphia, Pennsylvania's school system where high school students at 60 schools have been provided a contactless ID card needed to gain admission to school property, track attendance, and, in some cases, buy lunch in the cafeteria.

"We have 56,000 high school students and we wanted a better handle on (them)," said Patricia DiLella, senior project manager for Philadelphia School District's Office of Information Technology. "Before, everyone was assumed present until marked absent. We needed something to track students. With this new system, everyone is assumed absent until they tap (their card) and have physically been seen by school personnel."

Via a request for proposal process, the district selected ScholarChip Card, LLC, a seven-year-old organization whose origins date to higher education and has since incorporated K-12 schools in its lineup. While ScholarChip had been conducting a pilot program in two of Philadelphia's middle schools, it landed the five-year contract because it had "better technology, ease of implementation and cost," said Ms. DiLella. "It was state of the art and they had experience with smart cards in universities."

"We spent a year and half doing evaluations in the pilot program (with the middle schools)," said Dr. Maged Atiya, ScholarChip's founder and chief technology officer. "We've provided a contactless card (using NXP's MiFARE technology) to every high school student in the district."

Ms. DiLella added that the district, Pennsylvania's largest, was "in the process of implementing the system in three large middle schools. We concentrated on high schools first because they needed it."

Students are encouraged to wear the lanyard-attached badge around their necks, however, many are still simply carrying them on their persons, said Ms. DiLella. "We want them to get used to wearing the cards because they're going to be used (eventually) for classroom attendance."

The smart ID badge is tapped when a student enters school grounds. Attendance is taken in a classroom in the normal fashion and the results are compared with the records generated when the students first enter the school. In addition, the badges can be read by portable, PDA-style readers. So, if a student is in the hallway, the badge can be read by an administrator to determine where the student should be.

To accomplish this, the card contains the student's picture and also his class schedule. Other information can be added, such as any special health needs and whether he's on free or reduced lunch, which can be read by a POS device in the cafeteria.

The next step is implementing electronic attendance at the classroom level. She said some schools would like to put readers in classrooms so students can walk by, thus registering their physical attendance in the class. But that's not something the district is looking at as a whole because it's expensive and would require readers in each classroom.

"The (first) challenge is making sure teachers have computers," she said. "If a child is marked as tapping in (when he first enters the school) when the teacher gets to her class for the day, it shows he's present." She then manually identifies that the student is in the classroom. If he's not, a notation is made on the computer.

"We opted right now not to have devices hanging on the door," she said. Inevitably, they would be subject to vandalism. "So the teacher will be doing it. This system does help tremendously in finding kids and keeping track of them."

Eventually, the POS system in the cafeteria will be able to have the food service portion on the card and ultimately an e-purse. But right now it just notifies cafeteria personnel that the child is eligible for free and reduced lunch, said Ms. DiLella.

In, the technology-savvy Microsoft School of the Future in Philadelphia, the cards are also used to open lockers. "I don't think it will be implemented at our other schools anytime soon," she said. It would require either upgrading the lockers or, more likely, installing new ones, which is an expense the district isn't willing to undertake at this point.

Each school issues its own cards. "The school can queue a card and print it or we can print it at our data center," says Dr. Atiya. "It's all up to what the school wants to do. (It is a major) implementation of distributed smart card issuance and printing. We have almost 70 printers in the field."

The printers from Evolis are customized to encode the contactless chip during the print cycle. According to Dr. Atiya, as the blank card is physically printed, a unique digital ID is added to the card that contains the student's schedule data, emergency information, cafeteria e-purse, etc.

"Our approach is ideal ... for large urban school districts," adds Dr. Atiya. "We installed 300 devices in Philadelphia inside of five weeks. That's because of the architecture of our system. Everything is self-configurable."

It seems that the Philadelphia experience supports his claim. "The technology is unbelievable," Ms. DiLella said in rating the overall system. "We implemented in 59 schools in six weeks. That's unprecedented. ScholarChip was out here helping them with training and helping us get more accurate data. Now we're able to assist schools manage and keep accurate attendance records."

The printers from Evolis are customized to encode the contactless chip during the print cycle.



Contactless ready to make its mark on campus

Kieran J. Timmins, CEO

SmartCentric Technologies International Ltd.

Although the advantages of a highly secure card for multiple applications on a single platform were obvious, for many the perceived costs of implementing a smart card system outweighed such advantages. In 2006 there was still a lot of misinformation and misperceptions about smart card systems versus magnetic stripe and even proximity. We still see two basic arguments being put forward against smart cards:

- Online magnetic stripe systems provide sufficient security; and
- Cost, complexity, 100% offline operation and support of systems into the future are common misconceptions.

In 2007 we will finally see these arguments addressed with increasing deployment of contactless card technologies: technologies that allow you to have smart cards without the cost.

In addition to offering a cost effective solution for card programs, contactless smart cards offer the end user not only security, but also speed and convenience. A tap of a card on a reader can allow a cardholder to pay for meals, buy a book, enter a secured area or log on to a computer network. For areas requiring higher security, biometrics can be added to ensure higher levels of authentication for restricted access. In other words, a single secured card offering multiple applications.

Gone is the "all or nothing" approach which was needed to make the business case work for smart cards. In 2007, the cost of contactless technologies will allow campuses and businesses to deploy a smart card for a single application or in combination with other card types.

As the market moves towards contactless cards, it will be important to offer customers a simple migration path for existing contact chip, proximity, and magnetic stripe applications. This reduces the impact and the costs, offering the best solutions to accommodate many different environments. Some customers may like to use contactless chip cards for physical access and small purchases, but may still prefer to use contact cards for biometric logical access, and their existing magnetic stripe access application for some buildings, or even a meal plan.

