re:ID

Winter 2008

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

BEYOND ISSUANCE ...

e-passports struggle to achieve usage

Is identity broken?

EU considers student ID

Registered Traveler in flux

Plus NFC, RFID, biometrics

AVISIAN

PIVMAN

Handheld device
by DAP Technologies
www.daptech.com

Is he legit? Are you sure?

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

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

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

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

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

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

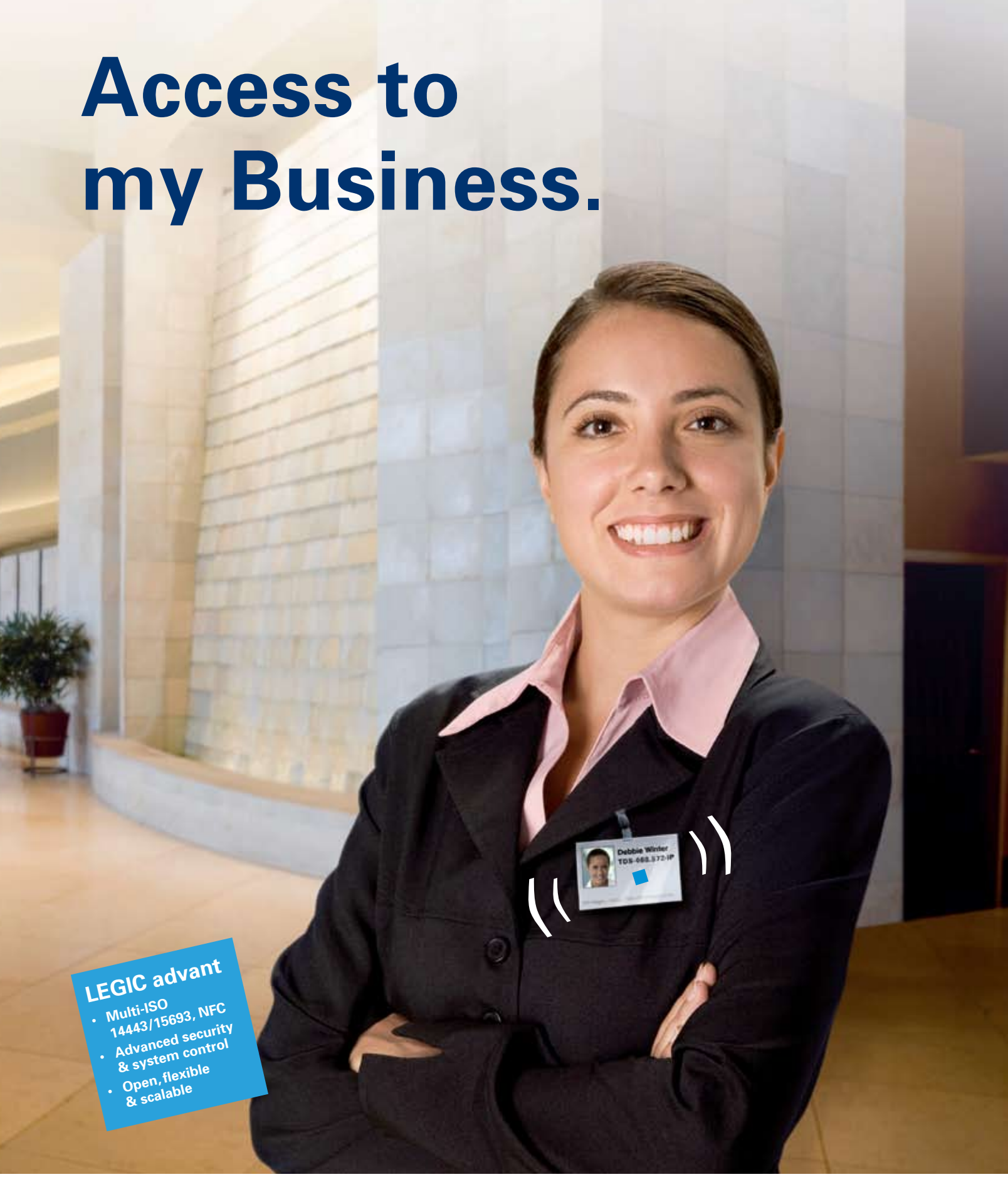
TSGP
PSGP
IBSGP
BZPP
SHSP
UASI
LETPP
MMRS
CCP
EMPG

CoreStreet ENABLED

174_0207

CORESTREET®

Access to my Business.



