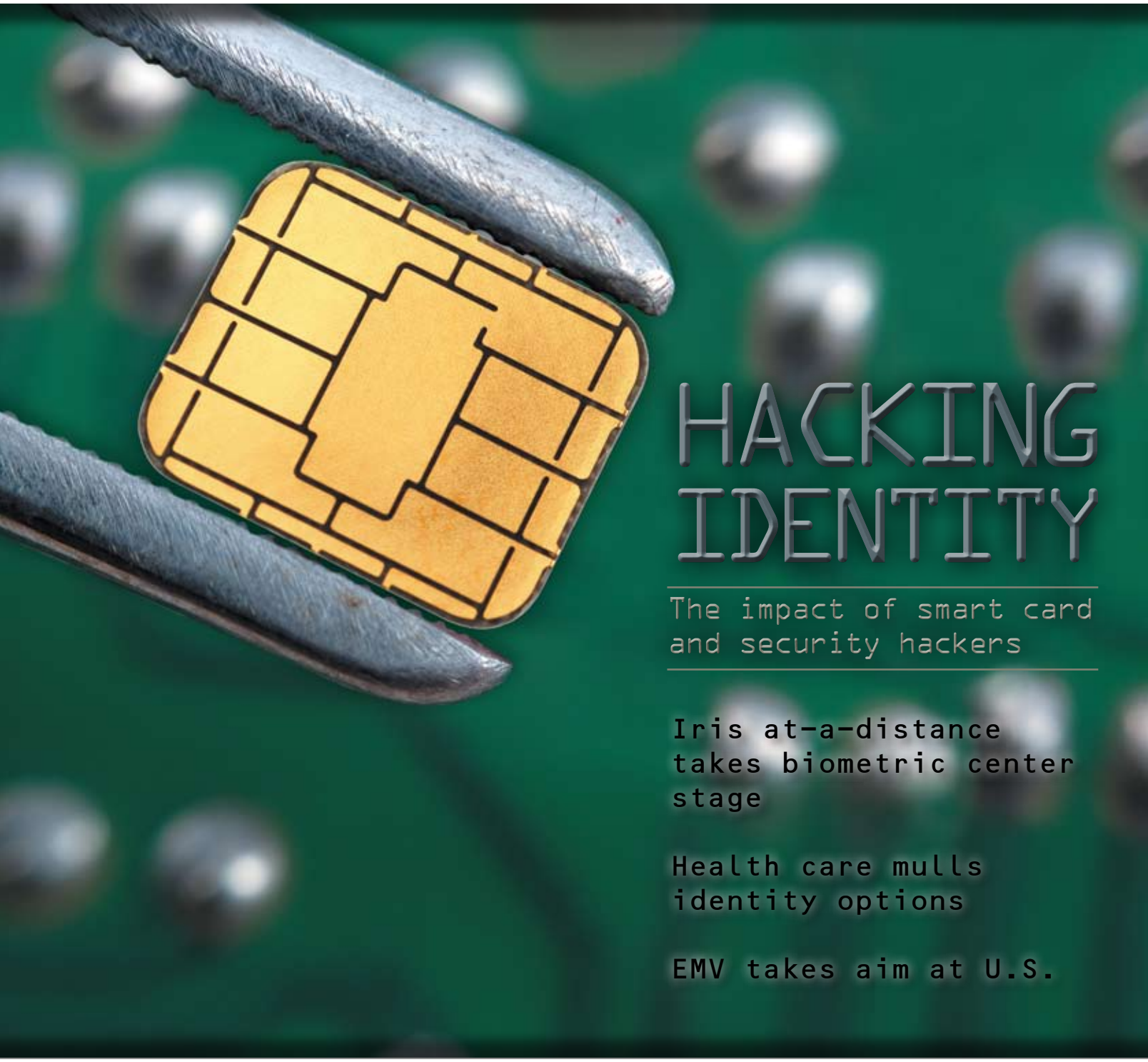
re:ID

Summer 2009

Regarding ID Magazine – a survey of identification technology • SecureIDNews • ContactlessNews • CR80News • RFIDNews



HACKING IDENTITY

The impact of smart card and security hackers

Iris at-a-distance takes biometric center stage

Health care mulls identity options

EMV takes aim at U.S.

AVISIAN

CoreStreet

We Make Credentials Work

CoreStreet PIVMAN Solution for TWIC Compliance

Your job: ensuring TWIC compliance. Individuals are coming to your facility with a new card that may be revoked and you've never seen them before.

They look right, but are they legitimate? Are they on the Hotlist?

The CoreStreet PIVMAN Solution allows you to check any TWIC card, confirm the bearer's identity, associated access levels, and log all activity. Anytime. Anywhere.

No network connections. Just grab a handheld and go!

The CoreStreet PIVMAN Solution provides rapid verification of TWIC cardholders for unescorted access and the audit logs required by USCG. CoreStreet PIVMAN is TSA ICE list approved, also supports CAC, PIV and FRAC cards, is reimbursable under various DHS grant programs and links to existing PACS systems such as Lenel OnGuard®.

Available on a range of Windows-based handhelds and PCs.

To learn more about CoreStreet's TWIC Compliance solutions visit www.corestreet.com/TWIC

The *Original* Multi-Technology Readers

The Most Versatile, Secure Readers in the Industry

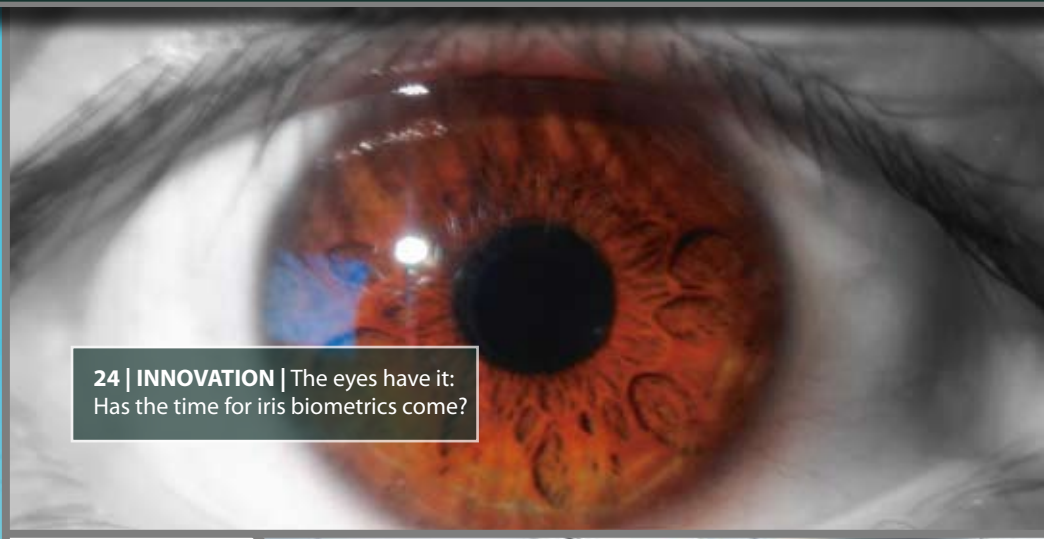
XceedID®
Xceeding The Ordinary

To learn more please visit: www.xceedid.com

Summer 2009

52 | SECURITY | Power grid hack may lead to PIV for utilities

Contents



INDEX OF ADVERTISERS

Perspective

EXECUTIVE EDITOR & PUBLISHER
Chris Corum, chris@AVISIAN.com

EDITOR
Zack Martin, zack@AVISIAN.com

ASSOCIATE EDITOR
Andy Williams, andy@AVISIAN.com

CONTRIBUTING EDITORS
Daniel Butler, Liset Cruz, Seamus Egan, Ryan Kline, Ed McKinley , Jay Swift, Angela Tweedie, David Wyld

ART DIRECTION TEAM
Darius Barnes, Ryan Kline

ADVERTISING SALES
Chris Corum, chris@AVISIAN.com
Sales Department, advertise@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 $200. 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
re: 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.

When beats collide

Smart cards could see more deployments in health care and payments markets

Zack Martin
Editor, AVISIAN Publications

The two years I wasn't covering the identification security market I spent writing about health care IT. It seems only fitting that the two are now converging.

There was a whole new alphabet soup to learn over there, electronic health records (EHRs), personal health records (PHRs), electronic medical records (EMRs), regional health information organization (RHIO) and health information exchange (HIE) are the big ones.

Early on I was at a conference about RHIOs and HIEs. A community was setting up a network where health care providers in the region would be able to exchange patient medical data. A lot of the discussion was about network configuration and logistics. When I asked how they would secure the network and identify patients I was brushed off. They had "other issues" to figure out.

Health care providers were more concerned with connectivity than security and identification.

Throughout my two years covering health care, I wrote many of these stories and continued to ask the same question, never getting a good answer. Health care providers were more concerned with connectivity than security and identification.

The issue has been highlighted more this year because of the $19 billion in the U.S. stimulus package for health care IT. Smart card and biometric vendors are battling over which technology would be the best fit for identifying patients (See stories, page 50 and page 58).

Both could play important roles in helping the health care industry secure information and properly identify patients. But if the two years I spent covering the market taught me anything it's that glaciers move faster than health care CIOs adopting new technology. The old adage that health care is five years behind everyone else when it comes to IT is true.

I recently had a conversation with a well informed identity consultant who told me health care providers will be using FIPS 201 before then end of 2009. Now this consultant is much better connected to me but I have my doubts.

I think we will eventually see smart cards and biometrics in health care, but it's going to be awhile. Projects like the ones at Mount Sinai Medical Center in New York and BayCare Health System and ValleyCare Health System will become more common, but if we see widespread use of high-tech identity technologies before 2012 I'll be pleasantly surprised.

***

A few months ago if you would have asked me if I thought the U.S. would switch to EMV I would have said it probably won't happen. Well, another data breach and a hearing by a U.S. House of Representative's subcommittee has left me not so sure anymore.

To accept credit cards now U.S. retailers must adhere to the Payment Card Industry (PCI) rules. These define how payment card information is stored and transmitted along with a variety of other stipulations. But many retailers don't like PCI. They claim the rules are confusing and they don't work (See story, page 32).

During the congressional hearing Rep. Yvette D. Clarke (D-N.Y.) said PCI doesn't go far enough and said it's time to start thinking about EMV. "Magnetic stripe-based technology is outmoded and inherently less secure when compared to smart cards or other developing technologies," she said.

The Committee On Homeland Security's Subcommittee On Emerging Threats, Cybersecurity, and Science and Technology held the hearing. There's a fear that that money from credit card fraud are going to fund terrorists. One terrorist has already admitted as much.

Unless a law is passed mandating EMV it's going to be interesting to see whether or not it happens in the U.S. It comes down to the typical struggle between banks and retailers.

The majority of time retailers are the ones who get stuck paying for credit card fraud. Banks don't have the impetus to start spending more money to issue a chip card.

There's also the question of who will pay to upgrade point-of-sale terminals to accept EMV smart cards. Visa and MasterCard have been subsidizing retailers adding contactless readers to terminals, but will they be willing to shell out additional funds for EMV?

I hope you enjoy the issue. ID

re:ID Podcast CHANNEL

re:ID Podcast
AVISIAN

Do you have an idea for a topic you would like to hear discussed on an re:ID Podast? Contact podcasts@AVISIAN.com

SPONSORED BY DIEBOLD

The U.S. passport security gap

A General Accountability Office report details some serious holes in the U.S. State Department's passport issuance. A GAO investigator was able to obtain four passports with fake breeder document information. Regarding ID Editor Zack Martin spoke with Janice Kephart, director of national security policy at the Center for Immigration Studies and a member of the 9/11 Commission, about the problem and the risk it poses to national security.

Highlights: "What terrorists want and covet most is a U.S. passport. Having a US passport gives them a kangaroo jump. The focus these groups have on the passport and the border shocked us. It's not fear mongering it's the reality.

"Auditors are completely blind. Unless they see something wildly, horribly wrong they're not going to flag the applicant. You have to back up the card with robust vetting of identity on the front end.

"There's no excuse for the State Department not to be checking Social Security numbers. What's truly doable and useful is hooking into the Social Security Administration. State dropped the ball on the Social Security numbers and there's no excuse."

To listen, visit SecureIDNews.com/tag/Podcasts and select "Episode 27"

Expanding contactless payment acceptance

Tap and go is the idea behind contactless payments. USA Technologies aims to bring that convenience to unattended devices, such as vending and coffee machines. Regarding ID Editor Zack Martin chatted with Mike Lawlor, vice president of business development and sales at USA Technologies about the company's latest deployments and where he sees contactless payments going.

Highlights: "Starbucks wanted to provide a payment system that was most conducive to customers. They can pay with a swipe or a tap of the debit or credit card.

"Our solution fits into the fastest emerging areas and that's the small ticket unattended market, whether it be a Starbucks machine, a coke vending machine or a parking facility or laundromat. Where's there's existing cash payments we're converting to cashless payments.

"We work in the traditional vending space, we have close to 50,000 devices across all the U.S. It is becoming prevalent in everyday life where you take out a contactless card and use it in the vending machine."

To listen, visit SecureIDNews.com/tag/Podcasts and select "Episode 28"

Channel
N

AVISIAN

Search

Celebrating 150 Years of Innovation 1859 - 2009

Vermont looking at smart cards for health care

There's $19 billion for health care to invest in information technology and electronic health records (EHRs) in the stimulus package. Vermont State Senate President Pro Tem Peter Shumlin wants to use smart cards to streamline billing. Shumlin talked with Regarding ID Editor Zack Martin about his idea.

Highlights: "What we learned through discussions with IBM research is the technology exists to get rid of the absolutely insane billing system we have today in health care.

"We spend 10 to 15 cents of every dollar chasing money around. We want to put a new model in place with a medical card.

"If you were building a system from scratch, like the one we have, people would say you're crazy.

"The medical card would enable a patient to show up at a physician's office for care and know right away how much the insurance company is paying and how much he needs to pay.

"It's like when you go to the store – you walk up to the counter and they tell you what you owe and you pay it."

To listen, visit SecureIDNews.com/tag/Podcasts and select "Episode 29"

Recent AVISIAN videos include coverage of ISC West and the National Association of Campus Card Users Annual Conference

SecureIDNews – Dell talking about its partnership with HID to bring contactless logical access to its laptops

CR80News – University of Texas at Arlington automating systems while focusing on security

CR80News – Colorado State expanding its RamCard program

ContactlessNews – Gemalto discusses the latest with NFC and what the ecosystem needs to thrive

SecureIDNews – Executives from Hirch talk about the identity life cycle and the company's latest solutions for converged physical and logical security programs

Look for us at these and other industry leading events:

CTST 2009

Biometric Consortium Conference & Technology Expo

The 8th Annual Smart Cards in Government Conference 2009

ID SHORTS

UK taps CSC, IBM for biometrics, IDs and passports

CSC announced that the UK Identity and Passport Service (IPS), an agency of the Home Office responsible for issuing UK passports and ID cards, has awarded the company a 10-year managed IT services contract to upgrade the IPS application and enrollment system. The agreement has an estimated value of $570 million.

IBM was awarded $390 million contract to run the UK's National Biometric Identity Service, which will deliver a database for storing facial and fingerprint biometrics for the UK passport and ID card. The company will replace the Border Agency's existing biometric database.

Under the terms of the contract, CSC will assume responsibility for several existing legacy IT service contracts supporting the IPS. CSC will upgrade the existing application and enrollment system with new capabilities to process applications for passports and ID cards. The additions include the ability for customers to apply online; improved background checking; a new system for reporting lost and stolen passports and ID cards; customer support for updating personal data; and new IT and telephony systems.

Working in conjunction with the IPS and its other delivery partners for the National Identity Service, CSC will help deliver the next generation of biometric passports and support the introduction of ID cards.

UK bank deploys ActivIdentity's one-time passwords

ActivIdentity Corp., a provider of strong authentication and credential management, announced that it has signed a contract with The Co-operative Financial Services, part of a consumer financial services provider in the United Kingdom.

ActivIdentity's 4TRESS Authentication Server secures money transfers, account updates and the addition of new payees. The Co-operative's 1 million retail customers will use a bank issued debit or credit card to generate one-time-passwords for authentication and transaction signing. By replacing static passwords with 4TRESS strong authentication the bank is trying to further protect customer data with EMV security.

The Co-operative Group is part of the Co-operative Financial Services. The Co-operative Financial Services offers a range of financial services including retail, business and corporate banking, investments, lending, and insurance.

Gemalto's consumer Web site registers 800K hits

Launched in mid-January, JustAskGemalto.com has registered more than 800,000 hits. The site aims to answer consumer questions on how consumers can keep personal information safe and has also had 500 questions asked on various security topics.

The site features questions and answers by category – traveling, communicating, surfing, personal data, buying and working.

The site also has a monthly focus topic, digital security news and articles by bloggers and experts, as well as 3D animations showing how devices, such as Wi-Fi routers, work.

The most frequently viewed questions are related to the loss of one's mobile phone. Another favorite centers around the security of social networking sites, blogs and e-commerce.

MasterCard PayPass hits 50 million mark

MasterCard Worldwide announced the issuance of the 50 millionth MasterCard PayPass card or device, as of the fourth quarter of 2008. In the last year this more than doubles the number of cards and devices in circulation around the world.

PayPass is designed to provide a convenient payment alternative to cash. Consumers need not swipe a card or even sign a receipt when making purchases of $25 or below. They just need to tap their PayPass-enabled devices on the readers in the more than 141,000 participating merchant locations worldwide.

DAP unveils new options for handheld ID reader

RMT Inc's DAP Technologies has released new options for its DAP Guard System. The handheld computer can now perform Transportation Worker Identification Credential verification, vascular biometric identification, remote control of video security and access control systems, and terrorist watch list interface.

DAP is able to add these functionalities through partnerships with AMAG Technology, CoreStreet, Hawkeye Technologies, Identica, inFront, Intellicheck Mobilisa, Senture Security Solutions and TransCore.

Highlights of the handheld include:

- TWIC Verification – Developed in conjunction with TransCore, Intellicheck Mobilisa and CoreStreet, DAP's Guard System can be customized with the TWIC configuration. It is FIPS 201 certified and has received Transportation Security Administration authorization for use in security clearance of millions of personnel accessing the nation's ports. Hawkeye, Identica and Senture provide additional identity-validation solutions.

- Vascular Scanning – Using near-infrared imaging, Identica's vascular biometric

scanners examine the thermal image of the vein pattern in the back of a person's hand to positively identify them.

- Database Management and Watch-List Checks – Intellicheck Mobilisa's software can read an ID card and run a check against more than 100 watch and terrorist lists. CoreStreet and inFront provide remote database-access solutions.

- Access Control – Utilizing software designed by Hawkeye Technologies or inFront and integration by AMAG Technology or CoreStreet, DAP's Guard System enables users, in real-time, to verify and manage cards, clear alarms, control hardware and view live video in the field using a Wi-Fi connection.

- GPRS – DAP's Guard System is enabled with Wireless Wide Area Network access, allowing users remote access to the Internet and virtual private networks.

- GPS – A second-generation SiRF GPS has been added to the Guard System, allowing for faster acquisition times and stronger signals in most locations.

- Universal Imager Camera – The new DAP Series Camera is an all-in-one solution that provides color video and still images in a variety of lighting conditions, and can read 1D/2D barcode and OCR fonts.

Mounties choose E-Seek driver license readers

The Royal Canadian Mounted Police will soon be equipped with E-Seek 2D bar code and mag stripe readers that will enable Mounties to swipe the license to obtain the driver's information rather then enter it manually.

The 4,600 dual card readers are being supplied by Softchoice Corp., a Toronto-based technology solutions provider, and its subcontractor, California-based E-Seek Inc., which develops detection devices for driver licenses and other state ID cards.

The E-Seek Model 250 incorporates a magnetic stripe reader with 2D bar code reading technology and will be capable of reading most government-issued ID cards in Canada.

The RCMP provides federal policing services to all Canadians and policing services under contract to the three territories, eight provinces (except Ontario and Quebec), more than 190 municipalities, 184 Aboriginal communities and three international airports. E-Seek's Model 250 gives the RCMP the ability to read both magnetic stripe and 2D bar code identification cards – both of which are used throughout the provinces in Canada.

Cubic, ViVOtech partner to enable mutli-technology cards

Cubic Transportation Systems Inc. is providing new capabilities for the Cubic designed Tri-Reader to enable an all-in-one reader that will process bank cards, prepaid cards and smart card-enabled mobile phones.

The latest generation Tri-Reader platforms and will obtain type certification for MasterCard Paypass, Visa PayWave, American Express, and Discover cards, which will enable contactless bank card acceptance at Cubic fare collection devices for public transit.

Tthe Tri-Reader, a ISO 14443 Type A- and Type B-compliant smart card processor, will provide a single reader that will seamlessly accept contactless bank cards, prepaid products like the First Data GO-Tag solution, and emerging NFC mobile phone technology, as well as currently issued transit cards and those conforming to national transit standards.

Cubic has installed more than 60,000 Tri-Readers across 17 major markets around the world. Major fare programs such as London's Oyster card system, Washington's SmarTrip system, and New York/New Jersey's SmartLink system are all supported by Tri-Reader technology.

GlobalPlatform releases match-on-card paper

GlobalPlatform, the specification body for smart card infrastructure, has published a white paper to explain how its existing technology can add value to biometric match-on-card solutions from research and development cost-savings and improved time to market, to compliance with industry security requirements.

"The GlobalPlatform Value Proposition for Biometric Match-on-Card Verification," targets government officials, project managers and consultants advising on the implementation of biometric match-on-card programs, alongside smart card technical audiences. It discusses how current GlobalPlatform specifications deliver the required security and privacy to enable the deployment of a secure, interoperable and flexible biometric match-on-card solution.