Changing over to smart card systems does not have to be complex or expensive and can be phased to suit requirements and budget. As smart card systems continue to advance and deliver value using contactless cards able to support a wide range of applications simultaneously, user uptake will increase and the result will be positive for the card issuers and cardholders alike.

SmartCentric in early 2007 introduced the next generation of its SmartCity platform supporting contactless technologies, TCP/IP and WiFi technology integrated into card readers and devices to allow for remote / online data collection, Web portals and an easy migration path.

Biometrics gets its 'fingers' into school foodservice and other campus environments

Ryan Kline

Contributing Editor, AVISIAN Publications

The use of biometrics for identification and authentication is taking hold throughout the country and in our schools.

Way back in 1972, far before many people were even thinking of using biometrics in conjunction with daily authentication, the University of Georgia began using biometrics in their dining halls. The campus had decided to simplify their mealplan offerings—from a ticket-based program to an enrollment program—and they needed a way to accurately identify paid customers. The same goal of simplification remains a core motivator when colleges, universities, and K-12 schools decide to use biometrics in their facilities.

Biometric identification is not a new concept. "The ancient Egyptians used bodily characteristics to identify workers to make sure they didn't claim more provisions than they were entitled—just like governments today are looking at biometrics to lessen benefit fraud," says Jay Fry, CEO of biometric developer, identiMetrics. And just like the University of Georgia has been doing for years.

Lower costs and increased accuracy has many school administrators looking to biometrics as means of authenticating students. According to Mr. Fry, "price is no longer an obstacle ... Today, biometrics can actually be priced competitively with barcode readers, swipecard (magnetic stripe) readers and PIN pads."

Though the number of schools utilizing biometrics is not known, Mitch Johns, CEO/President, Food Service Solutions, reports that his company has 65 school districts using their solution.

Bud Yanak, VP Marketing, BIO-key International, stresses that the advantages of biometrics far exceed those of other authentication techniques.

CR80News spoke with the three men in an effort to determine the state of biometrics in college and university as well as K-12 settings. Both are convinced that biometrics hold the key to solving the challenges of authentication in campus environments.

An interview with Charles Yanak, VP Marketing, BIO-key

What advantages do you think there are with a biometric system?

First, convenience ... With biometrics, there is no need to remember a password or carry an ID card. You simply place your finger on a biometric reader that takes a picture of your finger, digitizes it and then compares it against a database of templates. For students, this is a major plus, since it eliminates the need to constantly be replacing lost or stolen IDs and it eliminates the possibility of sharing ID cards.

Second, security ... Biometrics are far superior to current passwords/PINs and ID cards identification techniques for establishing identity. It's very easy to "share" a password or PIN with someone and worse yet, they are easily forgotten or unknowingly obtained by someone looking to access your personal records or assume your identity. In the campus environment, biometrics can help eliminate:

- "Buddy punching";
- students logging into systems using a teacher username and password to access protected information,
- identity theft.

Is this a cost effective strategy to implement in schools?

Definitely ... The cost to deploy biometrics has gone down significantly. Three years ago, the average cost of a fingerprint reader was over \$100. Now, they are included in most new laptop computers. External USB readers cost less than \$40 today, one-third the price they were two years ago. The cost to deploy a fingerprint biometric system is far lower than the costs to issue and manage ID cards and passwords.

"More and more schools are considering doing away with ID cards and using biometrics in the lunch process."

— Mitch Johns, CEO, Food Service Solutions

"Price is no longer an obstacle ... Today, biometrics can actually be priced competitively with barcode readers, swipecard (magnetic stripe) readers and PIN pads."

— Jay Fry, CEO, identiMetrics

"Biometrics ... can improve your privacy since it can virtually eliminate or substantially reduce unlawful/unwanted access to your private information."

— Charles Yanak, VP Marketing, BIO-key



Why do you think so many people are afraid of using such secure technology?

Great question. There is still a lot of misinformation about biometrics and "Big Brother" concerns. The reality is we all use biometrics every day. Biometrics are defined as the ability to recognize someone by their physical attributes. You intuitively use biometrics when you pick up the phone and recognize the voice at the other end, or when you meet a friend on the street and recognize their face.

However, people are concerned about how biometrics can be misused with "Big Brother" being able to track your every move. Banks, retailers and other institutions store and track a lot of information about us every day. Biometrics can protect access to this information! With biometrics deployed to access this information, our lives would be safer, since they would reduce or eliminate unlawful acts such as identify theft. Biometrics provide better security and confirm who has access to critical information and can improve your privacy since it can virtually eliminate or substantially reduce unlawful/unwanted access to your private information.

What sort of stereotypes can biometrics eliminate in the lunchroom?

Another great question. When two students are traveling down the lunch line side-by-side, they look identical to the system. When they get to the cashier, they both place their fingers on the reader to establish their identity and the system electronically debits their account. One of these students may in fact be buying his lunch with government aid. (With biometrics, there is no) negative stigma among peers. Another example ... very young students often forget or lose their ID. With biometrics, the lunch line flows faster and eliminates the embarrassment when the student discovers he has forgotten or lost his ID or password.

An interview with Mitch Johns, CEO, Food Service Solutions

Have parents expressed apprehension to using biometrics with children?

The association with fingerprint-based biometrics is generally associated with law enforcement. AFIS systems store actual fingerprints while commercial applications only store a numerical template of the enrollment scan. Post 9-11 events—including the Patriot Act and war on terrorism—have elevated concerns among Americans over the loss of privacy. Using Opt In or Opt Out at time of implementation gives parents a choice.