LEGIC advant

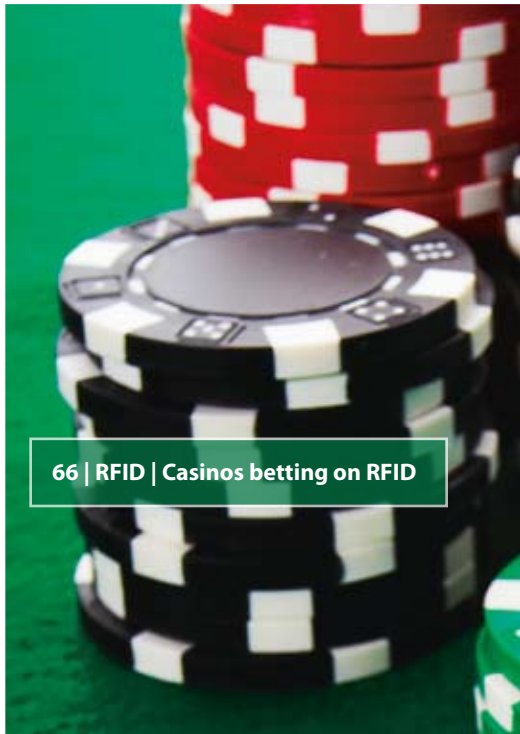
- Multi-ISO 14443/15693, NFC
- Advanced security & system control
- Open, flexible & scalable

Any application I can think of, any security level I demand.
All in one card – Proven and superior, the best value for my money.
Contactless smart card technology: www.legic.com

LEGIC®
innovation in ID technology

Winter 2008

Contents



INDEX OF ADVERTISERS

Broken Identity?

Zack Martin
Editor, AVISIAN Publications

Get ready to read about some great identity projects in the pages that follow … but also prepare to consider whether our concept of identity is fundamentally broken.

I've known Steve Howard for a number of years. Howard, vice president of business development at Thales e-security, is someone who can explain the most complex, technical aspects of systems to where just about anyone can understand it.

Since I joined AVISIAN Publishing we have chatted about him contributing to the publication and his first piece appears in this issue on page 36. He wanted the piece to be collaboration, something we both thought needed to be covered.

When we heard U.S. Department of Homeland Security Sec. Michael Chertoff's August speech we had a jumping off point. Chertoff spoke to the University of Southern California National Center for Risk & Economic Analysis of Terrorism Events about the importance identity plays in the 21st Century (See page 40 for the full story).

We must get to solutions that enable individuals to protect their own identity. Enabling protected identities for all will require new thinking.

The progressive thinking about identity expressed in Chertoff's speech surprised me. I felt that he said identity, as it's done now in the U.S., is broken and there needs to be more done to protect it. "It lies at the core of a great deal of what we do protecting our financial security, our personal security, and our reputational security," Chertoff said.

Howard and I used this as a jumping off point – one that hopefully will result in a series of articles on what can be done to improve identity in the U.S.

In this initial piece, Howard makes the argument that identification is indeed broken. He explores a number of different points to get to one conclusion: "We *must* get to solutions that *enable* individuals to protect their own identity. Enabling protected identities for all will require new thinking. And this requires specific action by government agencies, legislators and the private sector."

Don't get me wrong, there are a number of solid projects underway, Real ID and FIPS 201, but none of them go far enough. Real ID does a decent job on the vetting aspect but falls short on the actual credential. FIPS 201 is a laudable start but many are finding that it falls short in key areas, and it doesn't impact the citizenry.

One of the major issues I see is the Internet. There is no way for the average citizen to verify an identity online. Howard proposes enabling private companies to issue highly secure credentials to anyone who wants them. The individual would have to undergo intense vetting, but after that they would have a credential to authenticate identity in the real and virtual worlds.

The masses don't yet understand the importance of identity. Yes, they have some knowledge of identity theft and know that they shouldn't share their Social Security number or other private data, but that's probably the extent of it. And that is not nearly enough. The government and private corporations need to do more to help individual's protect their identity. In the future we will explore ideas of how this might be done.

We've issued 100 million e-passports, so now let's try to read 'em

Chris Corum
Executive Editor, AVISIAN Publications

This editorial marks the completion of the magazine's fourth year, 1088th printed page and sixteenth issue.

Like this issue, the cover of our inaugural magazine from February 2005 had an image of passports. But they looked a little different. Back then the now-common e-passport symbol wasn't printed on the booklets and inside there was nothing but paper.

That cover story investigated the bid process that was underway to select suppliers for the initial issuance of electronic passports in the U.S. The very first sample units were being 'taped together' for stress testing. When it came to the future of the program, very little was certain at that point.