GlobalPlatform on-card access control technology is also discussed within the white paper. This function can facilitate the delivery of multiple applications on one card, with each application able to securely utilize the match-on-card biometric in a flexible way without having to become biometric aware.

Entrust backing Master List Signing

Entrust is moving forward with supporting the Master List Signing, the company announced during the ICAO Regional Seminar on Machine Readable Travel Documents, Biometrics and Security Standards in Abuja, Nigeria.

The Master Signing List is a method to reduce expensive, time-consuming duplication that exists in the current e-passport verification process. The system involves countries importing the e-passport signature verification keys to the Master List so that they can be verified as authentic.

As Entrust has an existing working relationship with over 30 countries in areas concerning e-government and national security initiatives, they feel that their involvement with the Master List Signing is important to its success.

"While full adoption of Master List creation and signing is still on the horizon, its benefits are too important to ignore," said Bill Conner, Entrust's president and CEO. "We fully support this initiative – so much so, Entrust has enabled a Master List Signing certificate profile within the upcoming release of our proven e-passport security solution. This will enable our customers to strategically develop their Master List Signing capabilities from a trusted security partner."

Scottish company develops contactless for EMV systems

Scotland-based i4 Product Design has developed for another Scottish company, Tailwind Solutions, a contactless card payment solution for retailers that works in an EMV environment, allowing consumers to pay with their NFC-compliant phones or contactless EMV cards.

The PoS Paddle Tap-It is designed to work with all retailers' existing EMV configurations. Instead of swiping a payment card or handing a card to a cashier, consumers present their debit/credit card or NFC enabled mobile phone to the PoS Paddle Tap-It.

i4 Product Design has also developed PoS Paddle SafeBase, which allows retailers to lock down their EMV readers to the counter, to prevent theft and subsequent fraud. It too is compatible with all retailers' existing EMV devices.

Tailwind Solutions is working with several industry partners in bringing its PoS Paddle products to market, including Smart Technology Solutions, which has already integrated PoS Paddle Tap-It with its retail software.

Visa rolls out NFC-enabled payments program in Malaysia

Visa has put together a Malaysian partnership that includes a bank, a cell phone manufacturer and a mobile phone carrier to launch its first commercial mobile payments service using NFC technology. Consumers are now able to purchase an NFC-enabled mobile phone off the shelf and use it to make Visa payWave-enabled transactions at the point-of-sale in place of their credit card.

Maxis, Malaysia's largest wireless carrier with more than 11 million subscribers, handset manufacturer Nokia and Maybank, are the other partners.

The service enables Maybank Visa account holders to wave their NFC-enabled Nokia 6212 classic handset in front of a contactless reader to complete a secure Visa transaction. Maybank Visa account holders can download their Visa payWave credit account details directly to their Nokia handset over the Maxis wireless network. Once the account has been personalized on the phone, account holders can then begin to make purchases at any one of the 1,800 merchant outlets that accept Visa payWave in Malaysia.

The contactless chip embedded in the phone also powers several other functions, including a transit application that enables Malaysian commuters to pay for charges while using metropolitan transit systems, bus terminals, highway toll gates and car park facilities at more than 3,000 contactless payment touch points throughout Malaysia. Maxis has branded these mobile payment services under the name Maxis FastTap.

"We believe that Visa's NFC mobile payment launch in Malaysia signals a tipping point for the payments industry globally as we move from mobile payment pilots to commercial availability," said Elizabeth Buse, Visa's Global head of product.

VeriSign launches two-factor authentication for iPhone

VeriSign Inc. announced its VIP Access for mobile application is available on the Apple App Store. The application turns the iPhone into a one-time-password credential that can be used in conjunction with a username and password to strengthen the security of online accounts.

VIP Access for Mobile on the iPhone creates two-factor authentication for consumers – the first factor being the username and password (something they know), and the second factor being the iPhone VIP credential (something they have). With the new credential, iPhone users can enjoy strong authentication at more than 40 Web sites that are part of the VIP Network, including eBay, PayPal and AOL.

YO! Sushi goes contactless

Commidea, a card payment processing provider, has announced that it is providing its integrated point-of-sales systems with contactless technology to YO! Sushi. The system has been deployed in partnership with Clarity Commerce Solutions, a supplier of EPOS solutions for the hospitality sector.

YO! Sushi is using Commidea's payment solution in 30 of its 40 restaurants to improve throughput and eliminate transaction errors. The integrated system transfers the data from the Clarity Enterprise Suite software to Commidea's Chip & PIN terminal automatically from the till.

In addition, YO! Sushi has implemented Commidea's contactless payment solution, where the contactless enabled credit card is simply passed over a reader to make a purchase of $15 or under, without the need to enter a PIN code.

Another feature developed by Commidea enables YO! Sushi's customers to use the payment terminal to add a gratuity. This has removed the need for serving staff to request a gratuity from customers, and has resulted in an overall increase in tips.

Gemalto and Precise partner for new biometric technology

Gemalto has partnered with Precise Biometrics, a developer of biometric identity verification solutions, to create the Gemalto.Net Bio solution.

The product uses Precise's Match-On-Card fingerprint authentication technology, which stores the cardholder's biometric information on the card rather than matching to a database, to replace user passwords and create a system that enhances network security for organizations.

A man, a Mazda, an RFID implant

Jon Oxer, who has been labeled "Australia's geekiest geek" by a Sydney newspaper, has made some adjustments to his car. Most are not that surprising for a man who clearly takes his technology seriously: 24-hour internet access in Mazda RX-8 might be unusual, but not that extreme. The remote ignition controlled via his iPod Touch and iPhone could be considered downright handy.

Then there is the keyless entry option. Oxer has installed an RFID reader on the window of his car which is interfaced to the car's security system. This enables him to unlock his car with the RFID tag he has had implanted in his left arm.

Oxer has also modified his house to take advantage of the tag which operates door locks and other features. The tag was implanted via a tool usually found in veterinary clinics.

CoreStreet announces new products, partnerships

CoreStreet announced the availability of the CoreStreet FIPS-201 Suite of products to upgrade existing physical access control systems to be fully compliant with HSPD-12 and all functionality as defined in Special Publication 800-116.

Special Publication 800-116, as published by the National Institute of Standards and Technology in November, covers recommendations for the use of Personal Identity Verification credentials in access control systems.

The CoreStreet FIPS-201 Suite of products permits government agencies to upgrade systems to enable the verification of PIV cards, Common Access Cards, First Responder Authentication Credential cards and Transportation Worker Identification Credential cards without requiring the replacement of the existing system. The Solution verifies these cards at assurance levels as defined in SP 800-116.

The CoreStreet FIPS-201 Suite consists of the following components:

- CoreStreet FIPS-201 F5 System: Adds PIV, CAC, FRAC and TWIC credential compatibility to an existing PACS
- CoreStreet FIPS-201 Device Developer Bundle and CoreStreet FIPS-201 Head-end Developer Bundle: Software developer kits allowing OEM vendors to build SP 800-116 compliance into their products.

The other two announcements deal with CoreStreet's PIVMAN product. The PIVMAN Suite of software products provides solutions for identity and access management.

The standard CoreStreet PIVMAN Solution aggregates identity and attribute information from a variety of trusted sources for access to government buildings, port facilities or disaster sites as part of the National Preparedness Framework. Through integration with Lenel's OnGuard offering, the CoreStreet PIVMAN for Lenel Solution allows access levels configured in OnGuard to be displayed on mobile handhelds running the CoreStreet PIVMAN Client software.

Further, the CoreStreet PIVMAN for Lenel Solution retrieves audit logs from the clients and uploads them to OnGuard for display in the alarm monitoring application, and for use in activities such as mustering and reporting.

Also, CoreStreet and MaxID have formed a partnership to market the CoreStreet PIVMAN Solution on MaxID's iDLMax biometric handheld device.

VeriSign launches PKI platform for governments

VeriSign, Inc. has announced a new platform designed to meet the needs of governments looking to implement and manage their own Public Key Infrastructure (PKI).

The new VeriSign PKI Platform is an in-premise solution modeled after the same architecture that VeriSign has deployed as a managed service for customers around the world. This deployment model allows governments throughout Europe, Asia, the Americas, Africa and the Middle East to adapt to specialized security requirements that may be placed on such critical national infrastructure.

ID SHORTS

The VeriSign PKI Platform gives governments a way to offer citizens fast and easy access to e-services such as health and welfare programs, e-passports, and national ID programs.

PKI enables countries to leverage authentication, encryption, and digital signature technologies when issuing identity certificates, business certificates, and device certificates. The trust enabled by these certificates helps governments streamline operations, minimize the risk of fraud and waste, and disseminate information more easily and securely.

Recently, VeriSign has implemented several nationwide solutions with local partners, including:

- Greek Ministry of Interior: The Greek government's e-Gateway uses digital signatures to authenticate citizens and secure certain electronic transactions
- Receita Federal Brazil: Tax card in Brazil enables citizens to securely send income tax submissions via the Internet using PKI.

South Dakota taps L-1 for driver licenses

L-1 Identity Solutions Inc. was awarded a contract by the South Dakota Department of Public Safety for a complete driver license issuance system. The seven-year contract is valued at $8.8 million.

The new South Dakota system provides a process that minimizes the chance for fraud to occur at any point in the issuance process. The process incorporates a workflow for applicant enrollment based on document scanning and authentication technologies that validate breeder documents presented as proof of identity and facial verification of individuals as part of an image capture system.

Zebra launches speedy retransfer card printer

Zebra Technologies, a Lincolnshire, Ill. provider of specialty printing and automatic identification solutions, has rolled out its latest model, the Zebra ZXP Series 8, a retransfer printer that includes options for smart card encoding and networking. The printer is designed for such applications as high-security ID cards, driver licenses, gift cards and financial cards.

The ZXP Series 8 printer delivers photo quality, over-the-edge, high speed printing on different types of cards, including those with uneven surfaces such as smart cards, polycarbonate cards for security applications, and bio-polymer cards. The printer is available in single- and dual-sided printing configurations.

Options include a magnetic stripe encoder, combination smart card contact and contactless encoders, a contact station, USB or ethernet connectivity and security mechanical locks. Planned future options include support for a UHF Gen 2 RFID encoder, single- and dual-sided laminator, and 802.11g wireless connectivity. The printer will be available in the second quarter.

Confidex ships two million contactless paper tickets to Turkey

Confidex, a Tampere, Finland-based supplier of contactless limited use tickets and RFID tags, says it has delivered more than two million of the paper tickets to Konya, Turkey for the city's mass transit bus and tram system. The ISO-14443-A-compliant tickets were purchased by Teknikkart, an Istanbul-based smart card manufacturer.

Konya's mass transit system includes 248 buses and 60 trams with more than 2,070 bus trips and 310 tram trips each day. Konya officials estimated that passengers took more than 60 million trips during 2008.

The Confidex paper contactless tickets allow passengers to take two trips using a single ticket and provide the transit system with single ticket ride data via the ticket's serial numbers. The tickets can be read in 0.3 seconds.

The Confidex paper tickets can be printed and personalized according to the individual customer's requirements and delivered as either single cut or, as in Konya's case, on reel or fan folded.

L-1 unveils TWIC access control reader

L-1 Identity Solutions Inc. expanded its line of government access control solutions with the release of the TWIC-Station, a new access control device capable of reading a range of secure government credentials based on the FIPS 201 standard including Transportation Worker Identification Credentials, Personal Idetification Verficiation IDs and Common Access Cards.

The device also offers single or multi-factor authentication control with support for PIN codes and is capable of matching the fingerprint of a cardholder to the biometric stored on the card.

The L-1 TWIC-Station meets the latest TWIC Reader Hardware and Card Application Specifications issued by the Department of Homeland Security and Transportation Security Administration. It supports multiple credentials based on the FIPS 201 model and can read PIV fingerprints.

The unit's fingerprint algorithm is GSA-approved and FIPS 201 compliant and the UPEK TCSI fingerprint sensor offering 500 DPI is FIPS 201 compliant and FBI approved.

The federal TWIC program provides a tamper-resistant biometric credential to maritime workers requiring unescorted access to secure areas at U.S. ports and to vessels regulated under the Maritime Transportation Security Act. The cards are also issued to all U.S. Coast Guard credentialed merchant mariners. Government employees accessing maritime ports and vessels can use a PIV or CAC identification card for entry.

TWIC and PIV secure credentials are based on FIPS 201 that requires all government agencies to authenticate employees, contractors, and civil servants using strong authentication, including biometrics, for access control.

University establishes M-numbers for increased identity security

Students at Murray State University in Kentucky are having to adjust to a new student ID system that has eliminated the Social Security number as a student identifier. Like many other schools, the university is making the change to protect students' privacy and guard against ID theft.

The new M-number is generated from the college' s Banner system, an integrated software solution developed by Sungard Higher Education, that many colleges and universities use to manage their business operations. The numbering change will affect food services, the bursar's office, housing and any other place where the student's ID card is used.

SPS selected for French ID

The Imprimerie Nationale, the French national printing house, has announced the selection of Smart Packaging Solutions (SPS) to manufacture portions of future secure ID cards for France. SPS is a specialist in identity solutions, providing microelectronic components for national identity cards, driver licenses and biometric passports.

Imprimerie Nationale is the only company authorized by the French government to print high-security documents and ID cards featuring built-in security measures.

Law would expand biometrics at sea program

The U.S. House of Representatives passed legislation that requires all interdicted aliens at sea to be screened against Department of Homeland Security biometric watch lists. The legislation was sponsored by U.S. Rep. Gus Bilirakis (R-Fla.), member of the House Homeland Security Committee.

H.R. 1148 would require the Secretary of Homeland Security to formalize and expand the mobile maritime biometric identification program to combat aliens unlawfully attempting to enter the United States. The bill also requires DHS to ensure this biometric system is integrated into other systems within DHS and other agencies.

Homeland Security and the U.S. Coast Guard have had a pilot in place testing biometrics at sea.

Belgium expanding electronic ID program to children

The Belgian government is expanding it's electronic identification card initiative to include all children under the age of 12. The program consists of a dedicated electronic ID with specific features intended to increase the child's security in emergency situations.

In particular, a special hotline number is printed on the card body of the child's ID card so that his parents can be alerted as soon as possible. Zetes is the systems integrator for the project and Gemalto is providing the smart cards.

The size of a credit card, the new Kids-ID card features three main functionalities. First, it acts as an electronic national ID credential for Belgian children and also serves as an official travel document in most European countries. It contains all ID information as well as the child's photograph. This data is printed on the card body and also stored in the microprocessor.

The second capability is protecting the child in emergency situations. In case he/she gets lost, or is the victim of an accident, the hotline number printed on the card body enables notification of the next of kin or friend. The caller dials the hotline number and enters the child's 11-digit National Registry number. The call is immediately transferred to the first number on a list of up to seven contact phone numbers that the parents have selected upon card issuance. If this person is not available, the caller is immediately connected to the second number on the list, and so on until somebody is available. If no one is, the call is routed to the Belgian Child Focus hotline, operational 24 hours-a-day.

Lastly, the Kids-ID card can be used on the Internet for safer access to online chat and for use of services that require identification. A PIN code enables automatic authentication of the child and grants him access to web services he is allowed to use. Other potential uses include accessing library books, sport club membership or health care access.

Fedict (FPS Information and Communication Technology), the Federal Public Service of Belgium in charge of developing e-Government projects, has just started deploying the Kids-ID program.

Kids-ID is part of Belgium's nationwide electronic ID program, launched in 2003. In January 2009, the number of e-ID in use exceeds 8 million, representing over 90% of the targeted population, according to Fedict.

Gemalto provides first electronic student card in Serbia

Gemalto is providing the first multi-application contactless student card for identification and payment in Serbia. The cards have been delivered to Poslovno Informacioni Sistemi, a Gemalto reseller, which supplied the personalization solution for universities to issue cards directly to students.

The card is already in use by more than 30% of Serbia's student population, in the cities of Belgrade, Kragujevac, Nis, Novi Sad and Subotica. Deployments in Cacak, Kosovska Mitrovica and Uzice are currently in progress.

In addition to digitally identifying students, the Gemalto card is used for EMV debit payment. With the card, users can pay at student restaurants, as well as receive discounts at local establishments. The contactless functionality allows students to enter buildings and record their attendance in class simply by holding the card up to a reader.

Gemalto has shipped more than six million electronic student cards for universities around the world, primarily in Hungary, Latin America, Morocco, Poland, Portugal, Spain, the United Kingdom and the United States.

Air France trials biometrics for passenger boarding

French airline, Air France, has begun a trial of contactless smart cards with passenger biometric data to allow for expedited check-in. The system is in place at automated gates that enables the passenger to pass when the card information matches the sample given by the passenger. The traveler submits both index finger and thumb prints.

The trial is only for members of Air France's frequent flyer program and for flights between Paris and Amsterdam. However, if the trials prove successful they are looking to expand and add capabilities of the card to include information for car rentals and other airport services.

Visa testing new payment card security

Visa is piloting two new systems designed to prevent credit card fraud. One of the tests involves Fifth Third Bank. The institution is issuing cards that have unique digital fingerprints on the magnetic stripe of the card. Each stripe contains unique characteristics that can be captured and used to verify that specific card.

Another technology is being piloted at OfficeMax Inc. It involves the use of a challenge-response technique at the point of sale. When making a purchase the consumer is asked to respond to different questions, such as ZIP code, the last four digits of the phone number, or the first three digits of their area code, as part of the transaction approval process.

PayPal joins GlobalPlatform

PayPal has become the latest member of GlobalPlatform, the international specification body for smart card infrastructure.

Joining as a Participating Member, PayPal will play an active role in GlobalPlatform's Card Committee and its various working groups. Representatives from PayPal will also have the opportunity to participate on the GlobalPlatform Advisory Council and within the organization's Task Forces, including the important Mobile Task Force, sharing best practice and technical knowledge with other members.

Sony names MxN Media Group to FeliCa System Integrator program

Sony Electronics has signed MxN Media Group, as an authorized FeliCa technology deployment channel partner. The company is part of the FeliCa System Integrator Application Developer program.

MxN Media Group delivers digital merchandising products and solutions including menu systems, merchandisers, theater box office presentation systems, digital movie posters and more. New products in its road map include interactive and transaction-focused systems such as electronic couponing, ticketing, payment and loyalty using FeliCa contactless technology.

The FeliCa System Integrator Application Developer (SIAD) program offers integrators and application developers the resources, training and support necessary to deploy FeliCa technology-based solutions.

New Zealand Immigration says biometrics would have caught 9/11 terrorist

While making their case for a more than $100 million upgrade in biometric technologies, Immigration New Zealand, the country's immigration agency, stated that had the biometric systems been in place by 2006, the agency would have caught known terrorist and co-conspirator in the 9/11 attacks Rayed Mohammed Abdullah, according to a Stuff.co.nz article.

Further, identity program manager, Aaron Baker worries that the 316 cases of identity fraud that were detected between 2005 and 2008 may be nothing compared to how much fraud is actually going on. He is hopeful that a proper biometric system being in place could ease those worries.

With a new system in place, Baker asserts that the new immigration system would require all visa applications include a biometric sample. Further, enrollment would be available at the New Zealand border for first time visitors with returning visitors checking in via an automated gate. Both systems would be actively checking information given against known terrorists and wanted criminal databases as well as for fraudulent information.

French magazine embeds RFID linked to online content

The French technology and lifestyle magazine Amusement is offering an RFID-enabled bonus for purchasers of its latest issue. Each copy of the new issue, Amusement's fourth, has an RFID tag embedded in a page which can be scanned to access exclusive online content.

Amusement's RFID enhancement is the result of a collaboration between tech company Violet and GS1 France. An RFID tag provided by the Finnish RFID maker UPM Raflatac is fixed to the center of the magazine's first double page. This tag is designed to work with Violet's new

Mir:ror RFID interrogator, which plugs into a computer's USB port. Passing the magazine page near the device launches the exclusive content on the integrated computer.

According to a spokesperson for GS1 France, the RFID-enabled magazine serves as a way to expose new RFID applications, already deployed in the business-to-business world, to the general public.

"As the cost of RFID components has already come down significantly, we see opportunities for totally new industry take-offs based on innovative and value increasing services for the consumer," says Pierre Georget, CEO of GS1 France.

Florida deploys RFID monitoring for I-95 "HOT" lanes

The Florida Department of Transportation has turned to an RFID-enabled solution to create the state's first variably priced toll lanes. The project, known as "95 Express" turns two lanes of I-95 in Miami-Dade county into high-occupancy tolling (HOT) lanes, available for use by both high-occupancy vehicles and single drivers, with the single drivers tolled at variable rates based on traffic congestion patterns.

I-95 between Miami and Fort Lauderdale is one of the most heavily traveled highways in the U.S., carrying over 290,000 vehicles per day and with traffic volumes predicted to exceed 360,000 vehicles per day by 2030. Widening the highway was cost-prohibitive, so planners turned to alternate solutions to manage the congestion.

The 95 Express project was designed to create non-stop, express toll lanes. Two lanes in the northbound direction were outfitted with RFID-enabled open-road tolling apparatus. In the HOT lanes, variable pricing is used during peak travel times to manage capacity and help maintain traffic flow at speeds greater than 45 miles per hour.

The RFID applications were provided by TransCore, a division of Roper Industries. Funding for the 95 Express project came from the U. S. Department of Transportation as part of the Urban Partnership Agreement to fight traffic gridlock. The project will expand the express lanes throughout the region in the next year. Similar deployments are also under way in San Diego, Houston, Minneapolis, and Seattle.