POCKETTRACKER
POWERED BY **VISIONBASE**

- 1 Scan any ID card
- 2 Retrieve photo and data
- 3 Permit or deny entry

Eliminates data integration headaches. Connects to any ODBC compliant database wirelessly or in offline mode. PockeTracker handhelds are great for **mobile security guards**, **tracking attendance** at events, quickly **identifying absentees during emergencies**, and **tallying loyalty points** for event incentives.

Multiple Scanning Technologies

Contactless Barcode ID Card

Come See Us:
ISC West • Booth 22117 • Las Vegas • March 28-30, 2007

Visit us online at www.visionbase.com or call 1-800-951-2357

What do you think the future holds for identification at schools around the nation?

More and more schools are considering doing away with ID cards and using biometrics in the lunch process. Schools are currently testing or using biometrics and GPS for tracking bus attendance. As security becomes an even bigger issue for schools biometrics will be used for door entry and attendance.

An interview with Jay Fry, CEO, identiMetrics

What about privacy issues?

Biometric technologies don't conjure up the Orwellian fears they used to. In fact, people are now realizing that biometrics actually protect their privacy and that in many biometric applications their fingerprints are not stored anywhere and their fingerprints can never be recreated from the digital template. Minutiae based systems, like ours, use flat images to create templates. Flat images reveal the center of the finger and require only a minimum of unique identifying points in order to make a match. The purpose is to identify a person already enrolled in the software. Fingerprints can never be recreated.

Why would a school use biometrics?

Quite simply, to save time and money, and to improve the accuracy of reporting. Biometric technology can provide benefits in terms of convenience, safety and security. There are two areas of identification that schools have to manage: students and employees. Biometrics are beginning to be used in both of these areas.

In some schools, teachers, staff and employees (use biometrics) for time & attendance, making record keeping very accurate. It can be used to identify people that come into the school on a regular basis, like substitute teachers, contractors, parents, so you know who is in your school and when they left.

Biometrics can be used to identify students as well. The cafeteria is usually the first area in the school to embrace biometrics. With up to 80% of students forgetting or losing their cards on a daily basis or forgetting or sharing their PINs, lines are slowed and mistakes are made. Biometrics will be used:

- in vending machines to ensure positive identification of children eating free or reduced lunch
- for attendance to eliminate “buddy punching” and provide irrefutable proof of attendance and help cut down on “class cutting” when attendance is taken on a period-by-period basis
- in the library to checkout books
- in the nurse’s office to make sure that the students are receiving the correct medication.

How do you begin to implement biometrics on campus?

Start by making small improvements. You want to improve productivity, record keeping and, of course, safety. Take baby steps! Identify and assess your “pain.” Where in your school could the use of finger scanning instead of cards and PINs save you time and money? We have found that in most schools it’s in the cafeteria.

Why the cafeteria?

About 65% of purchasing that is not facilities-related in schools is done by food service departments. Food service is a business, and it needs to run efficiently.

There’s a growing interest in the use of biometrics for student ID in school cafeterias nationwide. By just about every measure, finger scanning biometrics outpace other options for efficiency and ease. When a child presses a finger into a scanner, there’s no doubt about his or her identity. There’s no risk of lost ID cards or forgotten PIN numbers. There’s no chance of fraudulent use of the child’s meal account by someone else. Biometric ID also provides anonymity and eliminates any stigma for the children who receive free or reduced-price lunches, (therefore increasing) participation in the National School Lunch Program. And increased participation can translate into more funding for districts.

Another key area of focus is healthier vending. Instead of going to the cafeteria, a student can purchase a prepaid, reimbursable meal from a vending machine. The machines being tested are tied into a point-of-sale system, and they can track the purchases to prevent a student from buying two lunches on the same day. And biometric finger scanning will ensure accurate record keeping – a must for federal and state reimbursement.

Any concluding thoughts for institutions considering biometrics?

Cost-effective biometric technology is here today with practical uses for schools. It’s a perfect solution for schools who are dissatisfied with the current student identification systems in place such as PINs and swipecards. Biometrics, and in particular finger scanning systems, provide irrefutable proof of identification. Unlike the complicated and expensive government systems in the past, biometric finger scanning systems can be simple, cost-effective and technology friendly. If children can do it, you can, too. It’s just smart business!

What should a school think about when choosing the right biometric solution?

Jay Fry, CEO, identiMetrics, provided this checklist for institutions evaluating biometrics for use in their foodservice or other campus applications.

- Choose a biometric identification platform that can eventually be used throughout your entire school. This means that students should be enrolled only once to be identified in a variety of areas in the school – the cafeteria, the front door or classroom for attendance, the nurse’s office, the library and the office for absence information entry. It’s just impractical to expect a principal to disrupt the entire school to enroll the entire student body for each application that requires student identification.
- Make sure that it can scale if needed. Some biometric technologies work great with ten students or less in a standalone environment, but fail miserably as the number of students increase in a networked environment. A more robust biometric technology might cost a bit more, but will be worth it in the long run.
- Make sure that it can integrate with your software applications that you already have in place, if you don’t want to replace them.
- Ask about performance accuracy. There are basically four metrics: false acceptance, false rejection, failure to enroll and failure to acquire rates. False acceptance rates are what you should be most concerned about. That means I place my finger on the scanner and your name comes up.
- Compare, but not just on price. Check up on customer support and rollout experience. Once again, make sure the technology works in a practical school setting and not just in a vendor lab.
- Communication, communication and communication! Make sure everyone—parents, teachers, students, administrators, the school board and the media have up to date and accurate information about biometrics. identiMetrics has a “Guide to Implementing Biometrics” that includes, for instance, sample letters to parents, biometric FAQs, best practices and other important information to make the whole process run smoothly and easily.