2009

MAY

CTST 2009
May 4 – 7, 2009
Ernest Morial Conv. Ctr.; New Orleans, LA

IFSEC 2009
May 11 – 14, 2009
NEC Birmingham; Birmingham, UK

Near Field Communications World Europe 2009
May 12 – 14, 2009
Hilton Tower Hill ; London, UK

2009 Biometrics Institute Australia Conference & Exhibition
May 28 – 29, 2009
Amora Hotel Jamison; Sydney, Australia

Transportation Security Forum 2009
May 28 – 29
Hyatt Regency Paris; Paris, France

JUNE

TranSec World Expo
June 3 – 4
Amsterdam RAI; Amsterdam, Holand

European Supply Chain and Logistics Summit 2009
June 8 – 10, 2009
Swissôtel Düsseldorf, Germany

RFID Smart Labels USA 2009
June 9 – 10, 2009
San Francisco, California

Contactless Cards and Payments: The Impact of Regulation And Risk
June 22 – 23, 2009
Copthorne Tara Hotel; London, UK

Large-area, Organic & Printed Electronics Convention
June 23 – 25, 2009
Congress Center; Messe Frankfurt, Germany

September

ASIS International 2009
September 21 – 24, 2009
Anaheim, California

2009 Biometric Consortium Conference and Technology Expo
September 22 – 24, 2009
Tampa Convention Center; Tampa, FL

October

ISC East 2009
October 28 – 29, 2009
Jacob Javits Convention Cntr., New York, NY

The 8th Annual Smart Cards in Government Conference 2009
October 28 – 30, 2009
Washington Convention Center;
Washington, DC

ID and security hackers: Do they help or hurt the industry?

Zack Martin
Editor, AVISIAN Publications

It was the week between Christmas and New Year's in 2007 when executives at NXP were notified that researchers made had hacked the Mifare Classic product line.

The presentation of the results was made at the 24th Chaos Computer Congress in Berlin and showed how to reverse engineer the Mifare Classic line of contactless smart cards. Henri Ardevol, Mifare's business manager at NXP, found out when a journalist called asking for comment on the presentation. "There was no pre-warning from the Chaos Computer Club or the researchers," he says.

NXP researchers spent the next month looking at the research and then notified end users of the vulnerability, Ardevol says. The company also met with Karsten Nohl, one of the researchers who presented the attack.

While vendors don't necessarily welcome the hacks, they aren't altogether unwelcome either. "Overall their presence in the ecosystem is a valuable one," Ardevol says. "We have come to recognize they are important to stakeholders because they can bring value on the technical side."

Prior notification

Technology providers prefer that researchers notify them of a hack before releasing the information to the general public. Vendors also take issue with the mainstream media portrayals of these attacks, frequently misinterpreting the findings and overstating the impact.

After the Mifare Classic weakness was announced there were media reports stating that every contactless payment card was at risk. That wasn't the case. Other claims have been made against electronic passports and other smart card systems that, according to some in the industry, have been blown out of proportion as well.

The Mifare Classic hack, however, is probably the most significant attack against a smart card system. After Nohl's announcement, two others were made public against the same system in 2008. As smart cards and other identity systems become more mainstream it's likely the technology is going to be challenged more.

More trouble for the Mifare Classic line

The Mifare Classic line includes the Mifare 1K, Mifare 4K and Mifare Mini products. The cards are used worldwide in transit fare collection systems, access control solutions and government ID systems. Large issuers include transit projects such as London's Oyster program, The Netherlands' OV-chipkaart, and Boston's Charlie Card. The line was first released in 1994.

Since the attacks were made public NXP has introduced new technology that takes care of some of the security gaps, Ardevol says. It introduced AES cryptography to more of its products in an effort to shore up security gaps. Still these modifications could not protect the existing Classic line of products.

Following Nohl's attack, the Radboud University Nijmegen presented a publication that described some of the practical attacks that can be carried out against the product line.

The university shared the information with NXP before publishing it. But the semiconductor manufacturer didn't have time to put all the proper countermeasures in place before researchers wanted to release the information. So NXP sued Radboud University Nijmegen to block details of the hack from being released.

Ardevol says that NXP has a working relationship with the university but was forced to take these steps when the university wanted to go public. "Our disagreements were on the timing," he says. "Even during the day in court we were having very healthy and constructive discussions on security."

The court denied the injunction and researchers released the information. Ardevol says NXP is still working with the university to fix vulnerabilities and come up with countermeasures.

In the other example of the Mifare Classic hack last year, MIT students were sued for presenting their hack of the Charlie Card. The students

were scheduled to present their findings at DefCon, an annual computer hackers' convention in Las Vegas in August. But the Massachusetts Bay Transportation Authority (MBTA) was granted a temporary injunction that prevented the presentation.

The MBTA stated that they violated the federal Computer Fraud & Abuse Act. The agency has also confirmed that there are security vulnerabilities with its transit card and is working to correct them.

While the gag order was in place the students' presentation was available for download online. The 87-page report, "Anatomy of a Subway Hack," details the variety of different ways the students were able to get free rides. The case against the students was settled and dismissed.

The major issue for industry vendors is how these attacks are announced. "The vulnerability should first be communicated to the people who can do something about it and then to the general public," Ardevol says.

When Nohl presented his findings on the weakness of the Classic line he didn't notify NXP ahead of time, he says. But his presentation didn't release specific information on how to break the technology, it just detailed that the vulnerability exists.

Nohl and his team spent two years working on the Mifare project. The gist of the effort, as he describes it, involved taking one layer of the silicon chip off at a time and then taking photos, to reconstruct the chip's structure. They had computers recreate the structure so they could understand what the chip was doing and output the code so the computer could access the cryptography.

Nohl was a University of Virginia graduate student when he did the research on Mifare Classic and is now an industry consultant. The idea was to look at technologies the public uses on an everyday basis but have never been publicly interrogated. "Mifare is very popular in public transportation," he says. "In Boston you pay more if you don't use the card."

Nohl knows that notifying vendors of a potential weakness is one of the bigger issues in the industry. "Before we released details of the actual vulnerability we made sure the manufacturers were aware of the vulnerabilities and are already working on a successor technology."

Hackers on campus

Hacking can mean many things. The image it conjures for most is that of a young man in a dark room lit by nothing more than the glow of a computer monitor, trying to break into some top-secret government system or steal credit card numbers.

And while some of the hacks against smart cards could impacts thousands if not millions of people, college students are testing the vulnerabilities of campus ID cards. On college campuses hacking can mean a number of different things and threats can come from students as well as outsiders. Hackers attack university databases and systems but they also are targeting the student ID card, which relies upon magnetic stripe as its line of defense.

Harvard hacker ushers in contactless

What happened at Harvard is just about a campus card director's worst nightmare. In July 2008 a Harvard undergraduate student was caught making fake Harvard University ID cards. Not just any cards, but duplicate cards of those belonging to the University President and two other high ranking administrators.

The student was able to replicate the magnetic stripe on the back of the card and gain access to buildings and gates across campus with only knowledge of the individual's university ID numbers and a $200 card reader purchased on eBay. He was also able to make purchases using the individual's Crimson Cash accounts, which are used to pay for items on and off campus.

The hack was the impetus for Harvard to launch new IDs for the students, faculty and staff in the Faculty of Arts and Science. The university rolled out iClass contactless smart cards from HID Global for physical access to facilities. The new card has two magnetic stripes on the back that are used for payments and other functions, according to the Harvard Crimson.

The Carleton case

Carleton University's card program was the victim of a hacker, sort of, says Kathleen Kelly, campus card coordinator at the Ottawa, Ontario university. "I would use the term 'hacked' loosely," she stresses, nothing that the student was able to access students' personal information, but he didn't break into the campus card system.

The incident occurred in the university's computer lab where print stations are equipped with magnetic stripe readers. When a student

Difficult line to walk

But it's hard to find the right balance between notifying the public that a weakness exists while also giving the vendor enough time to fix the problem, Nohl says. "It would take eight years to replace the cards completely," he says. "We don't want to hold the research back that long. It's almost impossible to find a good time."

The tug-of-war between academics and businesses probably won't be ending either, says David Dix, an electronic payments expert at Cryptomathic. "The academics are sometimes seen as a hindrance," he says. "Once a vulnerability has been identified it might take months or years to fix but sometimes the academic wants to get it out sooner while businesses want it to take more time."

Dix classifies hackers into three groups: academics, organized criminals and hobbyists. The organized criminals are the worst and the ones the public most often thinks of because their activity can result in the loss of millions of dollars.

Holly Sacks, senior vice president of marketing and corporate strategy at HID Global, adds another category of hacker: publicity seekers. "Some just want a level of notoriety," she says.

The research these individuals do may be misconstrued, Sacks says. "The way the conclusions are being publicized are creating fear, confusion and doubt. The real issue I have is that those who are enabling criminal behavior are being irresponsible. They may not have ill intentions but they are showing people how to do it."

The Golden Rule passport hack is one that fits into the misconstrued category, says Tim Moses, CTO at Entrust. In this case a researcher was able to replace the data stored on the contactless chip in an electronic passport.

But what was left out of most media reports was the tool he used to make the changes is for testing and if the modified passport was checked with a real world e-passport reader the digital signature on the chip would not be verified, Moses says. "It's a tool, not an inspection grade system," he says. "He didn't follow the ethical hacking route and frankly it was a non story."

If hackers follow ethical guidelines and notify vendors beforehand they do have a place in the market, Moses says. "They serve a valuable purpose," he says.

prints a job he goes to the station, logs-in with user ID and password and swipes his ID to authorize the job to print.

The hacker did two separate things to gain the student's personal information. He installed key logging software on computer in the lab to capture user names and passwords as they were typed. He also installed another program on the print station to record information from the magnetic stripe of the student IDs, Kelly says.

He then took these separate pieces of information and was able to match the student's ID card information with the user name and password, Kelly says.

Nothing illicit was done with the stolen student information. After collecting the student information he sent a report to university officials and the student newspaper with the names and data of the 32 students whose information he collected, Kelly says. From the report, university officials were able to backtrack to figure out what the students had in common and where the information had been obtained. He was charged with mischief to data and unauthorized use of a computer. The penalties for the charges range from fines to jail time. The student voluntarily left Carleton.

Though the student did not use the information in a malicious manner, the question of what could he have done remains. The mag stripe on the campus card can be used to pay for laundry, printing and small purchases at the university, Kelly says. There is a $12 daily spend limit on the card for vending machine or unattended purchases. The card is also used for physical access to two of the residence halls. A PIN is not required for either the payment or access transactions.

If the student had created fake cards using the information, he potentially could have gained access to the secured dormitories or made purchases with the stolen accounts. The usernames and passwords obtained could have enabled access to email accounts or campus services.

Mag stripe for payments, but not for access

At George Washington University in Washington DC, Ken Pimentel's biggest fear is someone copying the mag stripe on the card and using it to gain access to a dorm or somewhere else they should not go. "There's nothing wrong with mag stripe at the point of sale," says Pimentel, director of the university's GWorld Card Program. He admits that they have experienced unauthorized people using accounts to pay for items on campus, but says, "someone can steal some money and we can get it back, but it's much more dangerous when they can get into a door."

Securing access control is Pimentel's main concern. He would like to switch to a contactless smart card for access control but says it's too costly in the current environment. "I've been telling [university officials] that we need to get away from mag stripe because it's vulnerable," he says.

Replicating a mag stripe can be easy with the right equipment, says Pimentel. But universities also need to be sure to secure all the back end physical access control equipment as well. The reader, door controller and wiring all need to be secured so nobody can skim numbers from the devices. George Washington University has 44,000 active cardholders and more than 475 access control readers across its campus, Pimentel says.

Protecting the wiring for physical access control system is important. "People can get access to the readers and watch the communication," he says. George Washington runs all the wiring for the system in conduit to prevent unauthorized access.

Just the beginning

As smart card technology becomes more prevalent it's security is likely to be tested more by both ethical and non-ethical hackers. "With more technology out there it gives researchers more to play with," says Cryptomathic's Dix.

"It's an arms race," he says. "It's a war and every war leads to greater advances in technology. More technology will lead to more hackers which will lead to greater advances."

Vulnerability testing could become more standard

Vendors typically have employees on staff who test the security but Moses expects to see others step up too. "I think we'll see the equivalent of biological containment labs where you have people working with computer viruses in a lab to see what they do," he says.

HID's Sacks says some of the testing houses that review smart cards for standards compliance also get into the security testing arena. "I can see that extending into technology vulnerability testing," she says.

Standards-based technology is the best

Overall the smart card industry does a pretty good job, says Nohl. "The whole industry is getting better, it's like evolution where only the fittest survive," he says. "Many researchers are looking at these cards and they are finding vulnerabilities, but they're not finding anything as bad as with Mifare."

End users wanting the most secure technology should choose standards-based cards and readers, Nohl says. Federal standards are created by many people, trying to offer the best technology. The odds are that technology will be better than any from a single company. "Find the best fitting government standard and go with that," he suggests.

Exploring the Enhanced Driver License hack

Ari Juels knows the impact he can have when looking into identification technologies. The chief scientist and director of the RSA Laboratories has researched the electronic passport books, contactless credit cards and most recently the Passport Card and Enhanced Driver License.

One reason the U.S. Passport has a metallic cover that prevents it from being read unless open may be the research Juels did in 2005 that showed that information could be read from closed passport books. His research into the Mobile Speedpass payment device a couple of years ago also caused the issuer to make security improvements.

It's not clear yet if his latest research will have the same impact. Last fall Juels released a report citing problems with the Passport Card and Washington State's Enhanced Driver License. Both of these documents enable expedited passage through land and sea borders and are called for by the Western Hemisphere Travel Initiative.

The risk to individual travelers is low, but the problems create systemic weaknesses in the border-crossing system, Juels says. The tags store and transmit a unique ID number that correlates to the cardholder's photo and other information in a Homeland Security database. No personal information is stored on the card.

Among the risks the researchers point to, however, are the possibility that the tags could be cloned to produce false IDs. Hackers could also transmit a code that would cause the tags to self-destruct. And while the cards do not contain personal information, a long-distance scan of the cards could enable criminals to track individuals without their knowledge.

This was seen in action earlier this year when the ACLU gave Chris Paget $250 to buy some equipment to see if he could pick up individual EDLs and Passport cards. Paget, an information security specialist, bought the equipment on eBay and installed it in his car. He then drove around San Francisco to see what he picked up.

He had some hits, even though California isn't issuing EDLs. Paget posted the video of his drive on YouTube. The video had more than 205,000 hits as of early April.

Paget is concerned about the long-range RFID tags being used to track individuals. Homeland Security officials have said they don't think it's realistic for individuals to be tracked with either document. It would be too time consuming to try and connect the document ID number with an individual, but Paget disagrees.

He points to UK-based water park Alton Towers. The park offers a video souvenir package called YourDay. The wristbands activate a system of 36 cameras scattered about the park, which films the guest and stores the footage under the appropriate individual's account.

At the end of the day, the guest can choose to purchase a DVD of his trip, with his personal images blended with stock footage of the park.

"This is clearly a commercial implementation of tracking technology, it's viable," Paget says. "For DHS to say it's not worth anyone's time to do it is wrong."

Budget woes create opportunities for campus ID programs

Taran Lent
Vice President, Product Development and Co-Founder, CardSmith

Unprecedented strains in the U.S. financial system and economy are putting serious money pressures on colleges and universities. These pressures did not exist as recently as one year ago. Endowments are down, costs are up, and financing for education is in crisis. The turmoil in financial markets has hit quickly and hard. Its impacts are likely to be felt well into 2009, 2010, and possibly beyond.

As we look forward it will be imperative for institutions and administrators to review all departments and operations in an effort to achieve maximum cost effectiveness and operating efficiency.

The total cost of operating an in-house campus card system is already high and climbing. The past several years have seen increases in the cost of software licenses, required system upgrades and interface fees. This cost trajectory is putting more pressure on already strained operating budgets. At the same time, staffing requirements and costs have also increased significantly, as the scope and complexity of programs has expanded.

It is common for well-developed campus card programs to require three to five employees and annual operating budgets of a million dollars or more.

In response, industry suppliers and vendors need to offer innovative solutions to ease the cost and complexity of running card programs. Fortunately payments processing technologies and management methods have evolved, creating much-needed alternatives to buying, implementing and self-managing a traditional campus card system.

Software as a service, remote hosting, multi-school collaboration/sharing, open-source software and even complete program outsourcing are now commercially proven options. The cost savings of managed services are very real and are an imperative for any institution seeking operating efficiency while at the same time enhancing student services. In this context, my predictions for 2009 are:

1. The global economic crisis will continue to pressure endowments, enrollments and budgets, forcing spending cuts.

2. Administrators will need to aggressively re-evaluate and reform capital and labor-intensive service models.

3. Reliance on high-cost proprietary software, hardware and systems will be scrutinized and will eventually succumb to low cost, community-based, and open-source solutions.

4. Outsourcing campus card operations will become a crucial strategy to control and reduce costs.

5. Internet-based software will make it easier and more affordable for schools to centrally deploy, host and scale applications directly or in concert with professional service providers.

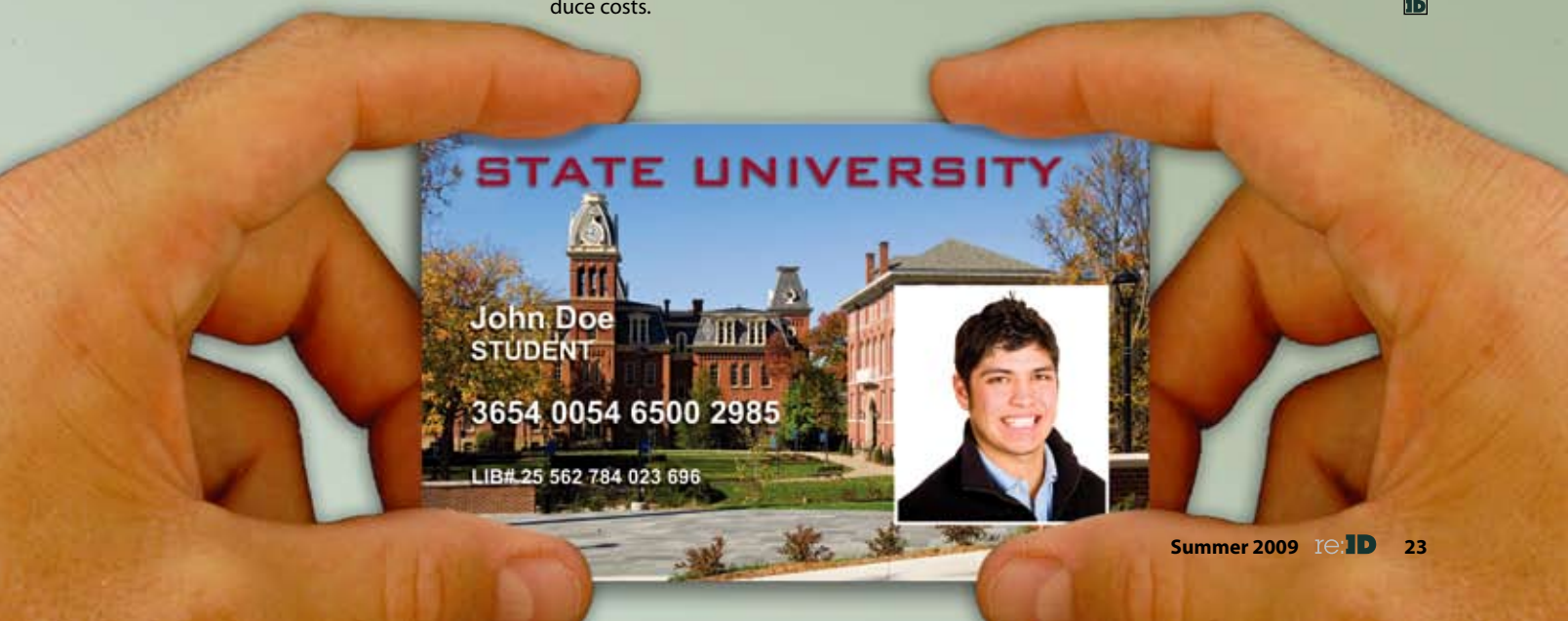
6. Student access to credit will diminish severely, increasing the need for financial support from home and making pre-paid campus card accounts and their inherent budgeting control more popular than ever.

7. Focus on cost control will overshadow technology and feature enhancements.

8. Neighboring schools and consortia will aggressively seek new and innovative ways to collaborate and share costs.

Since their inception, campus card programs have brought meaningful operating efficiencies to educational institutions by eliminating cash handling, reducing labor costs, consolidating reporting, increasing security and more. While financial instability creates uncertainty and change, it also fosters opportunity for those that can innovate and creatively navigate the pitfalls of the status quo.

The next big milestone in the campus card industry is that it discovers the cost efficiencies and service improvements made possible by a new generation of Web-enabled technologies and business models.



The eyes have it

Has the time for iris biometrics come?

Zack Martin
Editor, AVISIAN Publications

When talking about biometric technologies the list typically goes fingerprint and then iris, in that order.

Fingerprint biometrics have been the standard because it has been around longer and has a proven track record. But advances in iris technology along with new vendors and products may signal that the technology is about to take off.

The U.S. Department of Homeland Security has tested iris systems from three vendors for possible use with the US VISIT program, which checks all foreign visitors' fingerprints against a watch list.

Iris will also be integrated into the FBI's Next Generation Identification (NGI) system. The NGI is replacing the Integrated Automated Fingerprint Identification System, which incorporated fingerprints and biographical data. The new system adds iris as well as photos of tattoos to the profile.

"Fingerprints are the dominant one in terms of shear numbers but iris will start to catch on," says Victor Lee, senor consultant at the New York-based International Biometric Group. Iris is already more popular in the middle east, where the technology has seen its largest deployments, he adds.

But the technology may be starting to catch on in the U.S. and other western countries. Multiple vendors are offering systems that are easier to use than earlier systems and more initiatives, such as electronic passport projects in Europe, are calling for iris.

At Homeland Security, iris was tested as part of its Multi-Biometric Technology Evaluation (MBTE) project, an on-going technology evaluation that US VISIT started in January 2008. This is a effort launched in partnership with the National Security Agency, the U.S. Naval Academy and the National Institute of Standards and Technology to examine alternative approaches to capture biometrics to improve security and facilitate entry.

In July 2008, the evaluation team collected data from individual iris technology vendors. This evaluation was conducted in a laboratory environment, and the data was used to determine the level of image quality. The test looked at cameras from LG, AOptix and HBox.

In November of 2008, the MBTE team provided a demonstration of interoperability of iris sensors in a multi-vendor environment. The demonstration showed live matching across iris systems from multiple vendors.

In addition to the demonstration, evaluation data was collected to measure "real world" metrics including failure to enroll and failure to acquire rates. More than 100 US-VISIT employees and contractors participated in the MBTE evaluation phases at US VISIT headquarters. Details of the next step of the projects were not available as of press time.

Social issues impact biometric acceptance

Cultural issues have been an obstacle for iris biometrics in western countries and a reason why it has thrived in the Middle East, says Tim Meyeroff, director of North American sales at LG Iris. The Middle East has the largest deployment of iris technology, using it for border control and other applications.

The iris cameras in place require the user to be 10 to 14 inches in order to authenticate, Meyeroff says. For westerners this is uncomfortable, but not so for middle easterners. "It's more culturally acceptable to be that close to someone and be comfortable with it," he says.

And while this has worked in iris biometrics' favor, the same cultural issues have held fingerprints back in that region, Meyeroff says. "There's a much greater hesitation to touch something in the Middle East," he says.

AOptix classifies its iris cameras (left) as 'iris at a distance' while Global Rainmaker (right) calls its products 'iris on the move.'

Lee says iris is in a position to start making up some ground on fingerprints. An individual's iris pattern remains stable after the age of one year, but many factors can cause fingerprints to change. Some also say that iris is more difficult to spoof than fingerprints.

Usability has been the major knock against iris, Lee says. For some cameras a user had to get within inches of the scanner and it took some manipulation for enrollment and subsequent authentications. It also was difficult for taller people to use the systems because the cameras would be mounted at a lower position causing problems.

New iris systems improve usability

The newer iris systems attempt to solve these usability issues. These "iris at a distance" and "iris on the move" products can authenticate individuals from three to five feet away. But the systems are all fairly new and have few, if any, deployments.

AOptix Technologies Inc. rolled out its first iris-at-a-distance product in March. The Campbell, Calif.-based company is a Silicon Valley startup founded by astronomers from the University of Hawaii, says Phil Tusa, the company's vice president of biometric programs. The astronomers were working with adaptive optics for deep space imaging, "to improve imaging quality by correcting for the atmospheric disturbances," he says. It occurred to developers that the same image correction techniques could improve iris biometric imaging.

AOptix is different with its concept of operations than some of the other new iris technologies, says Tusa. "Our concept is to ask the subject for two seconds to look at the device and open their eyes," he says. "This will greatly improve matching accuracy results and we're not going to have bad images."

Other products don't have this requirement, but by asking for it AOptix says it can get better images and lower the failure-to-acquire rate, Tusa says. The system can also communicate with the user and tell him where to stand. With systems that don't require a user to stop this would be problematic. The AOptix device can capture iris images and facial images at the same time.

Sarnoff Corp. offers a complete portal product to its iris customers.

The first products shipped in April, Tusa says. Most of the first systems are going for pilots and other demonstrations.

Sarnoff Corp. and Global Rainmaker classify their technologies as iris on the move. Both authenticate individuals as they go through a checkpoint. For example, a camera could be set up at an airport security checkpoint and authenticate travelers as they move through the metal detector.

Along with the US VISIT project, Sarnoff participated in a test at Schipol International Airport in Amsterdam. Iris technology has been in use there for its trusted traveler program for years and the airport is thinking about upgrading, says Ray Kolczynski, product manager at the Princeton, N.J.-based company.

Sarnoff says it can capture iris images at about 10 feet and process 30 individuals a minute, Kolczynski says. But the system could be tuned to pick up images from as much as 98 feet away. "We offer real-time capture with minimal user cooperation," he says.

Through the years Sarnoff has received funding from the U.S. intelligence community, including the National Security Agency, the CIA and Department of Defense, Kolczynski says.

The individuals involved with Global Rainmaker's technology participated in some of the first iris systems. Keith Hanna, Chief Technology Officer and executive vice president at Global Rainmaker, worked with John Daugman, who holds some of the first patents on iris recognition technology.

Hanna is now a partner with Global Rainmaker and helped create the HBox, says Hector Hoyos, president and CEO at the New York-based company. The HBox technology is capable of authenticating 50 people per minute without any user cooperation at between five- and six-feet away, Hoyos says.

The HBox also has participated in the US VISIT and Schipol Airport trials and also has a full-scale deployment scheduled, Hoyos says. The company is working with a corporation to install iris cameras throughout for physical access. Cameras will be deployed in the garage, in the main lobby and on every floor for access. "When you look at any type of biometric access control system most of them use a token, a mag stripe of other type of card," he says. "We have moved away from the card."

Besides usability, the other obstacle for iris biometrics has been price. The cameras traditionally have been more expensive than fingerprint scanners. Though International Biometric Group's Lee says some of this is a fallacy. "There is a tendency to compare apples to oranges," he says. "People compare fingerprint scanners that are being used in laptops to iris scanner for access control. If you're talking about [fingerprint technology for] very robust access control systems the two are similar."

Hoyos says its eye swipe portal will retail for $1,995. AOptix hasn't released final pricing, but Tusa says the system is more expensive than high-end fingerprint scanners like those being used for US VISIT, but lower than iris-on-the-move devices. ID

EMV takes aim at U.S.

Technology may be a solution to domestic payment card fraud

Like a massive tidal wave, EMV continues to roll across the world, changing the global payments landscape. Since UK banks first committed to EMV five-years ago, more than 100 countries have taken the plunge in efforts to stem credit card fraud.

But the U.S. has always remained outside the EMV plan. This, however, may be changing as fraud, technology and business is changing the payments landscape.

Brian Byrne, head of product technology for standards and specifications at Visa estimates there are some 730 million EMV cards and 10 million terminals in existence around the world.

Toni Merschen, group head of chip at MasterCard Worldwide, notes that the Single European Payments Area initiative requires 38 countries to complete the migration to EMV by Jan. 1, 2011.

EMV gets its name from the companies which originally created it, Europay, MasterCard and Visa. Seven years ago Europay merged with MasterCard and the new standards body was renamed EMVCo. Its members now include Visa, MasterCard, Japan-based JCB and its newest member, American Express.

EMVCo's primary goal "is to facilitate global interoperability and compatibility of chip-based payment cards and acceptance devices through deployment of relevant EMV Specifications," says an EMVCo spokesperson.

EMV also goes by "chip and PIN," because the card contains a chip and a PIN is required before a transaction is processed. But nowadays, that chip and PIN moniker may be misleading. As Byrne, points out, many countries are foregoing the PIN part of EMV implementation, the predominant reason being that many consumers don't want to remember a PIN.

The country most advanced towards EMV implementation is the UK, the banks their were the first to adopt chip and PIN, says Merschen. Other markets that have reached maturity for EMV migration on either cards, point-of-sales devices and ATMs include France and Turkey in Europe and Malaysia in the Asia-Pacific region, he adds.

The migration isn't easy. Merschen says a number of infrastructure changes are required to handle EMV. "For issuers, there are new data elements that need to be supported by the issuer authorization and clearing host systems. Card data preparation, including key management, and card personalization also require hardware and software upgrades," Merschen says. "On the acquiring side, the impacts are similar. Acquirer host systems must be able to receive new data fields from terminals, which also need to be upgraded from both a hardware and software perspective."

Glitches all but resolved

In the early days of EMV there were issues, Merschen says, such as a shortage of approved products, lack of customer and vendor expertise with EMV and areas where the specifications left implementation options.

That was then. These issues from the early days of EMV have largely been resolved, says Merschen. "Robust migration processes are available to guide the banks, merchant, and consumers in their migration involvement," he adds.

Visa's Byrne describes the early road bumps as minor. "This card issued in country A was having some acceptance problems in country B. In some cases, some of the older terminals wouldn't work properly, but that was usually due to configuration issues, fairly minor stuff."

EMV in the U.S.?

So with the U.S. sandwiched between two EMV countries–Mexico and Canada–most think it's only a matter of time before the U.S. joins the EMV parade.

Paul Beverly, president of Gemalto North America, believes increased fraud will mandate such changes.

In an article in the spring 2009 issue of *Regarding ID* magazine, Beverly wrote: "The rest of the world is well on the way to EMV implementation. Europe and Asia have long been issuing cards and … Latin America, faced with exploding credit card skimming fraud, is fully committed to EMV smart cards. .. Yet stakeholders in the United States still find fraud losses and identity theft risks acceptable. It is disappointing that U.S. companies are trailing the rest of the world in this area."

Charles Walton, executive vice president for payments for INSIDE Contactless, believes that the U.S. will ultimately get on board with the

EMV curbs fraud but criminals find other methods

Latest card fraud losses reported by APACS, the UK payments association, show EMV does work, but it's not a cure all. Certain types of credit card fraud will require other measures.

While 2008 fraud loss figures totaled about U.S. $902.5 million the two main areas of fraud were on transactions not protected by chip and PIN: Internet, phone and mail order fraud, and fraud abroad committed by criminals using stolen UK card details in countries yet to upgrade to EMV.

This second fraud type has nearly doubled in two years, providing more ammunition to those pushing the U.S. to become EMV compliant.

Phone, Internet and mail order fraud (card not present) accounted for more than half of those losses at U.S. $485.9 million, just a 13% increase over 2007 losses but is double the losses suffered in 2004.

Counterfeit card fraud increased 18%, to about U.S. $250 million. But that's down from the 46% increase reported in 2007. The vast majority of this fraud is due to criminals stealing card details in the UK to make counterfeit magnetic stripe cards for use in countries yet to upgrade to chip and PIN, says APACS.

"The industry continues to apply pressure on those countries, such as the U.S., where chip and PIN has still to be rolled out," the APACS report adds. "Increasingly effective use of intelligence systems and the ongoing global rollout of chip and PIN have contributed to this slowdown."

Although card fraud losses have increased, losses as a percentage of plastic card turnover amounted to just 0.12% in 2008, equaling about a tenth of a penny lost to fraud in every dollar spent. This, too, reflects EMV's "positive effects as well as the fact that we continue to use our cards more and more each year," says APACS.

As to card not present losses, that can happen with or without EMV. More retailers, APACS notes, need to encourage cardholder and retailer use of the secure codes found on the back of most credit cards.

However, one area where EMV is still vulnerable is with ID theft. Card ID theft losses have increased by 39% where criminals take over the running of another person's credit or debit card. This fraud typically involves a criminal obtaining a genuine card and a genuine PIN, and has contributed to the fraud increases seen at UK shops and cash machines.

secure cards. "We're seeing inherent insecurities in the system, such as the Heartland Payment Systems hack. It's only a matter of time before these will become intolerable."

Walton says hackers will look at the weakest point in the payment chain and exploit it. "If you start securing one point in the chain, it begins to expose the other points, the path of least resistance for water, will find the lowest point."

MasterCard's Merschen says that these fraud migration and data compromise incidents, plus the possibility of government regulation will lead several U.S. banks to consider EMV.

The handwriting is on the wall, so to speak. "It's inevitable that the U.S. migrate to EMV, primarily because fraud is escalating," adds Randy Vanderhoof, executive director of the Smart Card Alliance. "Major financial institutions in the U.S. are also international so it will not be a big step for them to issue these cards in the U.S."

Contactless and EMV

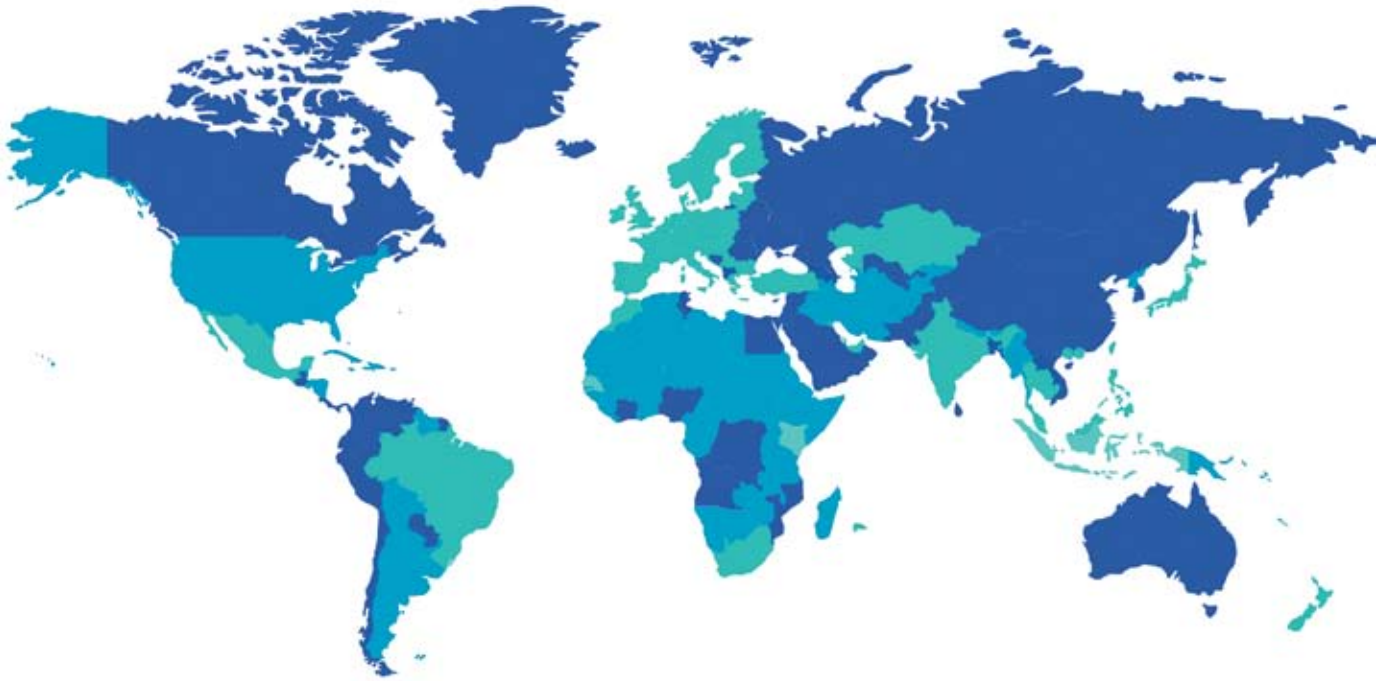
At first blush it would seem that contactless and EMV would be working toward opposite purposes, but Walton says EMV can run on top of contactless. "I would think of EMV as a security protocol that works with contactless as well as contact chips."

Visa is using EMV specs in its contactless payWave technology, Byrne says. "The way we're deploying contactless in the U.S. is using EMV specs," says Byrne. "It's based on EMV technology making use of strong security elements baked into EMV. These new cards will not only be accepted in readers in the U.S. but also in the UK."

The next generation of contactless cards will be a step toward EMV, says Vanderhoof. For example, MasterCard terminals certified for contactless also carry elemental portions of EMV. "We're seeing these gradual upgrades of the infrastructure to support it," he says.

EMV deployment and penetration
Q4 2008 view by country

MasterCard Worldwide



Countries where there has not yet been preparation to migrate

Countries in which one or more banks are migrating, or have completed migration to EMV chip

Countries where penetration of MasterCard Branded EMV cards, EMV POS, or EMV ATMs exceeds 50 %

Source: Best estimations collected from MasterCard customers and regional offices

Vanderhoof says these new rules for EMV contactless are different than those for EMV contact cards. Purchases under about $25 can be a contactless transaction in the UK, just like in the U.S. "Just tap it and go, no PIN or signature. After a certain number of transactions you might be required to enter your PIN."

EMV vs. contactless overseas

While EMV and contactless may have to coexist in the U.S., it's not that simple where's there's already an EMV infrastructure in place. "Europeans have a lot invested in EMV," says Urs A. Lampe, vice president, product marketing and new business for contactless smart card provider LEGIC Identsystems, in Switzerland. "Now contactless is happening and the EMV installed base is all on contact, so you'll probably see some swapping out of terminals in the next few years."

Or they could opt for integrated contactless readers or readers that are configured to accept contactless peripherals, adds Byrne.

Another solution is dual interface products in which a single chip can communicate in contact or contactless mode. INSIDE will be bring the Micropass 6002, a dual interface chip to market in the fourth quarter of this year, Walton says.

Merschen adds that a number of markets, such as Canada, the UK, France, Malaysia and Taiwan, have already embraced dual interface solutions, running both EMV contact and contactless transactions using one single chip. "Some banks have clearly stated that contactless will be a standard feature for many of their portfolios," he says.

Canada, Walton says, is an interesting market because 10 million contactless chip cards have been deployed. He projects that by the end of the year, dual-interface cards will make an appearance there. "We'll be seeing use of chip-based cards in the U.S. for security reasons. The buildup of EMV in Canada will tend to cause fraud to migrate to the U.S.," he adds.

But there's no getting around that the purposes of EMV and contactless can be at odds. "EMV certainly brings about much more security and flexibility to today's mag-stripe cards," Merschen says. "While contactless brings transaction speed and cardholder convenience."

In the U.S. it may come down to a question of speed versus security. As retailers transition to newer payment terminals it will be up to the card issuers on whether or not to deploy EMV and put a safeguard in place to help stem the tidal wave of payment card fraud.

Problems found in U.S. passport issuance

Security hole presents 'national security threat'

An investigator from the U.S. General Accountability Office was able to obtain legitimate U.S. passports with fake breeder documents.

The investigator used fake breeder documents, such as Social Security cards, birth certificates and state IDs, to obtain the real passports. With one of the passports the investigator purchased a plane ticket and used it to get through security.

Sen. Dianne Feinstein (D-Calif.), Subcommittee on Terrorism and Homeland Security, Committee on the Judiciary; and Rep. Jon Kyl (R-Ariz.), Subcommittee on Terrorism and Homeland Security, Committee on the Judiciary, asked the GAO to look at the security of the passport issuance system.

"Because passports issued under a false identity help enable individuals to conceal their movements and activities, there is great concern that passport fraud could facilitate acts of terrorism. In fact, the 9/11 Commission stated that 'for terrorists, travel documents are as important as weapons,' and further noted that terrorists need to travel 'to meet, train, plan, case targets, and gain access to attack,'" the report states.

Janice Kephart was a member of the 9/11 Commission and is now director of national security policy at the Center for Immigration Studies. During her time on the commission it was discovered that terrorist

groups, like Al Qaeda and Hezbollah, wanted no item more than a U.S. passport. "What they want and covet most is a U.S. passport," she says. "Having a U.S. passport gives them a kangaroo jump."

Three of the 9/11 terrorists were chosen because they had previous experience in the U.S. and knew how to get around. Members of Al Qaeda who were U.S. citizens were also prized because they would receive less scrutiny at the borders.

This is why Kephart calls what the GAO discovered in the report "a huge vulnerability. The focus these groups have on the passport and the border shocked us," she says. "It's not fear mongering it's the reality."

In the 9/11 Report the passport came out pretty much unscathed, Kephart says. The terrorist attacks did lead the U.S. and countries around the world to better secure the actual passport books and start issuing electronic passports. "The passports are stronger because the 9/11 Commission noted that the passports the hijackers had used were manipulated in a number of ways," she says.

But nothing changed on the issuance side, Kephart says. When an auditor is reviewing an application he doesn't have anything to check it against. "They're completely blind," she says. "Unless they see something wildly, horribly wrong they're not going to flag the applicant. You have to back up the card with robust vetting of identity on the front end."

Checking the validity of Social Security numbers is one step the State Department can take to better vet passport applicants, Kephart says. The Social Security Administration has a system that enables state driver license issuers to make sure names and Social Security numbers match up. The State Department should be using the same system, she adds.

State was supposed to hook into that system, but has not. "There's no excuse for the State Department not to be checking Social Security numbers," she says.

In response to the GAO report, the State Department stated that its fraud detection efforts are hampered by limitations to its information sharing and data access with other federal and state agencies.

Kephart doesn't buy it. "What's truly doable and useful is hooking into the Social Security Administration," she says. "State dropped the ball on the Social Security numbers and there's no excuse."

With Real ID on the horizon eventually the State Department will be able to check a state's birth and death records online as well as driver license information, Kephart says.

It seems that many of the data sources that could help with identity vetting prior to passport issuance already exist. It is the linkages and data sharing agreements that remain elusive. ID

Counterfeit or fraudulently obtained documents used to obtain genuine U.S. passports

Test number	Month of application	Documents submitted as part of passport application process	Number of days between application and issuance
1	July 2008	• Counterfeit West Virginia driver's license • Counterfeit New York birth certificate • Passport application form	8 days
2	August 2008	• Genuine District of Columbia identification card obtained with fraudulent documentation • Counterfeit New York birth certificate • Passport application form	Same day (passport issued the date of application)
3	October 2008	• Counterfeit West Virginia driver's license • Counterfeit New York birth certificate • Passport application form containing SSN of a fictitious 5-year-old child, which we obtained on a previous investigation	7 days
4	December 2008	• Counterfeit Florida driver's license • Counterfeit New York birth certificate • Passport application form containing SSN of a deceased individual	4 days

Source: GAO.