Using cellular telephones to make campus card payments

John Diaz, Vice President, Product Development
Sequoia Retail Systems, Inc.

Institutions are doing a fantastic job of making their campus card the preferred choice for making payments for goods and services, and in 2007 students, faculty, staff and other campus constituents will continue to push administrators for even more choices in where and when they can use their funds. Many institutions have already taken big steps toward providing anytime, anywhere access to their campus card programs through the use of PDA style devices that connect to the wireless infrastructure throughout campus. We see this trend continuing to grow in 2007.

Because of the benefits realized by using the wireless PDAs on campus, we expect that in 2007 there will be a push from another group of users who may not always be able to connect to the campus wireless network. This group includes a number of truly mobile operations such as shuttle busses, food delivery services and taxis that serve the campus community and would also greatly benefit from access to real-time campus card transaction processing technology.

Although many cities are now setting up wireless hot spots in their downtown areas, it will likely be a number of years before this becomes the norm. Meanwhile, mobile merchants will need a way to process transactions while serving customers located both on and off-campus. In order to accommodate this, we envision that campuses will begin using cellular phone technology to bridge the gap and provide real-time transaction processing capabilities for these vendors regardless of where they are located. Because these merchants may have the need for literally dozens of card reader units, it will be important that they be provided with not only a robust solution, but also a cost effective one.

To the advantage of the campus card industry, there have been numerous advances in this area not only for use by merchants, but also consumers. The time is right for expanding the acceptance of campus card payments beyond traditional boundaries and we expect this and other technological developments to make 2007 another year of innovation in the campus card marketplace.

Video Surveillance and Campus Cards: A Total Security Solution

Read Winkelman
The CBORD Group, Inc.



Video cameras are becoming increasingly common on college campuses. It is now estimated that more than half of junior high and high school students attend a school with one or more security cameras. We are becoming accustomed to being monitored.

As the role of campus card systems changes and grows in light of new technological innovations, access control and video surveillance will become increasingly ingrained in purchase decisions. Already, we have seen headlines about criminal cases solved on college campuses with the help of card system software linking cardholders to specific locations at specific times. Campuses are now starting to use the software to back this up with video footage of card usage, and tracking of security events that send alerts to the system, both of which allow security officers to follow cardholders' activities from one location to another.

When CCTV (closed-circuit television) and DVR (digital video recording) equipment is integrated with a campus card access system, the result is a powerful, flexible security solution. The systems work together to provide video capture of events detected by security features in the card system, as well as playback and monitoring of video records of those events. This software integration goes beyond simply monitoring activity. It allows campus administrators to react quickly to events as they occur, as well as track the events that precede and follow them.

For example, at North Carolina A&T State University, the school's campus card system is tied to a centralized monitoring station with eight DVRs networked to almost 150 cameras located throughout the campus. When an event is triggered in the campus card system within view of one of these cameras, live video can be pulled up on the screen. This enhanced security system provides students, guests, and staff a sense of comfort and strengthens police operations.

As security becomes increasingly important for administrators, students, and parents, any auxiliary system on-campus that can be used to improve safety will be called upon to do so. What this holds for the future of campus card technology is new and better integration between campus card systems and surveillance technology, as well as more alarm and security management features within the software itself. (And a better night's sleep for campus security officers.)



RFID leaps from the warehouse to the art museum

Galleries are tagging collections to improve inventory control, security, and the total customer experience

Ryan Kline

Contributing Editor, AVISIAN Publications

After leaving a museum, you may think you are an expert on everything from painting to sculpture, but there are a lot of artifacts that you passed right by. It wasn't that you went too fast and skipped over some unattractive pieces, many of the items you missed were out of sight, behind the walls in storage.

When the museum needs to find a particular piece of artwork for a special exhibition or to loan to another museum, the piece has to be manually located by searching the museum's—often vast—acks and storerooms.

Many museums utilize a barcode system to identify their collection's contents, but some feel an RFID tracking method works better. Why?

The ability to read multiple tags at one time

This cuts down on labor costs required when physically scanning every artifact the museum has barcoded. With an RFID reader, one scanner can read all items within a short distance. Reading 20 or more paintings stacked in a storage drawer at one time, significantly reduces the time it takes to make sure everything is accounted for. It is estimated that one individual could record the exact location of 10,000 pieces in about 2 hours.

"No touch"

"The one key advantage of RFID over any other identification technology is that pieces can be identified with no physical contact whatsoever, even when they are stacked, and the identification tag is not visible,"

said Bartek Muszynski, President of Canada's NJE Consulting Inc., an RFID system integrator and consultant. "Yes – a barcode can be read without physical contact, but would be an eyesore if it had to be exposed with the piece, and of course, cannot be read in a stack." With RFID technology, the transmitter can be read through most protective sleeves or cases housing the masterpieces. Mr. Muszynski adds, "RFID can significantly reduce the required handling of artifacts, contributing to the overall conservation goal of the museum."

The convenience of knowing exactly where each item is located

With RFID tracking, each piece can be located by a computer program that can help locate the position as needed. Imagine that a manually edited log book has a particular piece's last documented location in storage room A, but when that room got too full it was relocated to storage room B without any documentation. The RFID tracking system would automatically be updated allowing the searcher to locate it despite the inaccurate logbook.

Museums that move their displays frequently but do not have the staff needed for ongoing physical inventory benefit greatly from RFID tagging. According to Mr. Muszynski, "even with passive tags, there is a significant security benefit, since door readers can detect passive tags as they pass through."

Unlike Electronic Article Surveillance (EAS) systems, RFID lets the reader know exactly which piece has passed through the door, not just the fact that a piece has passed through." This ensures an accurate inventory at the same time as allowing security tracking. (EAS Systems are used to deter shoplifting from retail stores or pilferage of books from libraries via a simple on/off "switch" that is deactivated during proper check out.)

Therefore, when a museum loans inventory to another museum or displays it offsite, the artifacts are 'checked out' by the RFID reader and can be 'checked back in' as the exhibit reenters the museum.

RFID tags are more expensive than barcodes, but RFID supporters stress that ongoing cost savings, more accurate inventory, and better security outweigh the extra per tag cost.

Taking tagging to the next level: active tags aid in security

Although galleries use conventional security such as alarm systems, closed circuit television, and security guards, these systems are often turned off or used less during the hours when the gallery is open.

With active tagging, the applications for RFID in the museum expand greatly. Where the more common passive RFID tags derive their power from the reader in order to 'turn on,' active tags have their own power supply. Thus active tags can communicate with readers at much greater distances than their passive counterparts.

Long-range identification capabilities made possible with active tags allow artifacts to be read with a network of readers strategically placed throughout the buildings.

RFID monitoring allows the museum to know exactly where the tagged work is at all times, relaying information to a computer in real time. If someone were to move a tagged piece, staff could track the piece down and intercept it before it left the building. With a museum RFID protection system auditing a gallery's collection nearly 6,000 times a day, the treasures of yesterday are highly secure.

Tags can be assigned different functionalities depending on the type of artwork being protected. For instance, a painting on the wall can be tagged with a chip that has vibrations sensors, and if it is moved without authorization, a real-time gallery alarm will be generated. The systems can even be configured to contact third party alarm systems or integrate with security infrastructures already installed.

Tagging art lovers as well as art?

If a museum is tagging its pieces of art, why not tag each individual as they walk in the door? Physically tracking patrons through the exhibits allows the museum to generate statistics on several different levels. When each patron has a unique tag, the gallery can acquire information never before attainable. How long did you look at each piece of art? Who saw it with you? Couple the electronic information with a post-visit questionnaire and a wealth of insight can be learned. Was time spent in a specific wing

or crowd levels in that area impact the level of enjoyment? Did seeing a particular piece with another person have an impact?

This data can further help the museums and galleries know how to design their exhibits in regards to spacing, lighting, music, and more. This type of system monitors how long a visitor looked at a piece, and through analysis can determine which items attract the most visitors and revenues for the museum.

In 2004, Museum of Modern Art (MoMA) started a pilot project, handing Toshiba Pocket PCs to visitors. These PDAs are loaded with digital video and audio content about the museum's art and exhibitions that can be accessed on the fly via the museum's wireless network. At the end of the tour, the visitor can register their e-mail address. After their visit, when they log on at MoMA's web site at home, the visitor will find a personalized web site section with merchandise related to the artwork bookmarked during the tour. If they log on to the website before their visit, they can customize their tour. Upon arrival they receive their PDA with their customized tour-guide.

MoMA is also planning an RFID pilot project that will involve the tagging of artifacts for inventory purposes so that RFID can be used to automatically register where exactly any piece of art is located.

By issuing RFID enabled badges to employees, they too can be tracked throughout the monitored facility. Management could tell when people arrived and left and could even tell who is meeting with whom, and in what part of the building. Each employee therefore would be tracked in and out of storage rooms and therefore could be associated with pieces that are being moved throughout the building. Security of all items is also enhanced eliminating unauthorized persons access to restricted areas.

In a report by the technology provider building the PDA solutions for the museum, Steve Peltzman, MOMA's chief information officer said stated, "once all art pieces are tagged we will find other ways to take advantage of it." That seems to be a fitting statement for RFID in museums and other industries. It is less a solution than a leveraging point to build other solutions.

Is RuBee the next generation of RFID?

The race is on to see if this hot new technology will be an alternative, or a complement, to RFID

David Wyld

Contributing Editor, AVISIAN Publications

What if there was a technology that one-upped RFID? What if there was a way to have continuous identification, but without the extreme size, cost, and limited life of active RFID? What if there was a way to gain far greater read ranges? What if there was a way to overcome the problems of reading around water and metal that have been the operational "Achilles' heels" of item-level RFID? That possibility exists today in the form of RuBee. Already heralded by industry observers as "RFID 2.0," RuBee may be the most exciting development in the automatic identification marketplace. This article is a primer on RuBee and its potential prominent place in the auto-ID market.

RuBee 101: the basics of the emerging technology

RuBee is the commercial name for what is known officially as LWID (Long Wavelength ID), as defined by the Institute of Electrical and Electronic Engineers (IEEE). The moniker was given to the technology by engineers at Miami-based Visible Assets after the Rolling Stones' song, "Ruby Tuesday." In June 2006, the IEEE announced that it had formed a working group to begin work on a new visibility network protocol standard, which will be known as IEEE P1902.1™.

The standard, which the IEEE hopes to have in place by the second half of 2007, will provide physical and data-link protocols, based upon RuBee technology.

RFID and RuBee are almost polar opposites in a technological sense. This is because RuBee uses almost exclusively magnetic energy, rather than the electrical – or radio frequency – energy used with HF and UHF RFID. RuBee operates at low frequencies, below 450 kHz and optimally at 132 kHz, which is far below the AM radio band. Because RuBee uses only microwatts of magnetic energy to communicate between the tag and the reader (known as a router, which is simpler in design and lower in cost than RFID readers), RuBee alleviates any of the safety concerns with traditional RFID. Because the technology uses low frequencies that are not attenuated by water and metal, RuBee tags can be read in and around environments that contain high amounts of liquid and metal far more accurately than traditional RFID. RuBee tags have been demonstrated to be readable even when buried underground.