Note: In all four tests, our investigator also submitted two color photographs and a passport application fee. For the second test, the investigator also submitted an e-ticket for an August 2008 flight to Germany.

PCI under fire at Congressional hearing

Is Chip and PIN on the horizon?

The Payment Card Industry rules are policies retailers must follow to keep consumer credit and debit card information safe. But with data breaches still occurring on a regular basis there are some questions as to how much they protect consumers.

In late March, the U.S. House of Representative's Committee On Homeland Security's Subcommittee On Emerging Threats, Cybersecurity, and Science and Technology held a hearing "Do The Payment Card Industry Data Standards Reduce Cybercrime?"

The concern is that stolen credit card numbers are used to fund terrorists. Rita M. Glavin, acting assistant attorney general for the criminal division at the U.S. Department Of Justice, cites one case in Indonesia.

Imam Samudra wrote about the use of credit card fraud and "carding" as a means to fund terrorist activities in his 280-page autobiography. Carding refers to when large volumes of data are stolen, resold, and used by criminals to commit fraud. Samudra sought to fund the 2002 Bali nightclub bombings, of which he was convicted, in part through online credit card fraud.

The consensus from retailers and those representing them at the hearing was that PCI doesn't work. "Since its inception, PCI has been plagued by poor execution by Visa, MasterCard and the other credit card overseers of the program," said Dave Hogan, senior vice president and Chief Information Officer for the National Retail Federation. "The PCI guidelines are onerous, confusing, and are constantly changing. Many retailers say that basic compliance is like trying to hit a rapidly moving target."

Subcommittee Chairwoman Yvette D. Clarke (D-N.Y.) said PCI standards serve a purpose. "But I do want to dispel the myth once and for all that PCI compliance is enough to keep a company secure," she said.

One possible solution to stem credit card fraud: entering a PIN to verify each transaction. "Implementation of encrypted PINs for all credit and debit card transactions could be useful," a subcommittee report stated.

"The U.S. is being blown away by security investments overseas, and our 1950's era system is making us a weak link in the security chain," Clarke said. "Magnetic stripe-based technology is outmoded and inherently less secure when compared to smart cards or other developing technologies. While I am deeply concerned about our security, the payment card industry and issuing banks should be ashamed about the current state of play and doing everything possible to immediately institute improvements in infrastructure."

Michael Jones, senior vice president and Chief Information Officer at Michaels Stores Inc., testified about his experience with banks and the PCI, suggesting that the rules is that they were not created with the retailer in mind.

"They are very expensive to implement, confusing to comply with, and ultimately subjective, both in their interpretation and in their enforcement," Jones said. "It is often stated that there are only twelve 'Requirements' for PCI compliance. In fact there are over 220 sub-requirements; some of which can place an incredible burden on a retailer and many of which are subject to interpretation."

Jones has issues with the encryption standards in PCI. The standard states that all credit card information must be encrypted, with one exception, it doesn't have to be if the data is sent over a private network.

Jones said this is a gap that can be exposed. "The credit card companies' financial institutions, the very organizations that have created and are mandating this rigorous and highly-complex standard, do not accept encrypted transactions," he said. "We must decrypt the credit card number at our corporate headquarters prior to sending to the merchant bank for approval."

Michaels has wanted to encrypt all the transactions but was told it's too expensive to implement and too expensive to come up with an industry-wide standard.

The data breaches at TJX and Heartland Payment Systems exposed this flaw, Jones said. "Had it been encrypted they would most likely not have been able to read the data."

The PCI rules aren't bad and credit card information is safer now that it was before. But Jones urged the subcommittee to not pass any additional legislation around the matter. "We do not need more laws," he said. "The existing (sometimes) misguided enforcement and the proliferation of state regulations around these issues have created a difficult, if not impossible, environment for retailers to effectively meet the legal requirements imposed on them should a breach of information occur."

Instead Jones said the credit card companies need to take greater responsibility and better secure the systems that are already in place. JD

2005

2006

2007

OWN THE ENTIRE COLLECTION

1000+ pages of ID technology insight just $250

- Educate new employees
- Refresh your industry knowledge
- Research for presentations
- Review best practices
- Learn from the experience of other implementations
- Gain a competitive edge

For the first time, AVISIAN is offering all back issues of their industry-leading *re:ID magazine* in a packaged set. You receive three year's worth of top-notch news and insight – 15 issues of *re:ID* and 6 issues of *CR80News magazine*. Plus you get password-protected access to our online library with more than 1000 feature articles.

Limited quantities are available so act fast. To order, fill out the form on the back of this page or visit *http://subscribe.AVISIAN.com*.

AVISIAN

re:ID

SUBSCRIPTION OPTIONS

The following questions must be answered to complete your free subscription request. (U.S. residents only)

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 *re: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 approved U.S. addresses only. *International subscribers pay $200 per year to cover postage and handling costs.)

FAX this form to 850-222-4477
or subscribe ONLINE at http://subscribe.AVISIAN.com

❑ **I live in the U.S. and would like to receive *re:ID magazine* FREE.**
❑ **My address has changed. Please send *re:ID* to this address instead.**
❑ **I live outside of the U.S. and would like to receive *re:ID magazine* for $200**
❑ **I live on planet Earth and would like to receive an email notifying me when the electronic version of *re:ID magazine* is ready to be downloaded**
❑ **I would like to order all back issues of *re:ID magazine* and *CR80News* for $250. Please send my hard copies to the listed address and send my username and password for the online library access to the email address provided**

Name _____

Job title _____

Company _____

Address _____

City _____

State/Province _____ Zip/Postal Code _____

Country: ❑ U.S. (FREE) ❑ *Other ($200) _____

Phone _____

Email _____

Signature _____ Date _____

* Non-U.S. subscribers: Fax this form and we will send you an invoice for $200 to the Email address you provide. Your subscription will begin when payment is received. To begin immediately, visit http://subscribe.AVISIAN.com.

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 http://subscribe.AVISIAN.com

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

Stickers:

The intermediate step to handset-based mobile payments?

Ed McKinley
Contributing Editor, AVISIAN Publications

There's a number of things holding back near field communication, the lack of devices being number one or two on that list followed by the lack of a business case for mobile providers and financial institutions.

But some are moving past those obstacles. Major players in the payments industry are promoting near field communication stickers linked to prepaid accounts as an intermediate step toward paying with mobile phones.

MasterCard Worldwide has announced a deal with Alameda, Calif.-based Blaze Mobile Inc. to market the stickers, and Visa USA is working with Greenwood, Colo.-based First Data Corp. to popularize the GO-Tags that can take the form of stickers, pins, key fobs or wristbands.

"Nirvana is having the NFC chip embedded in the phone – this is an interim solution until NFC mobile phones are available," Michelle Fisher, Blaze Mobile CEO, says of the stickers.

Consumers may obtain and use Blaze Mobile MasterCard PayPass mobile payment stickers for free by logging onto blazewallet.com, says Simon Pugh, head of MasterCard's Global Center of Mobile Excellence. First Data says GO Tags will become available to the public later this year.

Consumers can affix the stickers to their cell phones or hand-held computing devices to make electronic payments at any contactless terminal. The stickers, about a third the size of a business card, contain a computer chip that communicates via radio signals to contactless payment terminals in a transaction insiders liken to an "electronic handshake."

"A contactless sticker is like a miniature adhesive gift card with an NFC chip inside," says Sarah Owen, vice president of product development for mobile commerce solutions at First Data.

The Blaze MasterCard stickers enable consumers to make purchases where contactless payments are accepted. However, the MasterCard and Visa projects are limited to making payments drawn from prepaid accounts. For now, issuers are not linking the stickers to debit or credit cards, sources say.

The hope is that NFC stickers will create bottom-up demand for contactless and for NFC phones, says Ed Lawrence, managing associate at Westbury, N.Y.-based Auriemma Consulting Group Inc. At first, consumers will want the contactless stickers, he says. Later, they will want all of their cards on chips inside NFC phones, he continues.

The prepaid market will drive demand initially, and then legions of youthful consumers will adopt the technology, says Lawrence. He points to the 18 to 34 year-olds of the world who are wedded to their phones and to doing everything conveniently and fast over the Web. "It will explode and the world will never be the same," Lawrence predicts.

Owen also foresees widespread adoption and cites convenience as a driver. A First Data study indicates contactless payments typically take place two to three times faster than cash or no-signature card payments and about five times faster than card payments requiring a signature, she says.

Despite the newness of NFC, a January 2008 First Data survey of more than 2,700 consumers aged 18 years or older indicated 65% of respondents were interested in learning more about the technology, 78% of self purchasers indicated interest, 60% of those interested indicated a likelihood of using contactless stickers at least once a week and 40% expected to use it more frequently than that, Owen says.

Blaze Mobile began experimenting with stickers about three-years ago, creating six iterations before settling upon a final design, Fisher says. An early version the size of a poker chip slipped off the phones, she recalls. Now, a third-party manufactures the final configuration of the devices to Blaze Mobile specifications, she says.

First Data generated some buzz for GO Tags last summer by providing delegates to the Democratic National Convention in Denver with contactless pins charged with $10 in free refreshment-stand purchases. Earlier, tests in corporate cafeterias indicated 40% of users visited the employee cafeteria more often when they had their sticker and 17% spent more per visit to the cafeteria, Owen says.

The stickers have no durability issues, says Fisher, who has carried a phone with a sticker attached in her purse for some time without incident. INSIDE Contactless is supplying the chips in pre-laminate stickers to First Data.

First Data generated some buzz for GO Tags last summer by providing delegates to the Democratic National Convention in Denver with contactless pins charged with $10 in free refreshment-stand purchases.

High reliability has new IDs

Evolis offers a unique **3-year warranty** on its single and dual-sided card printers, Pebble and Dualys.
Reliable, fast, and easy to use, an Evolis printer is always the best solution to print all your IDs.
Call Evolis now at **954 777 9262** & start printing!

Evolis Inc. - 954 777 9262 - evolisinc@evolis.com - www.evolis.com

evolis

NFC tracks trade show attendees

ITN aims to make conference and exhibit hall lead tracking easy, all with near field communication

Ivan Lazarev, president of ITN International, sees great potential for the bCard business and the way it works with NFC. The bCard – for business Card – was originally launched in 1999. Since then the company has grown to become a provider of mobile data management and information solutions for the event marketing industry. And ITN relies strongly on near field communication to get the job done.

"The bCard is based on smart card technology," says Lazarev. "We basically designed a better mousetrap. It was a universal business card that could be used to create a unique digital ID linked to an account on the Web."

The bCard is a contactless smart card that looks like a regular trade show badge, says Lazarev. But it's a badge loaded with information that an NFC-compliant phone can retrieve by a simple wave of the phone within an inch of the badge.

Lazarev and company have been in on NFC since it was introduced. "We became partners with NXP, one of NFC's developers, to deploy an NFC ecosystem for events and trade shows," says Lazarev. "We started in 2005 and all our events became contactless. Anytime you approach a reader with the card, it can be read and written to. It becomes an interactive media," he adds.

At the CTIA Wireless show, held in April in Las Vegas, ITN issued thousands of NFC-compatible cards. The cards held the attendee's ID on a chip which could be read by an NFC phone, says Lazarev.

This year, for first time, ITN was able to incorporate NFC phones from Nokia. "We bought a huge quantity of these phones (the Nokia 6212) and deployed about 500 at CTIA for use by exhibitors."

Everything in one place

ITN manages registration for the event it serves and with its Web site manages the data from the attendee badges. The company works with about 120 shows a year. "We've had a 20% growth every year and have issued five million cards," says Lazarev.

"We install the entire information management system and five days later, we pack it up and move to the next event," says Lazarev, who is based at the company's Bethesda, Md. location. "It's all about touch and go, whether its an ID badge or poster," says Lazarev.

The phones are rented to exhibitors to use for lead tracking and contact management during the event. Exhibitors can review the information obtained from the badges via a secure Web site and through the phone. "They can do 24-7 management, and not just at the booth. For example, at a reception they can continue reading cards," Lazarev adds.

The data from the badge is read by the phone and stored locally on the it but is also sent to a secure site for later access. "When you go to the Web site via your phone, you'll be able to see all the names you gathered, all the booths you visited, your experience at CTIA," he says.

This lead tracking can benefit both exhibitors and attendees because "80% of leads are never followed up on. You can work with Facebook or LinkedIn to move the information to where it would be readily usable."

Session access control

ITN can also go a step further, supplying show management services as well. "Shows all have incredible need for access control," he says. That means access rights can be stored on the card and NFC phones can determine if the badge holder has paid for the session he is attempting to enter.

"That's when NFC starts becoming a lot of fun," says Lazarev. "I write back to that card that you attended that session, so when you go to one of our Web terminals and tap your card, it knows that you attended a particular session and may give you an evaluation form which you can complete," says Lazarev.

The cards can also be used to keep track how long an individual attends a particular session. "For medical events, we read them in and read them out so we know how much time they spent in the room and can issue them continuing education units," he adds.

It works for what Lazarev calls product delivery too. "I go to a high-level conference and I want to receive a copy of the proceedings. We write to your card all the proceedings you're entitled to. When you go up to the proceedings desk, we know what you're supposed to get and we write to the same card that you picked up your copy," says Lazarev.

Another event function that ITN offers is the e-purse. A conference can elect to load onto the badge a specific amount of money. "We work with the venue and put a phone in the restaurants, for example, and attendees can pay with their badge."

The beauty of this feature is that the show's sponsor is only liable for the actual amount spent. "This has saved show producers a tremendous amount of money," says Lazarev. "They're paying for actual usage rather than generic usage." In the past, he says, show management was being billed for the full amount even if the badge holder only used a portion of that amount.

When NFC phones become more prevalent the business model may shift for ITN, Lazarev says. "Our next target is to go to the attendee side. They'll be showing up with their NFC phones and we'll be able to load the bCard information directly onto their phones," he says. "Right now, we're just waiting for the phones to come. I've been saying for several years they're coming, now I think they really are coming."

NFC Guru is bullish on ... well, NFC

Whether it's linking a Facebook account, or other social networking site, with your NFC-enabled phone, using the technology to reduce gate costs for transit agencies or using it in your home as a smart doorbell, Austrian researcher Gerald Madlmayr sees great things ahead for near field communication.

If you're not familiar with that name, you may know him under the pseudonym, the "NFC Guru," a post he occupied for two months earlier this year. It was probably his bullish attitude about NFC that prompted Nokia, a leader in manufacturing NFC-compliant phones, to entice Madlmayr to take on that mantle.

Madlmayr is a research associate at the NFC Research Center in Hagenberg, Austria, a joint-venture of NXP Semiconductors, mobilkom Austria, Assa Abloy (Omnikey) and the University of Applied Sciences of Hagenberg. There his work is focused on NFC/RFID-based applications as well as security and privacy in such systems.

While he doesn't work for Nokia, he has done some consulting work for the cell phone giant on NFC projects. He has also conducted several NFC pilots.

Madlmayr was involved in one of the first NFC trials in 2006 in Hagenberg on the University of Applied Sciences, Upper Austria, campus.

That trial was launched in November 2006 and ran until July 2007. Some 100 subjects – 50 students and 50 professors, lecturers and employees – were given NFC-enabled mobile phones to test and evaluate the services implemented. The trial tested a micro payment and access system based on Mifare, as well as loyalty cards for employees and a peer-to-peer information service.

Since then Madlmayr's lab has participated in other NFC competitions. In 2008, his research lab won the Operator Award at Gemalto's SIMagine Competition for its SmartDoorBell, an access control solution that replaces a standard intercom system with an NFC reader that works with an ordinary mobile phone for use in family homes as well as large office complexes with multiple entrances.

Information about the caller is sent via the NFC interface to a proxy, which then transfers it on to an access management application running on the homeowner's handset. If the person chooses to open the door, the access management application generates a response to the proxy, which in turn, unlocks the door.

No phone needed

His NFC Guru blog was designed to show how simple it can be to write an NFC application, he says. "In the beginning you don't even need a phone. There are nice tools from Nokia that allow you to use all the NFC functionality that a mobile phone provides in an emulator on the PC. Additionally there are lots of code examples and Wikis on the Web dealing with NFC development."

The guru site was designed to lure more software developers into the NFC world, he says. "NFC allows intuitive interactions to make your most-personal-device-ever a nice haptic (as in touch screen) interface."

Madlmayr says he got into NFC four-years ago when he first began work at the research lab. "In the beginning I loved to develop mobile apps and then I came across RFID technology. Well, NFC is the thing that combines both and thus I looked deeper into this topic," he says.

While his NFC Guru column was meant to spur people to write NFC applications, he found just as many, if not more, requests for help. "I got more private emails with support requests, most of them with professional problems, than posts," he says. He also has received several job offers.

He says that most of the people who contacted him wanted "to run either highly secure applications in the secure element and didn't know where to start working." What he didn't find were developers willing to divulge their ideas.

"I think the Web site is an important enabler, to show people that developing NFC apps is simple and discusses how you can benefit from starting to use NFC in your business," he says.

NFC and Facebook

Madlmayr also has a couple projects in the proposal stage. "A very popular area for NFC applications are social applications or social networks that make use of NFC for getting in touch with people," he says. With social networks, he explains, "you could use NFC to pair me with a friend on Facebook so I don't have to search for him. Or I could be meeting someone in a bar and we could touch each other's phones. Then it becomes a virtual interaction, a link between the digital and physical world."

Another example, if a member of a site is at a bar he could touch a tag in that bar and rate it. "The Facebook API would allow us to do this already. We're working on building a client for an NFC device. Or we could do some kind of navigation system where you just punch in where you are, you're waiting somewhere or you're at the movies and it sends a message to your Facebook site," Madlmayr says.

With transit, contactless ticketing is already popular but he'd like to incorporate NFC to eliminate gates or turnstiles. "You could have a small RFID reader at the train's entry point or check in at the seat just by touching a reader," he says. "Another scheme is checking in and checking out via a smart poster at a train station, with the fare automatically deducted. There are different approaches for ticketing schemes for countries without gates. In Germany it would take a billion Euros to install gates. We are currently writing a research proposal with public transit operators in Upper Austria to pilot such a system," he adds.

Making NFC commercially viable

Still, Madlmayr knows that full commercial deployments are a ways off. While he admits that NFC commercial roll outs are hampered by the lack of phones, he thinks the bigger problem has to do with the silicone that goes into those phones to make them NFC-compatible.

"A lot of people blame handset manufacturers, but if someone says they need 10 million pieces to produce a secure element on the SIM, no silicone manufacturer can produce that many to support the single wire protocol," the NFC standard set by GSMA, says Madlmayr.

As he puts it, there isn't a fully working ecosystem to support NFC yet. "There is no manufacturer on this planet that has produced one single device you can purchase in enough quantities," he adds, "and handset manufacturers aren't able to produce new phones because they can't get the NFC chips."

Madlmayr also says higher data rates for NFC is needed. "Today you have data rates of a maximum for 424 kilobits and we are already thinking of having a several megabit transfer rate. When you see that RFID passport at an airport take 10 or 20 seconds to read, with high data rates you can just tap and go."

But he will continue researching and working on NFC because he knows it's just a matter of time before the ecosystem catches up with demand. And even though the NFC Guru is no longer officially live, Madlmayr says he will still answer questions and "I intend to keep posting some new articles."

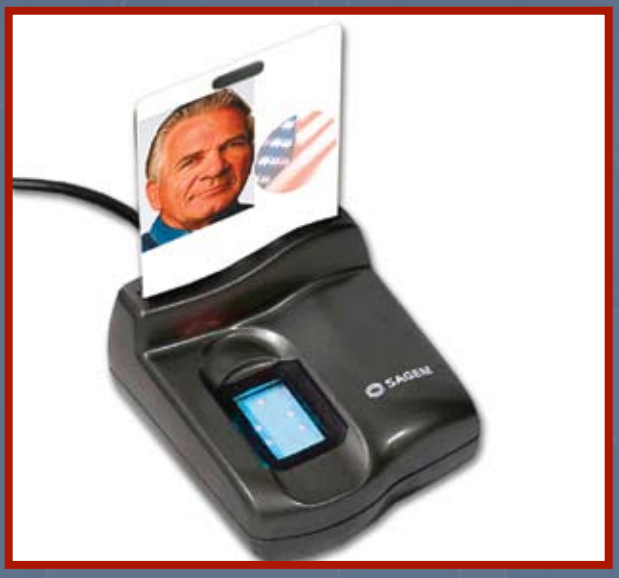
He is also willing to help other universities who might be starting their own NFC labs. "We have the core competency for NFC and we can hand this over to other universities so they don't make the same mistakes," adds Madlmayr.

Does he consider his NFC Guru site a success? "It depends," he says. "From a personal perspective, it was a success because lots of people have been contacting me because they have NFC problems. I think it was a success for Nokia because it did enable other people to start developing NFC applications."

Featured FIPS 201 Products

iCLASS R10
HID Global Corporation

iCLASS 13.56 MHz contactless smart cards and readers make access control powerful, versatile and secure through data encryption and mutual authentication between the card and reader. iCLASS readers are user friendly, delivering the same convenience and reliability of HID's Prox technology, with state-of-the-art features, driven by evolving industry requirements. Included on the GSA FIPS 201 Approved Products List, iCLASS readers provide ability to use smart cards for field firmware upgrades to address future updates in FIPS specifications.



MSO 1350e
Sagem Morpho, Inc.