The reading capabilities of RuBee are starkly different than traditional RFID technology. Indeed, the read ranges of RuBee are far higher than UHF and HF RFID. Using volumetric loop antennas (as opposed to dipole for traditional RFID), RuBee has been shown to have a far greater read range than passive RFID tags, with performance estimates ranging from a radius of 8-20 feet (using a 1 square foot antenna) to as high as 100 feet x 100 feet, meaning an possible read range of approximately 10,000 square feet. Today's RuBee tags are active, in that they are powered by coin-sized lithium

batteries that are low cost and have an expected life of between 10 and 15 years. The IEEE P1902.1 standard will also cover passive RuBee tags, which are under development, but which would harvest energy and reflect magnetic signals in the same manner as passive RFID tags.



From the viewpoint of Reik Read, lead RFID analyst for Robert W. Baird & Company, "the key downside element of the RuBee technology in comparison to RFID is a slower read rate." While HF RFID tags can be read today at 100 per second and UHF tags can be read at up to 150 to 200 per second, the read rates for RuBee tags are approximately 6-10 per second. While such read rates will make RuBee impractical for most supply chain and postal/shipping applications, the slower rates could actually work in RuBee's favor in other venues, such as animal identification, assuring product authenticity, and medical applications. Also, while the read rates are far slower, the read accuracy of RuBee tags has been shown to be superior in tests and pilot applications to EPC-RFID tags, with less susceptibility to ambient noise and other RF signals.

And yet, speed is not everything. According to John Stevens, chair of the IEEE's P1902.1 Working Group and chairman of Visible Assets Inc., the concept is that "RuBee is a visibility tool, whereas RFID is a tracking tool." RuBee thus is envisioned as a "visibility" system, providing far more information than the simple tracking of objects or products through an assembly line or in a warehouse. While tracking systems collect data on where an object has been, visibility systems can provide for both a real-time information system on the status of people and objects, as well as historical information on items and an audit trail on objects (which has become extremely important for corporations operating in the United States today in the wake of the requirements of the Sarbanes-Oxley Act). As such, RuBee thus presents intriguing technological advantages and conceptual design differences over the traditional EPC-RFID model.

The design of RuBee technology also allows for peer-to-peer communications, not only between tags and routers, but also between tags themselves. With this capability, the tags themselves could be programmed to issue "pair-wise" matching alarms, so that each RuBee tag could be used to provide an alert if an item was shoplifted from a smart shelf in a retail setting or if there was an unauthorized removal of a controlled substance or a high-value item. The P1902.1 standard will also have a "real-time, tag searchable" protocol for RuBee tags, which will allow for tags to have

Advantages of RuBee Technology

- Ability to be read in adverse conditions (i.e., water, metal)
- Greater read range
- Long battery life
- Peer-to-peer tag communications ability
- Cost-effective versus active RFID tags
- Information travels with the item with memory on the chip
- Greater read accuracy with less susceptibility to other RF signals

unique "tag" URLs associated with them and be searchable via the Internet. As opposed to the EPC model, where tag memory is kept to a minimum and the tag is a pointer to records and info on the tagged item, RuBee tags will be designed to have memory capacity to carry information on the item about the item. As John Stevens recently commented: "If you've got 50 items on a conveyor that need to be read in under a second, RFID will work, but if you have a product where you want access to internal records inside a warehouse and want to find out about its history from the day it was born ... that's visibility." With these capacities however, RuBee tags will cost far less than any competitive active RFID tags presently on the market.

Analysis of RuBee's potential

Writing in *Computer Power User*, Kyle Schurman projected that the market prospects for RuBee are bright because "this new technology should fill in some of the gaps in the market that RFID can't meet." Indeed, with its differentiated capabilities, RuBee may be ideally suited for applications in the retail sector, in health care and pharmaceuticals, in animal identification, and in a whole host of areas where traditional RFID has been considered technologically impractical or cost ineffective. In retail, there may even be room in the retail market for RuBee tags to be used in tandem with EPC-RFID tags on high value items, much as has been proposed for the dual use of RFID and bar codes on items for some time to come. RuBee also has promising capabilities for smart asset management.

Thus, at present, we stand at the threshold of a very exciting period in the development of radio – and magnetic – identification technologies. With the finalization of the IEEE protocol standard in the second half of 2007, it is likely that we will see an upsurge of interest and investment in RuBee technology. Already, RuBee has the support of leading technology providers, including:

- Epson,
- Hewlett-Packard,
- Intel,
- IBM,
- Motorola,
- NCR,
- Panasonic, and
- Sony.

It also has drawn interest from leading retailers, including Best Buy in the U.S., U.K.-based Tesco, Metro Group in Germany, and France's Carrefour. However, it is unlikely that RuBee will be, as one industry analyst put it, "the death knell" for RFID. Rather, as veteran RFID analyst Pete Abell with IDC's Manufacturing Insights recently commented, the emergence of RuBee is proof that "the RFID world, moving forward, is not going to be a one-size-fits-all environment." Steve Winkler, who is a standards architect for SAP, recently observed that: "There is enough room for peaceful co-existence and even a symbiotic relationship between the two technologies. RuBee can ride the coat-tails of RFID's popularity to gain adoption, while RFID vendors don't have to try to be the be-all end-all and can focus on the scenarios to which they are best suited."



The death of the 'six month rule' for retail RFID ...