The MSO 1350e is GSA FIPS 201 approved as both a Single Fingerprint Capture Device and a Transparent Reader. Combining both an ISO 7816 contact smart card reader and a compact optical sensor that is FBI certified for image quality, this new biometric device is suited for integration into PIV logical access applications. One USB connection enables PC communications to drive both the PC/SC smart card reader and the built in biometric sensor. The MSO 1350e is supported by the MorphoKit, which includes PC software for image capture, ANSI 378 template processing, authentication and identification of up to 1:20,000 persons.

Newly approved FIPS 201 products

PIV Card

Gemalto TOP DM with ActivIdentity Digital Identity Applet Suite
Gemalto

Single Fingerprint Capture Device

MSO 1350e
Sagem Morpho, Inc.

Facial Image Capturing Station (Physical)

PreFace SDK with Canon SX 110 IS
Aware, Inc.

Transparent Card Reader

iCLASS R10
HID Global Corporation

iCLASS R15
HID Global Corporation

iCLASS R30
HID Global Corporation

iCLASS R40
HID Global Corporation

iCLASS RP15
HID Global Corporation

Transparent Card Reader (continued)

iCLASS RP40
HID Global Corporation

Motorola Embedded Smart Card Reader kit for MW810 Displays
Motorola

VISIT FIPS201.COM TO RESEARCH AND COMPARE APPROVED PRODUCTS

FIPS 201.com

THE PREMIERE RESOURCE FOR COMPLIANT CREDENTIALING

The way the government handles security changed drastically in August of 2004 when FIPS 201 Standards mandated the standardization of identification security and credentials. These standards are rapidly expanding throughout the U.S. government, and are already influencing the private sector, educational institutions, state and local government, and international markets.

AVISIAN Publishing is announcing our latest information source, FIPS 201, as the newest addition to our publications suite. Thousands of people turn to our other resources daily for news and the latest product information. Make FIPS201.com part of your daily routine, and you will have the opportunity to view approved products and services, photos, web links, brochures, contact information, and more.

Make sure that you don't miss out on the FIPS 201 revolution.

SEARCH FOR APPROVED PRODUCTS BY CATEGORY OR SEARCH BY PRODUCT NAME OR VENDOR

RECENTLY APPROVED MEMBER LISTINGS ARE HIGHLIGHTED ON FRONT PAGE, AS ARE RANDOM LISTINGS

CONSTANTLY UPDATED NEWS FEED KEEPS VISITORS UP-TO-DATE ON FIPS 201-RELATED CONTENT

RESOURCES SECTION ENABLES MEMBER COMPANIES TO PROMOTE WHITE PAPERS, WEBINARS, EVENTS.

Get your FIPS 201 Approved Product listed on FIPS201.com today. Contact info@fips201.com for more information.

Contact: **Ryan Kline**
FIPS201.com Coordinator
850-391-2273
ryan@AVISIAN.com

AN AVISIAN ID TECHNOLOGY RESOURCE

Contactless logical access gains momentum

Adding IT applications to the existing physical security badge paves the way

Using contactless technology on the desktop to lock down computers is starting to find more proponents as companies begin to ratchet up their portfolios to include more logical access devices that make it easier, and potentially less expensive, to migrate to the systems.

Logical access can involve either contact or contactless ID cards as well as key fobs but it goes beyond simple passwords. The majority of logical access smart card systems up until now have involved contact cards. But as contactless smart cards become more prevalent for physical access, vendors have introduced products so the same card can be used for logical access.

It all comes down to using the same badge to get in the front door and to logon to a computer. This has been problematic in the past because of cost and technology issues, says Dan DeBlasio, director of business development of identity and access management at HID Global. "Many organizations have not yet moved beyond password-only security because traditional alternative log-in solutions have been too involved or too costly," he says.

HID has released two products that aim to make using contactless on the desktop simple: HID on the Desktop and naviGO.

NaviGO is a software credential management system that is used for setting up cards and managing access, says DeBlasio. The product works with either HID's prox or iClass smart cards.

"The same software is used regardless of the type of card or the approach a company has to access computers," DeBlasio says. "Organizations do not need to re-badge as prox and iClass cards can be user provisioned in the field in a self service manner."

The naviGO product helps establish the second factor and links the card to the company's IT system via a self service portal. "This naviGO capability removes what has been a significant impediment to the adoption of logical access control: the deployment and ongoing management of the IT credential," says DeBlasio.

More user control

It also gives the user more authority in managing access to the computer, enabling the setup and reset if PINS, says DeBlasio, this saves the company money since users have fewer calls to a help desk when he forget a PIN or needs it reset.

HID on the Desktop, enables a user to enact two-factor authentication to a company's IT network. Computer maker Dell has rolled out versions of its Latitude E-Family laptop series that contain contactless smart card reader technology and software with the capability to read HID's iCLASS cards, says DeBlasio.

After turning on the Dell laptop, a user must present his iCLASS card to the contactless smart card reader located in the palm rest of the laptop. If the card is determined valid, the laptop will continue to boot to the Windows operating system.

It's all about convergence

Urs A. Lampe, vice president of product marketing and new business at LEGIC Identsystems, looks at logical access from a convergence perspective, using the same card for multiple purposes. This can be anything from a credit card or employee ID badge that can also be used for logical access. "You can use one card to do many things," Lampe says.

For example, says Lampe, a Visa contactless payment card could be used as a multifunction credential for campus cards or for entry into a work place or computer. "You can use the same card to manage your student account at the bank or to gain access to buildings. It becomes a device that can help a student manage his life," he adds.

LEGIC has one system it calls card-in-card. It's designed to simplify adding applications to a customer's existing smart card, for example, handling logical access in addition to the card's other duties that may include physical access, an e-purse, etc. "You have to move your applications into the customer device, which may be a credit card, a logon token or a mobile phone," Lampe says.

The applications are stored in the LEGIC virtual multi-application transponder on the micro-controller of the credit card. This allows the integration of applications for personal identification with contactless or dual interface smart cards provided by third parties, says Lampe. "You want them on the same chip but they don't necessarily have to talk to each other."

Lampe says contactless for physical access is popular in Europe. "It's one of the best alternatives because contact doesn't work. It's not suitable for opening doors thousands of times." Still, logical contactless access has a ways to go, at least in Europe, "It's elegant, but is it practical?" Lampe asks.

Dell thinks it is, says Craig Durr, senior product planner for security and software in business client marketing at Dell. Especially during touch economic times when corporations want to use what they have.

"IT administrators and chief security officers want to leverage existing infrastructures," Durr says. "Here's another opportunity for someone to leverage integrated contactless smart card technology into the system they already have to login to the desktop and to the network."

Contactless payments: What's next?

Multiple applications on one card bode well for the technology's future

Andy Williams
Associate Editor, AVISIAN Publications

It's an interesting time for contactless smart card technology. The payment cards are in the hands of consumers but now it's a matter of getting them to use them.

The next year may be tough in terms of numbers but there also may be some important developments as more readers are deployed and different form factors released. Beyond that it's a matter of adding additional functionality to the card.

Last year was a good one for some supplying the payment cards technology. "We saw a market growth in issuance and demand in 2008," says Charles Walton, executive vice president for payments for INSIDE Contactless. "For INSIDE, it was a good year, as we shipped 65 million chips for Visa- and MasterCard-branded cards" with about 90% going to North America. In the U.S. the company has shipped 110 million chips since 2005, he adds.

Randy Vanderhoof, executive director of the Smart Card Alliance, says the industry is expecting 80 million cards to be issued through 2009 and up to 100,000 terminals. "Deployment hasn't slowed down and plans are still underway to continue the roll-out of the infrastructure." He sees more roll outs in Europe and Latin America. Still, the biggest population for contactless cards resides in the U.S.

While the economy may put a damper on some of these growth plans, says Vanderhoof, analysts he's talked with indicate an increase in the next five years.

Walton says INSIDE has downgraded projections for 2009. "I imagine it could be a fairly flat year because of the economy and we could see smaller quantities deployed."

Vanderhoof says the U.S. will continue to lead the way with contactless card issuance. "The merchant infrastructure is already in place. Even though you see cards being issued in the UK, Singapore and other locales, the number of merchants they have configured to accept contactless payments is low. We'll likely see some significant card volumes but the actual number of merchants and likely volume of transactions will be fairly small."

Urs A. Lampe, vice president of product marketing and new business for contactless smart card provider Switzerland-based LEGIC Identsystems, agrees that contactless will continue forward. "We're getting huge acceptance in several markets. LEGIC has been in contactless since the early 90s and I see contactless gaining vast acceptance as standardization drives interoperability."

Changes ahead?

However, some changes may be afoot, which has less to do with the economy and more towards producing a profitable business model.

Walton says he sees a shift away from the credit card giants subsidizing terminal deployment. While the number of cards in use has grown, there hasn't been a corresponding growth in contactless terminals. "Visa and MasterCard have invested in terminal deployment for several years but in 2008, I think they realized they couldn't continue to pay for terminals forever and that the merchant community will have to stand on its own," says Walton.

What's starting to happen now, since those merchant subsidies have been eliminated, is that retailers are replacing point-of-sale systems though natural turnover and adding contactless, says Vanderhoof.

He says merchant terminals last anywhere from five to ten years. "Folks in that renewal cycle are now making that small incremental investment even if they're not seeing significant numbers in contactless use, knowing that in a few years those numbers will increase, and certainly with NFC as a driver that could accelerate that."

Walton sees fully integrated contactless terminals increasing in 2009 and more self-service readers, such as those on vending machines or in taxi cabs.

Vanderhoof says the merchant climate is changing as well. "Fast food restaurants were early adopters and were supported by financial incentives," he says. While the quick service segment will remain the primary driver for low-value transactions (less than $25 where no signature is required) he's seeing more retailers who don't fit that normal low end, such as the larger box stores like Costco.

Debit surpasses credit

Vanderhoof is also hearing that contactless debit card usage has now become equal with, and in some places, exceeded credit card usage.

Case in point: Wells Fargo is replacing all debit cards with contactless, says Vanderhoof. "It's going to be different strategies with different issuers. American Express has five or six different cards they offer, but only a couple are contactless."

JP Morgan Chase is targeting specific regions of the country, adding contactless technology to some, says Vanderhoof. "The issuers we've heard from are satisfied that the incremental transaction value increases and customer retention and activation rates makes good business sense," he adds.

Next contactless killer app?

Walton sees transit carrying the heaviest load in future contactless deployments. "Globally, transit systems are predominantly using contactless. And most of the major U.S. cities that have transit systems are using contactless–Atlanta, Washington D.C., New York, Los Angeles."

These transit cards could be used for transactions other than boarding a train or bus. "Those are the places where you might also grab a coffee or a newspaper," Walton says. "These become natural places to offer converged contactless applications, such as payment plus transit on a single card."

Walton compares contactless transit to building a mall. "If you think about retailing and you try to start a mall, you need an anchor client. So it is for contactless. You need some anchors. I think transit is a good anchor for a lot of cities around the world."

Another change is bypassing transit tickets completely, allowing Visa or MasterCard acceptance at the train. "This is a fairly significant trend that we see," says Walton. He also sees a greater interest in using contactless on both student and corporate campuses for building access. "There's a lot of interest in combining a payment card with an access card."

Rewarding customers

Retail loyalty is another area where contactless can shine. "Being able to present my AAA card or Barnes and Noble discount number and receive discounts automatically, or a co-branded card from a bank or airline where you're able to put frequent traveler numbers on the card," says Walton.

For Vanderhoof, couponing will gain a larger foothold. "As more merchants start to accept contactless, they're able to target specific customers with electronic couponing or a marketing program tied to the card," he says.

"We've seen a few pilots, such as BART in San Francisco with Jack-In-The-Box. I expect others will follow. With payments processors, who are all seeing their profitability shrink as the transaction value shrinks, they will be looking at ways to promote any value-added service."

For LEGIC, which views contactless from more than just a payments perspective, there's a network of possibilities available for the technology. This would include contactless use in access control–logical and physical–and mobile.

Contactless cards for originally intended single applications are now handling multi-applications for multiple purposes. "Contact cards are going contactless; the contact based login cards for PCs become multi-functional credentials offering contactless applications such as opening a locker, accessing company facilities or using copy machines," says Lampe.

Lampe also sees mobile applications converging with the contactless cards, "or the other way around, cards becoming virtual and moving to the phone, or my transit ticket moving into the phone."

I have what in my wallet?

Still, many people are carrying a contactless card in their wallet or purse and don't even know it. "There's been quite a bit of discussion about getting people used to contactless," says Vanderhoof. "We did a survey of issuers and asked them how they are marketing or promoting their contactless features. The majority of issuers felt the more effective way was through targeted marketing programs directed to their individual customers rather than broad TV advertising," adds Vanderhoof.

"The types of programs they felt were more effective were inserts with the card. Also, when customers call to activate their cards, the script or recording used alerts the customers of the feature and those programs have resulted in higher awareness," adds Vanderhoof.

"Over time, people's habits begin to change and those with cards in their wallets will become aware more and more about merchant locations where their contactless cards can be used. It's an escalating curve that will keep going up," says Vanderhoof.

Testing the limits of new banking technology

U.S. Bank explores future of identity and payment cards with high tech pilots

With today's tech-happy consumers, providing them with the latest gadget or innovative service could lead to a happier bank customer. Banking today is about more than just parking your money in a brick and mortar facility or even with an online system. Customers, especially younger ones, expect innovation.

To that end, U.S. Bank is involved in several trials that if deemed viable, could find their way into customer's wallets, desktops and even mobile phones.

Dominic Venturo, U.S. Bank's chief innovation officer for the retail payments solution division, says the bank learned much from a recent six-month pilot involving near field communication with Spokane, Wash. residents as well as students from Gonzaga University.

"The intent was to run a public pilot with real consumers," says Venturo. "From our perspective that pilot was a success. We learned what we hoped to learn and we got good feedback from participants."

He says the bank "ultimately concluded that the hypothesis of consumers finding value was proved. Participants liked it because it was faster and better than cash."

Another lesson learned was "that people have a personal relationship with their mobile phone and strong opinions about that phone. We gave them one phone, a Nokia 6131, a flip phone, not a bar phone, not a smart phone. Because people have such strong preferences, they love the idea of payments but they want that capability on their own phone, not one provided for them," says Venturo. "What that says is there's a need for the handset community to have broad support for NFC for it to be widely accepted."

"The other thing we heard from users is that while there was good acceptance in the merchant community, participants would like to use the mobile device in more places. You need the contactless readers. That is a challenge," says Venturo. "We learned that we were on the right track, they liked the form factor, but we have a ways to go with merchant acceptance and handset adoption."

So U.S. Bank is looking at the next best thing, which turns out to be a contactless sticker that can be affixed to a cell phone. "We have an internal pilot involving U.S. Bank employees with a Visa debit card on a sticker," says Venturo. That pilot started late last year and will run for six months.

Who needs computer to access bank account?

"We've expanded our offering within the banking side for access with a mobile device. You can go to m.usbank.com using a Web browser on a cell phone to log in and check your balances or make transfers between accounts."

But for those phones not equipped with Web browsers, the bank is also looking at expanding its text alert program. "We've been doing alerts, like email alerts to your computer or mobile phone, for two years, but what we're now testing is the ability to set parameters about when you receive your messages," says Venturo. "You could get an alert at the time the card is swiped. The purpose of the pilot is to see if we can do this reliably and see how customers like the feature."

For example, one parameter a customer could set is to be notified of a sales amount when your card was used. "It augments the mobile alerts that we do on the online banking side," says Venturo. The message would include the location of the transaction, merchant name and amount of purchase.

Venturo says the feedback from this pilot has been interesting. "For instance, it detected fraud before anyone else has. So if you get an alert you don't recognize, you can look into it pretty quickly."

It can also be used for online purchases and as a reminder about recurring bills. "Basically anything you want to know about your account you can have it sent by email or SMS messaging. Plus you'll also have mobile access to your account."

Again, the feedback for this pilot has been positive, says Venturo, but there are a few glitches to be worked out.

"A couple of things we've learned is that you don't always get text messages. The message doesn't always make it to your handset. Because we're talking about financial transactions, this is something we need to look at. Is it our issue? The carrier's issue? That's the kind of thing we're looking at," says Venturo.

"We've been moving in phases. We added SMS for all transaction types late last year. Whether we move to real time, I can't tell you."

And who needs a card or phone?

Another pilot involves a number of vending machines at U.S. Bank facilities. These machines were enabled for contactless payment, says Venturo, noting that the jury is still out on that trial.

The bank has also issued the Visa Micro Tag, a small contactless payment key fob. "It's a promotional item we did for 4,000 employees in the bank. It's basically a gift card and we allowed vending machines to take this as a means to test being able to actually create, distribute and load a keychain," says Venturo.

With all these pilots underway, it seems likely that the way customers interact with their financial institutions and the way they make payments will likely look very different in the coming years.

The push for electronic health records raises the bar for identity management

President Barack Obama has set aside $19 billion for health care to invest in information technology and electronic health records (EHRs).

Still unresolved is just how to ensure the EHRs are properly secured and that patient's are positively identified. Several recent developments point to growing recognition of the need for identity technology in the health care system.

Vermont State legislators want to use smart cards to lower health care costs and streamline billing, says State Senate President Pro Tem Peter Shumlin. "We spend 10 to 15 cents of every dollar chasing money around," he says. "We want to put a new model in place with a medical card."

The medical card would enable a patient to show up at a physician's office for care and know right away how much the insurance company is paying and how much he needs to pay. "It's like when you go to the store – you walk up to the counter and they tell you what you owe and you pay it," he says.

The Vermont legislature will adjourn in early May and Shumlin plans to have language in the appropriations bill to get the system rolling. He also plans to apply for grants from the stimulus package for the program.

The plan is to meet with health care providers and insurers to get them on board with the project. The cost savings should be an incentive for the health insurers, Shumlin says.

On the technical side Vermont has talked with representatives from IBM Research about the project. The technology will be a challenge, Shumlin adds, because a system like this has never been put in place before.

Smart cards for patient ID in New York

Mount Sinai Medical Center is continuing on its patient smart card ID initiative. The health care provider is deploying smart cards from Giesecke & Devrient (G&D) through partnerships with EXTENSION Inc. and TrustBearer Labs.

EXTENSION Health Connect provides patient identification and information exchange. It links data, patients, and health care providers together to reduce administrative costs and improve the patient experience. EXTENSION Health Connect uses G&D patient health cards to securely identify patients to hospital information systems. The card also holds a personal health record for each patient that can be securely accessed.

"Accurate patient identification is a critical issue in health care especially as we expand the use of electronic medical records and health information exchanges," said Paul Contino, vice president of information technology at Mount Sinai Medical Center. "These new health cards will ensure that patients are securely and accurately linked with their personal medical information across multiple institutions and care providers, reducing administrative burdens, improving patient care and satisfaction."

These types of solutions can help meet the information security goals of HIPAA by providing a highly secure method for access and authentication to health information and EHR.

Industry group responds

The Smart Card Alliance released a brief for federal health care policymakers on the importance of reliable identification technology in the market.

"This is the right time to bring health care identity management to the forefront," said Randy Vanderhoof, executive director of the Smart Card Alliance. "If you look at the problem from inside the health care industry, identity management is an essential first step that is not well understood today. The lack of the proper identity management infrastructure will later undermine achieving the program's goals."

There are a number of reasons patient identification should be a priority for health care providers, including reducing medical errors caused by mis-identification and decreasing redundant testing which can lead to lower costs. There should also be concerns with protecting patient's privacy.

"Dependably accurate identification and authentication of patients seems like something that should already exist in health care, but studies show it is a major problem," said Vanderhoof. "And if we are aiming for wider interchange of information, there must be a way to uniquely and securely authenticate that person across the health care system, including over the Internet, in a secure and privacy sensitive way."

"Effective Health Care Identity Management: A Necessary First Step for Improving U.S. Health care Information Systems" is a one-page, brief that explains the problems with identity management in health care and its costs.

It also proposes solutions without reinventing the wheel by leveraging existing standards developed for other federal identity programs, including the FIPS 201 Personal Identity Verification of Federal Employees and Contractors standard now being used for federal employee identity programs.

Power grid hack may lead to PIV for utilities

News in early April that the electric grid had been penetrated by cyber spies from Russia and China has given ammunition to those who say utility companies need to be using strong authentication, like FIPS 201, to gain access to those networks. "Using PIV as a robust form of authentication can reduce the threat of attacks," says Tony Cieri, principal at the Cieri Consulting Group Inc. and a consultant on U.S. credentialing projects.

In fact the U.S. Department of Defense mandated that the Common Access Card be used to login to its networks hacker attacks have dropped 52%, according to the DOD.

The North American Electric Reliability Corporation (NERC), a group of electric utilities and other electricity suppliers, had considered aligning with the Federal PKI before but considered it too complex and too expensive, says Salvatore D'Agostino, CEO at IDmachines LLC.