Rapid progress of early-adopting retailers is stretching their headstart beyond the industry's often cited 'six-month' comfort zone

David Wyld

Contributing Editor, AVISIAN Publications

In *Line56 Magazine*, Tamina Vahidy recently observed that the Wal-Mart mandate has already effectively "changed the face of retail ... making what had been a niche technology into a mainstream application." Since 2004, Wal-Mart's commitment to the technology has certainly been a driving force for the entire RFID market. And the well-reported work of the University of Arkansas' RFID Research Center has shown the demonstrable impact of RFID at improving the mammoth retailer's supply chain visibility and execution, dramatically reducing out-of-stocks, cutting back unnecessary orders, and improving the effectiveness of promotional efforts.

Recently, Wal-Mart's CIO Rollin Ford pronounced: "We continue to work with suppliers to help them see the vast potential of RFID. We're already fully convinced of its value and are ready to step up the pace since we

know we are only touching the tip of the iceberg when it comes to the benefits of this technology ... We are actively engaged in designing some new initiatives that will accelerate our program even further and, in so doing, create even more value for everyone involved."

Well, when it comes to RFID, retail executives are known to have an often unspoken "six month rule." Plain and simple, many are willing to let the pioneers of the technology, like Wal-Mart, Target, Best Buy, and Metro take the arrows, expend the time and money, and learn the lessons about RFID. However, in reality, their mantra is "Don't let me get more than six months behind Wal-Mart in RFID adoption." Yet, as was recently written in *Retailspeak Magazine*, "the reality is that if you were waiting to hear Wal-Mart's recent statement on RFID, you are already more than six months behind."

Late last year, the retailer announced a significant acceleration of its RFID initiative, doubling both the number of suppliers – from 300 to 600 – that would be required to ship RFID-identifiable pallets and cases and the number of Wal-Mart stores – from 500 to 1,000 of its 3,900 stores – that would be RFID-enabled by January 2007. Moreover, after June 30, 2006, Wal-Mart had stopped allowing its participating suppliers from using Gen 1 technology, making them switch to EPC Gen 2 tags exclusively.

Writing in *Directions Magazine* on “The Strategic Implications of Wal-Mart’s RFID Mandate,” David H. Williams outlined what he called the “ripple effect” of the giant retailer’s initiative throughout the supply chain. Despite the immediate, short-term prevalence of “slap and ship” solutions and rather low RFID investments among Wal-Mart suppliers, Williams projects that suppliers will gravitate to using RFID tracking in their own operations and with their own suppliers upstream in the value chain. Likewise, with suppliers RFID-enabled, pressure will be exerted on transport carriers to use RFID-based tracking so that door-to-door visibility will be extended throughout the value chain. This “ripple effect” will serve to greatly multiply the numbers of companies impacted by the Wal-Mart mandate and cause sharply increased overall demand for RFID tags in the coming decade, which will further enable economies of scale in production of tags/smart labels and drive unit costs for RFID-based identification down.

As RFID tag/label prices drop, we will see a significant acceleration in the proliferation of tagging at the item level. The use of EAS (electronic article surveillance) tags in retail serves as a useful precedent. At present, there are six billion EAS tags produced annually at a price point of approximately one cent per unit. This represents marked growth over a few years ago, when the unit price was between five and eight cents and the market was one billion tags.

According to market projections for 2016 from Dr. Peter Harrop of IDTechEx, over half a trillion consumer items will be individually tagged, and the market for item-level tagging will exceed US\$13 billion annually. As can be seen in the table on this page, unique identification of consumer packaged goods (CPGs) will account for the vast preponderance of such item-level tagging. How will this impact individual companies? Take Altria, a leading consumer products manufacturer, for example. Altria has an exceptional stable of brands from its Kraft, Miller and Philip Morris units. If Altria were to individually tag each of items, this would amount to approximately 80 million tags annually for this company alone.

In sum, why is the much-heralded “Wal-Mart Way” becoming more and more RFID-enabled? In short, it is because the retailer’s RFID efforts are producing tangible results, both from an operational standpoint and

The Market Size for Item-Level Tagging (Annual Potential Number of Tags)

Application	Tags (in Billions)*
Laundry/Rented Textile	.1
Library Books & Materials	.1
Aircraft/Machinery Parts	1
Blood Bags/Medical Specimens	2
Military	20
Book Manufacturers	50
Prescription Drugs	50
Cigarettes	100
Postal	550
Other Consumer Packaged Goods	5,000 -10,000

Source: IDTechEx, “Item Level RFID - The Prosperous Market 2006-2016,” August 2006

for the retailer’s bottom-line. In the process, the retail giant is increasing revenue for participating supplier’s products by improving on-shelf availability and the sales velocity of the turnover of items. As RFID tagging proliferates and tag prices decline – especially in light of promising developments with non-silicon based tagging – we will see unprecedented opportunities for the retail supply chain to be interlinked. While mandates from large retailers around the world will continue to be important, suppliers and manufacturers will gravitate to earlier tagging – down to the item-level – to create a truly visible supply chain. Over time, we will see great benefits accrue to those firms that take the lead in innovating and discovering the future of RFID in consumer products. And, as the pace of change accelerates, six months will become a very, very long time in the retail market space. Those who follow the “six month rule” could find themselves out of pace with the new landscape of RFID-enabled retailing and be at risk, both operationally and strategically.

About the author:

David C. Wyld (dwyld@selu.edu) is the Robert Maurin Professor of Management at Southeastern Louisiana University, where he directs the College of Business’ Strategic e-Commerce/e-Government Initiative and teaches business strategy.