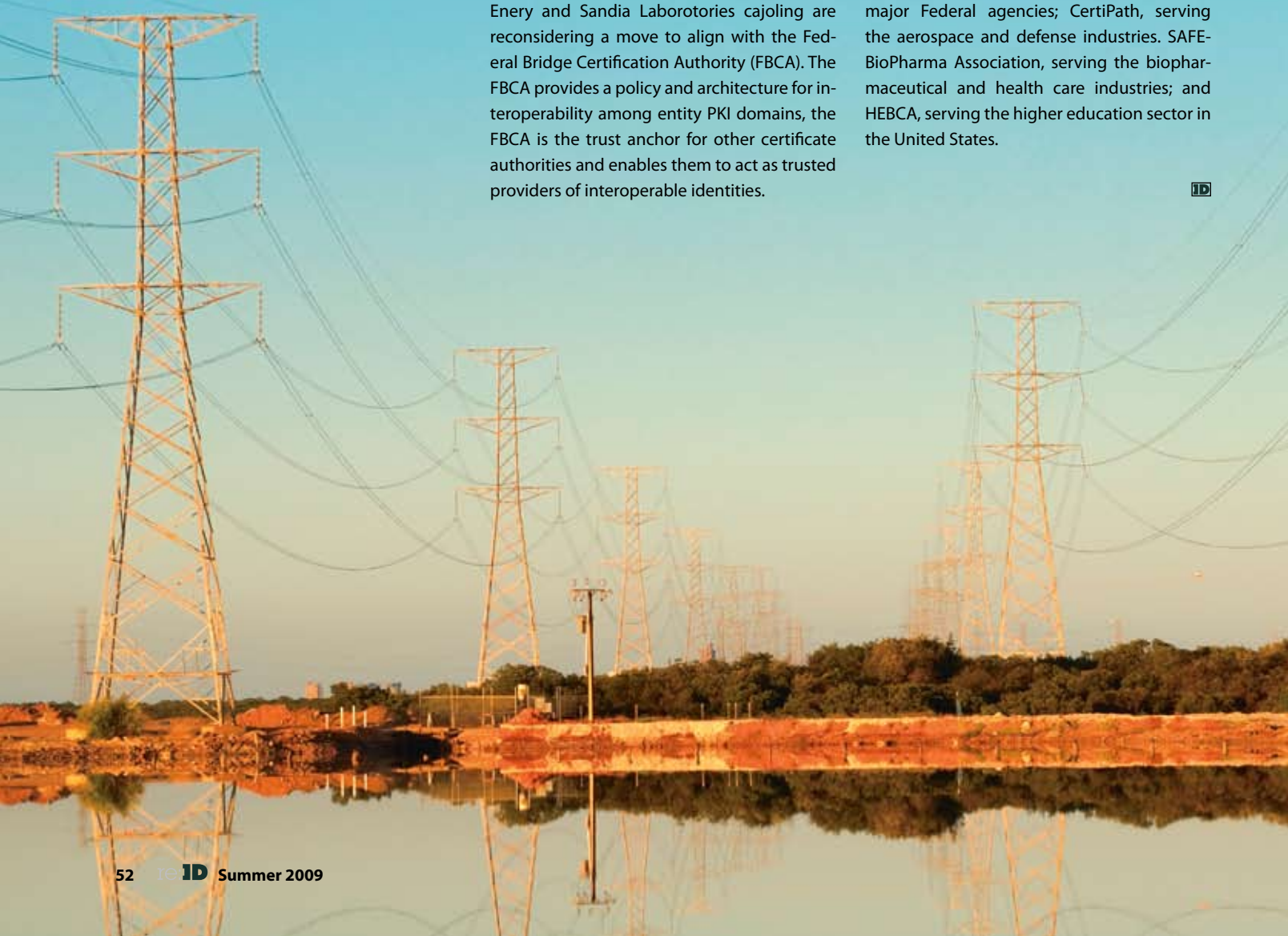
"It's time to extend HSPD-12 to include IT infrastructure as well as the critical infrastructure components," D'Agostino says. "Under this scenario operators login and perform other grid related IT functions using interoperable FIPS 201 credentials. Any intelligent grid component – the kind that can be hacked – would identify itself using its device certificate and expect the same from its relying party human or device."

NERC and the North American Energy Standards Board with some U.S. Depatrtment of Enery and Sandia Laborotories cajoling are reconsidering a move to align with the Federal Bridge Certification Authority (FBCA). The FBCA provides a policy and architecture for interoperability among entity PKI domains, the FBCA is the trust anchor for other certificate authorities and enables them to act as trusted providers of interoperable identities.

If the energy companies go this route they will be able to use the same technology that federal agencies are using. "Leverage the same architecture that protects government networks and facilities to protect critical infrastructure, its already being leveraged by the bio-pharma, aerospace and higher education sectors – why not apply it to the grid," D'Agostino says.

Even though HSPD-12 and FIPS 201 is still in deployment there's a concerted effort to extend the Federal Bridge even further. The Four Bridges Forum was created to facilitate trusted electronic business transactions across major federal agencies, U.S.-based pharmaceutical companies, aerospace and defense contractors and colleges and universities.

Members of the forum include: the Federal PKI Architecture (Federal Bridge), serving the major Federal agencies; CertiPath, serving the aerospace and defense industries. SAFE-BioPharma Association, serving the biopharmaceutical and health care industries; and HEBCA, serving the higher education sector in the United States.



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 US 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**.

WORLDWIDE OUTREACH

UNRIVALED EDUCATION

TASK FORCES & REPORTS

CONFERENCES

NETWORKING

Mapping out the future of biometrics in the U.S.

Biometrics will play a role in how the federal government identifies individuals in the future. To make sure the technology is used properly the FBI and the Mitre Corp. released a roadmap for how the U.S. government should move ahead with the technology.

This report outlines the "State of the Art Biometrics Excellence Roadmap study," that included an survey of biometric modalities, products, systems, performance evaluations and research activities.

The MITRE team was provided access to FBI laboratories where discussions with analysts and scientists contributed to understanding the breadth of forensic biometric applications and how they are used. The MITRE team also had support from external consultants.

The team visited representative federal, state, and local booking and detention environments and saw large surveillance systems used for security and gaming. The visits provided a perspective on the constraints and challenges that must be considered for the FBI to fully realize the Next Generation Identification (NGI) system.

The proposed roadmap recognizes the FBI's work in fingerprint technology as a solid foundation for expansion and seeks a way to move on using cost-effective supporting technologies.

The report's recommendations for the next two years

- Continue augmentation of fingerprint systems to include palm prints and the beginning of automated searching of major case prints.
- Continue development, analysis and publication of extended features used by human examiners but not supported in automated fingerprint identification systems.
- Continue collection of latent data sets for development and evaluation of applications with improved automated latent matching accuracy and interoperability.
- Continue development of standards to support mobile identification, for example template-only transactions.
- Augment the planning, and science and technology support to current modality specific applications within the labs, special applications, and National Backstopping Unit.
- Provide quality-assessment tools and other feedback mechanisms to state and local submitters and integrators. Feedback should contain examples and clear remediation steps.
- Conduct off-line analysis for the reconciliation of records; develop working solutions and feedback mechanisms for resolving data integrity issues and inconsistent use of standards.
- Conduct technology evaluations and consider trial use for the automated comparison of scars, marks, and tattoos.
- Provide quantitative methods and application performance requirements for comparisons between biometric data of differing qualities (this is a prerequisite for multi-biometric searching and fusion across different sources).
- Initiate pilot experiments for common collection and searching of additional biometric features along with, or in addition to fingerprints.
- Augment performance evaluations to include computation performance, and encourage vendors and research programs to use techniques to better leverage commodity hardware (e.g., blade servers, multi-core processors, graphics processing units, and field programmable field arrays).

The report's recommendations for the next two to five years

- Continue collection pilots and searching of additional biometric modalities along with or in addition to fingerprint, for example: Forensic quality face images and high-quality open microphone speaker recordings.
- Develop integrated tools for human analysts to support visualization, annotation, and comparative measurement.

The report's recommendations for the next five to 10 years

- Combine cost-effective facial and iris collection, storage, and automatic comparison.
- Support sciences for defending Daubert challenges. The Daubert challenge is a set of criteria to make sure evidence is reliable and admissible in a court of law.

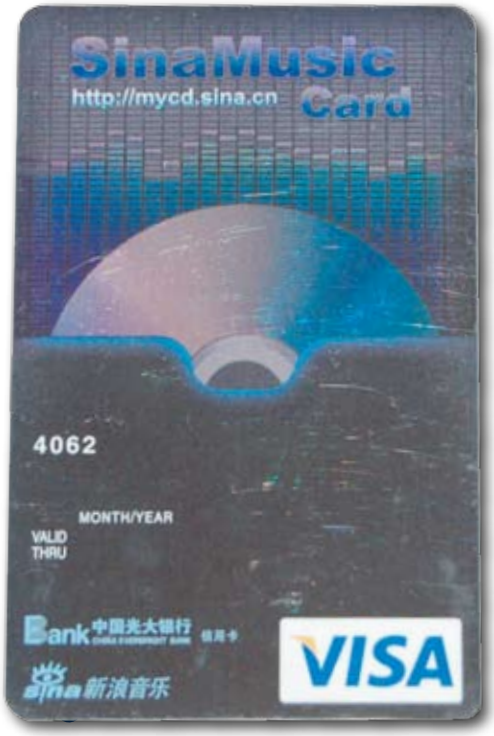
ICMA awards for card manufacturing, innovation

The International Card Manufacturers Association (ICMA) announced the winners of its annual Élan Awards for Card Manufacturing Excellence at an awards ceremony in April as part of the four day ICMA EXPO in San Juan, Puerto Rico. The awards recognize the latest innovations and technical achievements in card design. Entries were judged solely on the card's features as entries were not identified by company.

In the identification category the winner was the Nunavut Driver License that is manufactured by Canadian Bank Note Company Ltd. The U.S. Passport Card and Guanajuato Driver License were finalists in the category.

The judging criteria for the identification category is most creative, attractive or unique card used for identification purposes based on the aesthetics of printed surface design as well as technical advances to meet application security standards and other customer needs.

In the access control category the winner was the Illinois River Energy Card manufactured by Vanguard ID Systems. Illinois River Energy produces ethanol. The access control card criteria was judged on most useful, attractive or creative card used for access control.



The winner for the secure financial card design category was Sina Music Channel co-branded credit card. The card is manufactured by Huangshi G&D Wanda Security Card Limited for China Everbright Bank.

Finalists in the category included Xelion MasterCard manufactured by Future Card for Bank Pekad SA of Poland and Elevate Card manufactured by CPI Card Group for Virgin America/Barclays Bank.

Judging attributes in the secure financial card design category include the creativity that went into the card's design, such as the aesthetics of its printed surface that meet the parameters of Visa, MasterCard, American Express, Discover, JCB and Diners Club.

Biometrics make payroll check cashing easier and safer

When you're in the payroll check cashing business, you want to make sure you don't get stuck with bad paper. You also want to make sure that the person you're cashing a check for is legit. If he's willing to leave his fingerprint, he likely is.

A company that specializes in providing check cashing service using fingerprints is Herndon, Va.-based AllTrust Networks. In business for 11 years, the company until last March, was called BioPay Paycheck Secure. The check cashing system itself is called Paycheck Secure. "When we began the business, we had a much different intent," says George Rice, AllTrust's executive vice president for sales and marketing.

"The old name came from biometrics we supplied to the mainstream U.S. consumer population letting connect their fingerprint with a loyalty or check card," he adds. The name change is part of the company's strategy to position itself as a provider of what it calls "decisioning" data in the alternate financial services market, i.e. check cashing.

"We have a different focus," says Rice. The company has expanded to prepaid card issuance and bill payment services to complement its base check cashing system which enables retailers to better meet their customers' needs and perhaps gain new customers.

The purpose behind the system is to make sure individuals don't cash bad checks. Once the individual enrolls in the system, if they pass a bad check they won't be able to do it again at that location or any of the retailers using AllTrust.

So far, AllTrust has 2,000 retailer locations in 47 states – primarily in California, Texas and Florida – utilizing its fingerprint ID management service. It also has 5.5 million fingerprints stored in its database. About half of those retailers are grocery stores. Others are liquor stores and check cashing locations.

When you first enroll at a retailer a government-issued ID is also scanned and the fingerprint is enrolled. The whole process takes about 30 seconds, says Rice.

Compare that with a check cashing process in a store not using fingerprints. "If someone walks up to the counter of your grocery store and hands you their paycheck, you would normally have to call the bank and employer, maybe even ink fingerprint them. It could be a five minute process," says Rice.

AllTrust uses a fingerprint scanner to capture an image of the fingerprint. The software then collects data points and comes up with a resulting template. "A fingerprint ID needs to be accurate and fast," says Rice. "Normal fingerprint technology is usually not able to scan a large size database quickly enough."

The fingerprint template is stored with both the retailer and at AllTrust headquarters. Once signed up the consumer only needs to be fingerprinted once. "An individual who is enrolled at one location is enrolled at all locations," adds Rice. And once enrolled, all a customer has to do is present a finger when cashing the check.

"As easy as it is to get fake IDs today and print bogus checks, this system eliminates the opportunity for folks to recreate their identity," says Rice.

The service also enables retailers to service customers. "We're capturing identifications and measuring people who are generally not on the credit map," Rice says. "They don't have credit histories, many don't have Social Security numbers, but they're honest people and we provide a very valuable service for that individual."

AllTrust packages its product with several options for the retailer. There's an up front expense to implementing the hardware and software part of the system, says Rice. There's also a monthly subscription charge that includes unlimited use of the program.

A third element is elective for the retailer and includes check guarantees and electronic depositing. "In the check cashing business, cash is your inventory and a retailer is very interested in quick settlement of that transaction. Our clients have these funds available the next day." ID

Standard European ID card moving forward

The European Union is funding a project to create a standard university ID card for students. The project has been granted U.S. $1.3 million to create a prototype system for the credential, said Eugene McKenna, chief executive of campus services, Waterford Institute of Technology in Ireland.

McKenna, who also chairs the European Campus Card Association's Standards Committee, made the comments at the National Association of Campus Card Users Annual Conference in Orlando, Fla.

The idea behind the student ID is to set up a framework where students can study at different universities across the continent without having to physically carry academic records, McKenna said. The ID will act as a key for students to access these records.

For example, if a student were going to study aboard for a year he would go to the registrar's office and have his academic records uploaded to a secure server. The student would be authenticated with the ID and a fingerprint biometric.

After arriving at the other university the student would again use the ID and biometric to be authenticated and this would enable his records to be downloaded to the other university.

"We're trying to get a few basic standards in place that would work on campus," McKenna said.

If universities were using the same card technology it would be easy to grant a student access rights with that ID instead of issuing a new card. The student's ID could be programmed with the proper rights when he arrives at the new university.

In the trial phase, students from Waterford and the Technical University of Lodz in Poland, two members of the consortium, will become trial exchange students.

The project will use NXP's Mifare technology to start, but will review other options as well, McKenna said.

Europe-wide standardization of campus cards is the brainchild of the ECCA, founded six years ago. It was modeled after the National Association of Campus Card Users in the U.S., and now has more than 500 members representing some 5,000 higher education institutions.

McKenna said European campuses are six to seven years behind U.S. campuses. He said that unlike the U.S. market, there aren't many vendors selling campus card solutions in the European market and only about 20% to 25% of campuses even have an ID.

Biometrics *catching* in health care?

As health care providers move to electronic records, correct patient identification becomes a priority

President Barack Obama wants every citizen to have electronic medical records. One of the challenges in health care though is making sure the correct record is linked to the right patient and that the information is secure.

Smart card and biometric vendors are vying for position in the rapidly emerging patient identification market. One vendor who is tailoring biometrics to the health care market is Tampa, Fla.-based HT Systems. The company has taken Fujitsu's palm vein biometrics and customized it for health care and patient ID.

Palm vein biometrics uses infrared light to capture the user's vein pattern. Health care could be a good market for palm vein because it requires little to no actual physical contact with a scanner, unlike fingerprint biometrics. The scanner reads the palm vein pattern from a few inches away.

BayCare Health System and ValleyCare Health System have deployed the solution from HT Systems in the past year. Both are in the process of rolling out electronic medical records throughout their facilities and each saw the importance of accurate patient identification.

Mike Wisz, an independent health care IT consultant, says that patient identification can be tough for large health systems. Patients with common names, and duplicate records are all issues that providers have to deal with, he says.

Biometrics is one possible solution, Wisz says. But it may be a few years before there is widespread use of the technology. "Some people see biometrics as something a bit more futuristic," he says.

But for some the future is now. Tampa, Fla.-based BayCare Health System is in the process of transitioning its 3.1 million patient records to an electronic format, says James Shwamb, vice president of patient financial services at the provider.

A big part of the initiative is to make sure the patient and medical record are correctly matched. "For us to bring all this to bear we have to be able to quickly and accurately identify the patients," Shwamb says.

Before the transition, if BayCare couldn't positively identify a patient it would start a new record, Shwamb says. This could lead to confusion as multiple records for the same name appear in the database. BayCare wanted something that could help assure identity.

Shwamb says executives looked at smart cards, but didn't think the carry rate would be high enough, and decided against fingerprints because of the stigmas surrounding that technology. "We found palm vein and it seemed to be a perfect fit," he says.

BayCare started the project in March 2008, says Lynda Gorken, director of management support at the health care provider. Since then the system has deployed 350 palm vein readers system-wide at nine hospitals, 11 clinics and 23 labs.

When a patient arrives at registration he presents a hand for authentication. If the patient isn't already enrolled in the system he must present a government-issued photo ID and other information, which is entered into the system. The patient also has the palm vein information scanned and entered. "It takes less than a minute," Gorken says.

Upon return visits the patient provides date of birth and the biometrics to check in for appointments, Gorken says.

Registering and using the system is voluntary, Gorken says, and so far BayCare has enrolled 140,000 patients. "Patient reaction has been positive, very few have refused," she says. "One patient refused and was given a pamphlet and then came back and enrolled."

Shwamb says patients were concerned about identity theft and saying their Social Security number in a crowded waiting room before an appointment. All patients need to do if enrolled in the palm vein system is state a date of birth.

Lowering the risk of identity theft is how Pleasanton, Calif.-based ValleyCare Health System is selling the system to patients, says Rogel Reyes, director of patient access at the health care provider.

ValleyCare launched the system on Sept. 30 at its two facilities, deploying 35 devices and as of March enrolling 13,000 patients. The health care system wanted to comply with "Red Flag Rules," which makes sure providers are doing everything possible to correctly identify patients, which went into affect last year, Reyes says.

ValleyCare's use of the palm vein system is otherwise similar to BayCare's, though Reyes says the hospital is looking at other applications for the technology. For example, if a patient is hospitalized his palm could be scanned for positive identification before medication is administered.

As patients and health care providers become comfortable with the biometric ID system, the opportunity for expanded safety, privacy, convenience and efficiency all can be improved.

BayCare started the project in March 2008, says Lynda Gorken, director of management support at the health care provider. Since then the system has deployed 350 palm vein readers system-wide at nine hospitals, 11 clinics and 23 labs.

iPhones invade college campuses, but will they replace the student ID?

University campuses have gotten smaller, not in terms of physical layout, but in the time it takes to reach out to a student. Land line telephones are old news as students are tethered to their cell phone. The challenge for many college administrators today is how can they put that cell phone to work for both students and the college.

In the wake of tragedies at universities around the country many have deployed emergency alert systems that text or email students if there's a problem on campus. But there are other ways to take advantage of the mobile device that may be seen as "cooler." And if you're going to dive into this area, why not do it with one of the most popular phones around, at least for the college-age student, the iPhone. It has even led to the development of a cottage industry of applications, anything from help in managing finances to tracking where the stimulus dollars are being spent and how they're being used.

In Palo Alto, Calif., home of Stanford University, developers of an iPhone application called iStanford 2.0 hopes one day to see the iPhone replace the campus ID card. The entrepreneurial Stanford students have already produced a suite of iPhone applications that access the university's course catalog, campus map and other resources.

The application suite was rolled out in October and has already garnered national attention, including winning the $10,000 grand prize for AT&T's "Big Mobile on Campus" contest for best smart phone application. One of the student members of the firm said he hopes to see the iPhone replace student identification cards in the future.

But with projects of this magnitude, baby steps are needed. Blackboard Inc., which provides various software and services to colleges and universities, has also dipped its toe into the iPhone application market.

Blackboard has tapped the power of the iPhone, giving students one more way to easily access their grades, course assignments and more.

Blackboard's Learn offering is in use at 2,000 higher education institutions as well as K-12 and government and corporate entities. "It's an online education platform whose primary purpose is to manage online course delivery for institutions," says Greg Ritter, Blackboard's director of product management.

While some institutions rely on Blackboard Learn for delivering curricula entirely online, "most institutions use it in some sort of blended approach, like Georgetown will offer classes face to face but will also have a Blackboard site to extend the classroom beyond four walls," says Ritter.

The company earlier this year released a free iPhone and iPod Touch application, available from Apple's iTunes store, that enables students to access course information wherever and whenever they are. Students accustomed to logging in to their institution's Blackboard Learn platform every day can now tap in to mobile learning opportunities by receiving updates and alerts on grades, assignments, tests and other information.

The iPhone application follows the earlier release of a Blackboard Learn extension that interacts with the popular social networking site, Facebook, enabling users to access academic information within the Facebook interface.

"Millions of students every day log into Blackboard and into Facebook and it just made sense to bring the academic information to places where users already are," says Ritter. "The amount of time they (students) spend in Blackboard Learn is dwarfed by the amount of time they spend in Facebook or on their iPhone," adds Ritter. "We wanted to make sure they had the ability to get information about what's going on in their course without having to leave Facebook or their phone."

Why the iPhone?

Blackboard went with the iPhone because it offers a "robust" platform to application development, says Ritter. As to other smart phones, like the Blackberry, Blackboard has no plans to support them. The "market is pretty much scattered" with other smart phones, he adds.

Whether Blackboard Learn will extend its iPhone application beyond accessing course work and keeping up with grades, the company isn't saying. "We're always exploring the opportunity to improve or enhance our offerings to users," says Matt Maurer, Blackboard's director of public relations. "Using the iPhone in Blackboard Transact (the company's campus ID card solution) is something we've had internal discussions about."

Want more campus ID related news?

Subscribe today to receive CR80News Magazine twice per year following the fall and spring semesters of higher education.

Sign up below...

Name _____

Job title _____

Company _____

Address _____

City _____

State/Province _____ Zip/Postal Code _____

Country: ❑ U.S. (FREE) ❑ *Other ($100) _____

Phone _____

Email _____

Signature _____ Date _____

* Non-U.S. subscribers: Fax this form and we will send you an invoice for $100 to the Email address you provide. Your subscription will begin when payment is received. To begin immediately, visit http://subscribe.AVISIAN.com.

❑ I would also like to receive a FREE subscription to the CR80News eDigest sent to my email address.

FAX this form to 850-222-4477
or subscribe ONLINE at http://subscribe.AVISIAN.com

RFID in the crime lab: Using technology to track evidence

David Wyld
Contributing Editor, AVISIAN Publications & Southeastern Louisiana University

There is no setting in the private or public sectors where a verifiable "chain of custody" is more essential – or more lacking – than the handling of evidence in criminal cases. In the United States, the legal system is dependent on the proper handling of all forms of physical evidence – from bodily fluids to cigarette butts to guns, knives and weapons of all sorts.

Such evidence must be managed from its retrieval from the actual crime scene through storage (with handling by police investigators and both criminal prosecutors and defense attorneys) until the items of evidence are presented in court often times years after the crime has occurred.

Thus, all law enforcement agencies must be concerned with the "chain of custody" as they collect, register, store, ship and track the evidence in their possession. Ensuring that this very unusual supply chain is secure and verifiable has been categorized as one of the fundamental responsibilities of law enforcement agencies, one that underpins the effectiveness and accuracy of the criminal justice system.

However, most law enforcement agencies have evidence handling systems that remain largely unchanged from the 1950s. Most police departments simply have an evidence room or warehouse.

These critical items are managed most often using paper-based systems, often without computerized inventorying. Not only are such manual evidence tracking systems time and labor intensive for police officers, they are prone both to inaccuracy and hope for intentional misuse and abuse.

Criminal cases have had to be dismissed before going to trial or lost in the courtroom due to critical items of evidence simply being lost in the evidence room. Likewise, all across the country, cases have been brought against police officers for internal theft of valuable items – such as narcotics, guns, jewelry, electronics, and cash – stolen from evidence storage facilities.

When agencies do conduct manual inventories of their evidence rooms, they are often surprised at the items that are not found – and confounded by some that are there. Some have dated back to cases that are decades old – items that should have long ago been returned to their rightful owner, or else, sold at auction, donated to charity, or simply disposed of after the case they were being held for had been adjudicated.

Surprisingly, there has been very little use of "new" technology in this area, with many agencies just now moving to hybrid systems with computerized databases fed by manual record keeping. To date there are very few bar code based evidence tracking systems on the market.

RFID is on the Case

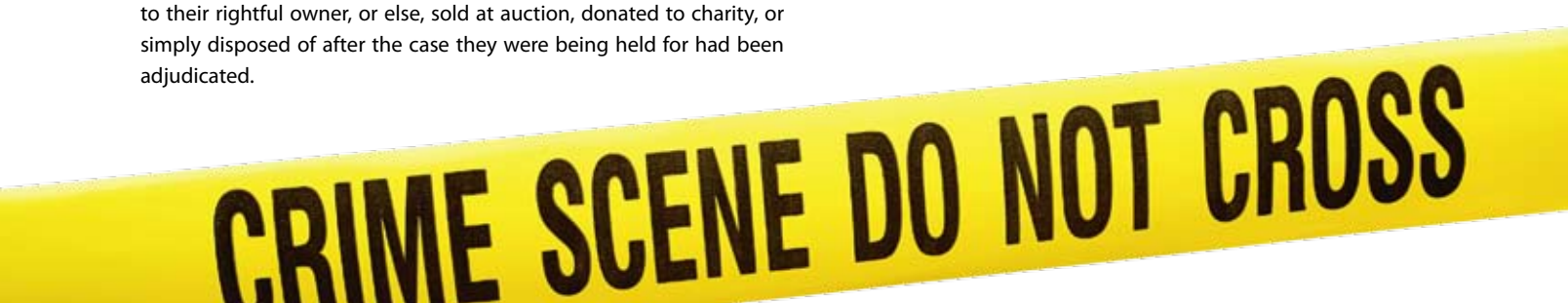
This sounds like a job for RFID, and today, there are several American firms that are looking to automatic identification technology as a way to reinvent the evidence management and tracking process. With RFID-based systems they can offer law enforcement agencies an electronic, verifiable chain of custody for evidentiary items in criminal cases.

Such systems also hold forward the prospect of not just more effective evidence management internally within a single agency, but new possibilities for bringing visibility and connections to what have been heretofore the ultimate information silos – with each separate police department having its own, often non-computerized and accuracy-challenged evidence tracking system.

The leading players in this market to date include:

- Intelligentz, based in Austin, Texas, offering the Clues and Blutrax tracking systems
- Lockwood Technology, based in Manchester, New Hampshire, offering the QuickTrac system
- Sysgen, based in Melville, New York, offering the eTraxx system

Each markets a variation on the same idea – RFID-based tracking of evidence from the point of collection in the field to the evidence storage facility and tracking all movements of such articles throughout their life span. Passive labels or tags are applied at the crime scene, with location and date/time data recorded through the use of either RFID readers or PDAs equipped with GPS. When the items are brought in from the field, they are held in a secure space with fixed RFID readers monitoring the doorways of the evidence storage room or warehouse.



Hand-held readers can then be used to locate items within the evidence facility. The systems work with either proprietary inventory management systems and/or standard database software to provide constant inventory reporting capabilities. They also offer the ability to create an electronic chain of custody report for individual pieces of evidence to know "where" and "when" the item was viewed or moved. As smart cards and electronic IDs are integrated into police agencies, "who" actually handled the item can be automatically recorded without any human intervention as well.

All three firm's systems are gaining traction in the law enforcement marketplace, each having multiple agencies using their tracking systems

Unique Features

The handheld reader used in the QuickTrac system not only tags the evidence on-site, but captures a digital photo of the item in the field.

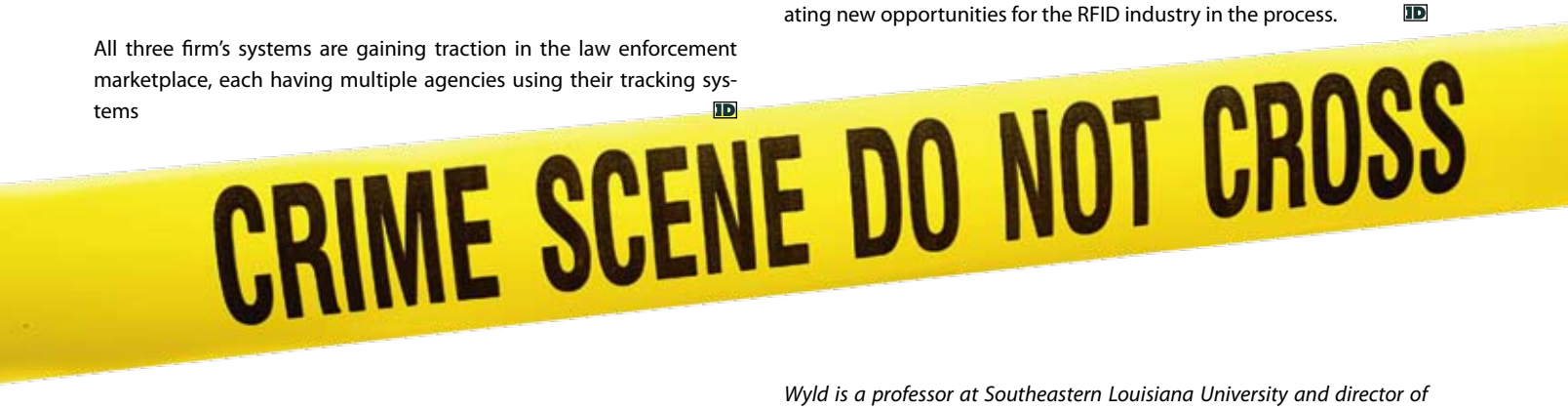
Intelligentz's Clues system includes the option of using active tags to track higher value. As such, the system can send alerts to supervisors if such high-security evidence is moved without.

What does RFID evidence tracking mean for the future of law enforcement and criminal justice – and the RFID industry? Certainly, the timing of the convergence between the technological leap forward that RFID represents and the rising expectations in criminal justice will propel many law enforcement agencies to have to seriously examine their evidence tracking processes.

This should bode well for these early entrant RFID integrators that are pioneering auto-ID technology in the law enforcement area. However, it will likely mean that we could see bigger RFID players also enter the law enforcement vertical as a new growth market for their own hardware, software and services or through market consolidation. If there is movement toward standardizing RFID–based evidence management protocols and further sharing of information between law enforcement agencies' databases, this could usher in nothing less than a new era in policing.

Michael Lucas, the founder and CEO of Intelligentz, recently described his vision for how such standardization and interlinking of law enforcement evidence management systems might work: "Having multiple agencies using a unified chain-of-custody application would create an unprecedented level of crime scene visibility. Lucas emphasized his point by illustrating that: "A size 5 glove found at a crime scene in one city might match the same type of glove found in another state. Without using such a system, there's no easy way to link those pieces of evidence."

So, over the next decade, RFID will likely play an increasingly vital role in helping to piece the puzzle together to help solve crimes by improving evidence collection, management, and tracking capabilities – creating new opportunities for the RFID industry in the process.



Wyld is a professor at Southeastern Louisiana University and director of the strategic e-commerce/e-Government initiative in the department of management. He can be reached at dwyld@selu.edu.

Managing airline trolleys with RFID to boost revenues

David Wyld
Contributing Editor, AVISIAN Publications & Southeastern Louisiana University

Introduction

The airline industry is being tested as never before. The business press has been replete with bad news for the industry of late and all over the world airlines are facing fast-rising costs, as jet fuel becomes their largest expense item by far.

They are also flying into a headwind, as demand for travel is falling in the wake of an economic downturn, and as availability increases for tech tools that enable us to meet and collaborate as never before. They have a product that is all-too-often viewed by consumers – jaded by their own personal bad experiences.

As reported in an August 2008 report entitled *Ancillary Revenue Generation: The New Operational Imperative for Airlines*, as point-to-point transportation for passengers becomes regarded as the base service level, all other services – checked baggage, meals, beverages, headsets, etc. will increasingly be offered only for the additional revenue streams they can generate. As such, more and more airlines worldwide are adopting the business models pioneered by low-cost European carriers, such as Ryanair and Easyjet.

U.S. airlines made headlines this past summer by implementing fees for checked baggage, to meals and soft drinks, and even certain coach seats. All of these actions may be precursors for a new business model for the airline industry. Advocates point to the fact that last year, the world's airlines generated over $2.5 billion in such ancillary revenue, with growth rates of 20% to 30% per annum. As the extra becomes the core, new revenue can be generated by not just traditional airline services, but expanded in-flight entertainment and shopping, as well as gambling. In fact, Ryanair CEO Michael O'Leary believes so strongly in the possibilities of ancillary revenue that he plans to offer half of the airline's seats for free by 2010.

Managing Airline Trolleys with RFID

Airline trolleys are increasingly being viewed as key elements in an airline's strategy – and perhaps its very survival. Why? In a nutshell, it's because these simple metal carts are the workhorses of airline customer service. They are the vehicles through which food, beverages, and a variety of service items are routed through a complex internal and external network to provide in-flight passenger service. However, today they are also the retail floor for the airline industry.

In the aisle of the commercial airliner, before a captive audience, airlines know that airline trolleys represent the future of a changing business model, increasingly dependent on what is referred to in the industry as "ancillary revenue." Yet, airlines often have no idea how many of these critical assets they own, where they are stationed, and what condition they are in.

In fact, according to the IATA (International Air Transport Association), airlines typically have to buy three to five chipsets (the quantity of trolleys required to fill all aircraft galley positions) when outfitting a new aircraft, just to ensure that they will have sufficient trolley stock available across their network of operations. This is an area ripe for the application of automatic identification technology.

As part of its "Simplifying the Business" Initiative, the IATA has targeted a wide range of airline operations that could be better managed and achieve cost savings through the application of RFID technology. In a study conducted last year by the IATA, the airline organization found that the world's airlines could achieve both immediate and long-term benefits from RFID-based trolley tracking.

Airlines would benefit from improved business intelligence to optimize the management of their trolley stock, enabling them to dramatically reduce the number of trolleys in operation to achieve their present service levels by eliminating unnecessary safety stock and having improved capabilities to manage the maintenance of trolleys. In the latter regard, the IATA believes that maintenance can be made much more proactive than it is at present, as all too often, flight attendants must work with inoperable or damaged trolleys.

Further, as trolleys are commonly interlined between air carriers and between catering services supporting airline operations, the improved inventory accuracy and movement-tracking capabilities will provide further savings. The IATA found that through improved tracking of the food and beverage contents of trolleys (some long flights on jumbo jets require upwards of fifty trolleys to service a full flight), airlines could cut costs by reducing the number of wasted meals, while bettering the in-flight experience of customers with special diets and other needs. To date, RFID pilots for trolley tracking through passive RFID systems have been ongoing with Air Canada and KLM/Air France and their catering suppliers, with official results expected early in 2009.

Analysis

The IATA believes that airlines that implement RFID-based tracking systems of their trolleys would experience immediate benefits from having increased visibility and control of trolley inventory. This increased business intelligence would translate into better management of their trolley stock in the field and the contents on-board the trolleys. In all, the IATA has constructed a business case that trolley tracking will provide quick ROI for airlines, often in the 12 to 24 month range, and even shorter if RFID trolley tracking investments are combined with an overall RFID strategy involving baggage handling, ULD tracking, and surveillance of parts and safety equipment.

Overall, the IATA estimates that while costs and benefits will vary based on the size and route structure of each air carrier, the world's airline industry could achieve almost half a billion dollars in annual savings from RFID-enabled trolley tracking, over and above the almost $50 million in immediate acquisition cost savings from reduced trolley purchases to support their present operations (with trolleys typically ranging between $600-$1000 per unit).

RFID-based trolley tracking will thus play a central role in this "brave new world" of the fast-changing airline industry. With the newfound emphasis on ancillary revenue generation, flight attendants will be tasked with being sales agents for these revenue items available on-board. As such, it will become increasingly important to have properly stocked trolleys with passenger consumables ready for use.

Airlines that implement RFID-based tracking systems of their trolleys will experience immediate benefits from having increased visibility and control of trolley inventory. This increased business intelligence would translate into better management of their trolley stock in the field and the contents on-board the trolleys.

Expanding touch points for contactless payments

Customers may not be able to use contactless payments when they go to a Starbucks in the U.S. but the coffee purveyor is deploying coffee machines that accept the tap and go payments.

Malvern, Pa.-based USA Technologies is the company putting the payment mechanisms into the coffee makers. The company's primary business is putting payment card readers along with the backend transaction processing into unattended devices, such as vending machines.

As more contactless payments cards are being issued – MasterCard announced it has 500 million PayPass devices in the field – the company is seeing a demand for contactless readers, says Mike Lawlor, vice president of business development and sales at USA Technologies. "What we're seeing is where there's existing cash payments we're converting to cashless payments," he says.

The integration with the Starbucks coffee machine is just the latest, Lawlor says. The brewer, which serves up an individual cup of Starbucks coffee, is being placed in hospitals, offices, hotels and other hospitality locations. Customers walk up to the machine, choose what they want, either swipe a mag stripe card or tap a contactless card, and the machine brews a cup of coffee for them.

USA Technologies is seeing activity in other micro transaction markets too, Lawlor says. Merit Industries sells touch screen games to bars and has incorporated contactless and mag-stripe readers into the games.

The Air-Serve Group, which provides vacuums and air pumps to gas stations and convenience stores, has put the payments technology into machines so customers don't need change, Lawlor says. Also, since USA Technologies provides connectivity to the machines the company can extract sales and operational data.

Along with providing the hardware for the vending machines, USA Technologies also handles the transaction processing. "We pre-authorize each card transaction and do the settlement in a batch process," he says.

Lawlor expects more devices to be equipped with contactless readers too. "It's becoming very prevalent," he says. "We have 50,000 devices already in vending machines across the country."

ctst 2009 THE AMERICAS

Smart Card Alliance

CONFERENCE AT-A-GLANCE

May 4-7, 2009
Ernest N. Morial Convention Center
New Orleans, LA

EXCLUSIVE OFFER: $300 Off Registration Rates! Use Code AVI
Or Free Exhibit Hall Pass! Use Code AVIP

Monday, May 4, 2009

9:00 AM - 12:00 PM	**WORKSHOP A** Smart Card Alliance: Smart Card Technology and Payments Applications	**WORKSHOP B** Mobile & Contactless Payments From EMV to NFC Collis
12:00 PM - 1:00 PM	Lunch Break	
1:00 PM - 4:00 PM	**WORKSHOP A** Smart Card Alliance: Smart Card Technology and Payments Applications (cont.)	**WORKSHOP B** Mobile & Contactless Payments From EMV to NFC (cont.) Collis
7:00 PM - 9:30 PM	Smart Card Alliance OSCA Awards & Networking Reception	

Tuesday, May 5, 2009

8:00 AM - 9:00 AM	Continental Breakfast				
9:00 AM - 9:30 AM	Welcome Remarks				
9:30 AM - 10:30 AM	Keynote Session: Payments Industry Executives Roundtable				
10:30 AM	Exhibit Hall Grand Opening				
12:00 PM	Lunch in Exhibit Hall				
	Concurrent Sessions - Choose from the sessions which best suit your needs.				
1:30 PM - 3:00 PM	**TRACK A: IDENTITY & SECURITY** gemalto Identity Concepts in a Digital Age	**TRACK B: PAYMENTS & APPLICATIONS** First Data Contactless Payments	**TRACK C: MOBILE & NFC** Mobile Technology & Applications	**TRACK D: EMERGING TECHNOLOGY** Biometrics Standards & Technology	**TRACK E: HEALTHCARE** Healthcare Data Management
3:00 PM - 3:30 PM	Networking Break in Exhibit Hall				
3:30 PM - 5:00 PM	Identification and its Role in Securing Cyberspace	EMV Payments	Mobile Business Model Roundtable	Smart Cards, Tokens & Digital Identity	Health ID Cards & Applications
5:00 PM - 6:30 PM	Networking Cocktail Reception in the Exhibit Hall				

Wednesday, May 6, 2009

8:00 AM - 8:30 AM	Continental Breakfast				
8:30 AM - 10:00 AM	Keynote Session: Identity and Security Executives Roundtable				
10:00 AM - 10:30 AM	Networking Break in Exhibit Hall				
	Concurrent Sessions - Choose from the sessions which best suit your needs.				
10:30 AM - 12:00 PM	**TRACK A: IDENTITY & SECURITY** Citizen and Government ID Applications and Usage Models	**TRACK B: PAYMENTS & APPLICATIONS** Payments Trends and Applications	**TRACK C: MOBILE & NFC** NFC Technology & Applications	**TRACK D: EMERGING TECHNOLOGY** SIMcard and Secure Memory Card	**TRACK E: LATIN AMERICA** ID & Security
12:00 PM - 1:30 PM	Keynote Luncheon (Conference Attendees Only/ Exhibit Hall Only Attendees $50 Fee) Enabling End-to-End Trust in the Digital Transaction Age Randy Vanderhoof, *Executive Director,* SMART CARD ALLIANCE * *See Session Description Below*				
1:30 PM - 3:00 PM	Employee ID Applications and Usage Models	Transportation Payments	NFC Mobile Payment Ecosystem and Business Model	Secure Chip Design & Manufacturing	Payments
3:00 PM - 3:30 PM	Networking Break in Exhibit Hall				
3:30 PM - 5:00 PM	International Government ID Applications	International Payments Models	NFC Beyond Payments	Cryptography	Transit/Mobile
5:00 PM - 6:30 PM	Networking Cocktail Reception in the Exhibit Hall				

Thursday, May 7, 2009

8:00 AM - 8:30 AM	Continental Breakfast			
8:30 AM - 10:00 AM	Keynote Session: Mobile Business Executives Roundtable			
10:00 AM - 10:30 AM	Networking Break			
	Concurrent Sessions - Choose from the sessions which best suit your needs.			
10:30 AM - 12:00 PM	**TRACK A: IDENTITY & SECURITY** Biometrics Identity & Security Applications	**TRACK B: PAYMENTS & APPLICATIONS** Payments Security	**TRACK C: MOBILE & NFC** International Mobile Use Cases	**TRACK D: EMERGING TECHNOLOGY** Smart Card Readers and Controllers
12:00 PM - 1:00 PM	Lunch			
1:00 PM - 2:30 PM	Using Trusted Identity Across Domains	Prepaid & Loyalty Programs	Mobile Security	ID Card & Security Standards
2:30 PM - 3:00 PM	Networking Break			
3:00 PM - 4:15 PM	Roundtable Discussion Sessions - Identity/Security and Contactless/Mobile			

Identity and Access Management Solutions

Physical Access

Logical Access

Convergence

Card Issuance

Embedded Technology

Identification Technology Solutions

Cashless Payment

Industry & Logistics

eGovernment

Food & Animal

HID Global, the worldwide leader in access control cards and readers, now offers an entire spectrum of secure identity solutions.

HID has built a global reputation for quality, reliability and innovation in access control cards and readers. Now, we've expanded our offering to include everything from IP-based access control to public transport solutions to the design and production of credentials. We believe the future of secure access and identity lies in open platforms, flexible products and the convergence of technologies. We're making that a reality. So if you need a secure identity solution, look to HID. Chances are, it's already in the cards.

hidglobal.com

HID

ACCESS choices.