Creating an ePedigree for sports collectibles with RFID

With well more than half of all autographed items likely fake, memorabilia dealers are turning to technology for help

David Wyld

Contributing Editor, AVISIAN Publications

The business of sports has grown rapidly worldwide. According to the most recent report from the Sports Business Journal, the size of the American sports industry has reached an astonishing US\$213 billion annually and the global market has been estimated to be close to a trillion dollar market. One Canadian media analyst has labeled our passion for sports as our new societal obsession, which he terms “sporno” (the idea that athletes and sport are the new pornography).

The market for sports collectibles has grown as a byproduct of this increased focus on professional sports and sports stars. It represents a significant part of the over \$10 billion retail collectibles market – market that serves approximately 50 million collectors in the United States alone. In the past, sports memorabilia was purchased mostly at large trade shows or on a private sale basis. Today however, the sports collectible market has burgeoned into a part of mainstream online and offline retailing, with product available in a wide variety of venues, from eBay to your local mall.

Today, you can walk into almost any mall in the country and find a small shop dedicated to selling sports-themed collectibles, including items such as LeBron James’ autographed photographs, Indianapolis Colt’s helmets signed by Peyton Manning, and baseballs signed by everyone from Albert Pujols to Barry Bonds. Teams and leagues are getting in on the action themselves, selling autographed items and “game worn” uniforms both in the stadium and on the web.

However, the sports collectibles marketplace is perhaps the ultimate caveat emptor arena. According to FBI statistics, at least 70% of all autographed sports memorabilia is fraudulent and an estimated half-billion dollars is lost annually to fake sports collectibles in the U.S. The field is ripe for counterfeit items due to both the growing demand and the limited supply of genuine autographed and game-used items.

Despite the apparent ease of creating fake sports collectibles, especially given the powerful computing and printing technology at our fingertips, sports counterfeiting has become something of an art form. In fact, the majority of counterfeit sports memorabilia distributed across the United States can be traced to a finite number of counterfeiters. However, these rogue operations supply an enormous amount of high-quality fake memorabilia. These counterfeiters usually sell the fakes to large-scale distributors of sports collectibles, who in turn supply the items – knowingly and unknowingly – to major retail outlets, other smaller distributors, or directly to the public. These distributors – and ultimately the variety of retail outlets – are cognizant of the “fuzziness” of their supply chain.

How can RFID work to authenticate such items? There are several companies today vying to market RFID-based solutions for sports memorabilia, but the leader in the field to date is the Irving, Texas-based Prova Group, whose business model is to use RFID technology to be a third-party authenticator of the genuineness of sports collectibles. One of the founders of Prova is Emmitt Smith, the Hall of Fame running back who led Dallas Cowboy teams of the 1990s to three Super Bowl victories.

The Prova system works by having a tamper-proof RFID tag applied directly on the surface of the collectible to be autographed by an athlete. Then, at the point of signing, the Prova system records the exact time of the signature to the second, when the item (a ball, a jersey, a helmet, etc.) is placed within 12 inches of an antenna set up near the athlete’s hand. The autographer’s secure identification code is written to the tag, recording who signed as well as when and where the signature occurred. The data for this unique item is recorded in Prova’s online registry.

By accessing the item in Prova’s database via the Internet, the collector or subsequent prospective buyers can access an item’s history

and view an undeniable “chain of custody” from the creation of the autographed item.

Likewise, sports teams are using Prova RFID tagging systems to verify the authenticity of “game worn” uniforms (such as jerseys and helmets) and balls. The company already has deals in place with the Dallas Cowboys and St. Louis Rams to tag each jersey worn by their players in NFL games. The Prova system then tracks the time at which the uniform is logged in and out for use in each game. Thus, in addition to being able to print a hard copy certificate of authenticity, a collector could direct prospective buyers of that item to the firm’s online registry for verification of the game use of the jersey. Craig Noonan, Prova’s Chief Marketing Officer, observed that by marking collectible items with RFID and providing an online registry, “we give you a way to track an item’s ownership history similar to a title search on a house ... we’re protecting authenticity from generation to generation.”

The sports memorabilia marketplace is at a crossroads. With more and more interest in sports on a global basis, the market prospects for sports collectibles is bright. However, the wave of counterfeit items threatens chaos in the market. With today’s technology, RFID can be a tool to add an indisputable assurance of authenticity to sports collectibles, enabling buyers and sellers alike to work with an e-pedigree for memorabilia and fostering even greater growth in the global market for these items.





Government

Financial Transactions

Public Transport

Industry & Logistics

Food & Animal

Access & Security

IT & Corporate ID

360° competence in contactless ID

You are looking for a partner that is ahead of the times working on the contactless ideas of tomorrow? One that is as easy as the contactless ID subsystems he creates? Then you should read on: ASSA ABLOY ITG supports system integrators worldwide by selecting the ideal technology platform and creating contactless ID subsystems that work in the real world. Because as an innovative forward-looking company you have to understand more than one technology.



Transponders



White smart cards



Printed smart cards



RFID reader modules



PC-connected readers and chip sets



Operating systems & middleware


$$+ \frac{\theta^4}{4!} + i \frac{\theta^5}{5!} - \dots$$
$$] + i \left[\theta - \frac{\theta^3}{3!} + \frac{\theta^5}{5!} - \dots \right]$$
$$\frac{n+1}{n+1}!$$
$$\theta$$

Brain.



Trust.

There's a reason our prox cards and readers are used all over the world, and that iCLASS contactless smart card technology is quickly becoming an industry standard. We've sold over 200 million cards. Our products come with quick lead times, a lifetime warranty, and they offer unmatched reliability and flexibility. In security, there is no single factor more important than confidence. And there's only one way to gain that from customers. You earn it.



hidcorp.com

ACCESS confidence.