Fast-forward four years, sixteen issues and 1088 pages … to this cover story showcasing tremendous e-passport progress. Literally, we have gone from zero to 100 million. Worldwide e-passport issuances now top the 100 million mark with the U.S. nearing the 15 million milestone.

As we learned from the recent interoperability tests conducted in Prague, the challenge of issuance has been replaced with the challenge of inspection. For the most part, countries around the world have ironed out their difficulties with procuring, producing and delivering the advanced documents to citizens. The long lines and lengthy delays common in the early years have subsided greatly.

But insiders fear the lines may simply be moving from one point in the process to another. Very few inspection points are making use of the "e" in e-passports. The new challenge is occurring in the field, at customs and entry points around the world. The equipment and training required to read the data in the contactless chip, make use of the stored biometrics, and implement the security provisions built into the booklets provide the next great obstacle.

This challenge is further complicated by the evolution of the security methodology used to control access to personal data and biometrics stored in the chip. The initial Basic Access Control methodology is being replaced in some countries with a more secure alternative. The newer Extended Access Control has been mandated for use by European Union countries by June 2009.

When will we start to utilize the investments made in the new passports? The real answer is unlikely to come from a mandate. More likely it will occur when the vendor community and those agencies responsible for inspection points around the globe get the equipment and the process figured out.

Inspection can't cause any truly significant delays or the public will revolt. Because if I have learned anything in the four years of producing this magazine, it is that the people want security but they don't want to be inconvenienced by it.

I hope you enjoy these 68 pages as much as I have enjoyed helping to bring all 1088 to you. ID

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

EDITOR
Zack Martin, zack@AVISIAN.com

CONTRIBUTING EDITORS
Daniel Butler, Liset Cruz, Seamus Egan, Ryan Kline, Jay Swift, Angela Tweedie, Andy Williams

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.

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

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

Contactless IDs for EU students? Efforts underway to standardize campus identity cards across Europe

Eugene McKenna, Waterford Institute of Technology, spoke with re:ID podcast host Chris Corum about the efforts underway to develop standards for campus card programs across Europe. The European Union is currently considering a proposal to provide funding for the project, which is being called the European Education Connectivity Solution. Other topics include the differences and similarities between campus identity programs in the U.S. and Europe as well as the vendor landscape for the European market.

Highlights: "The campus card scene in Europe is at the very early stages, in years, I would say that it is fifteen years behind the U.S. The first key change took place here in 2002 when we set up the European Campus Card Association, which was modeled on the National Association of Campus Card Users in the U.S. Since 2002 the association has grown in membership to have approximately one hundred members.

"The problem in Europe is that we don't have a standard product, and that is what our whole project is about: developing a standard campus card system that can be used right across Europe.

"The purpose of the European Education Connectivity Solution is to research and develop a secure standardized campus card system. There are also some barriers that exist from one country to another in Europe. The key aim of this is that if a student is studying in Ireland one year and wants to move the following year to Poland or Germany, they should be able to bring their campus card with them. They should be able to bring their academic information with them. And there must be a standardized approach.

"You don't have a different system in every university, and a different system in every country."

To listen, visit SecureIDNews.com/podcasts and select "Episode 20"

Time to 'custom' make the donuts: Retailers use biometrics to personalize message

Customized offers based on your appearance using facial recognition biometrics? That's what YCD Multimedia is touting and will be piloting at Buffalo, N.Y.-based Dunkin' Donuts stores. Regarding ID Editor Zack Martin spoke with Barry Salzman, CEO at YCD Multimedia, about his company's technology and where he sees it going.

Highlights: "The facial recognition aspect is still in beta, and we are going to introduce that later on in the pilot. It is a pretty standard simple use of pattern recognition technology, and there are a whole lot of third party vendors in the market place that have developed this technology for different applications. We're working with a couple of those partners to integrate the pattern recognition capabilities with the YCD media playback capabilities.

"Very simply those pattern recognition technologies can identify somebody standing in front of a screen by gender and classify them into large age brackets: young kids, everybody in the middle, and senior citizens. Depending on our custom application, in some instances those demographic markets are an important part of market segmentation and targeting.

"In those instances, we would consider deploying facial recognition integration with the YCD media player capabilities, and what that will do is when somebody who fits one of those demographic markets stands in front of the screen, in real time, it will override whatever the preset playlist was and trigger the playlist for senior citizens for example."

To listen, visit SecureIDNews.com/podcasts and select "Episode 21"

Identity TV?

In 2008, the buzzword at AVISIAN Publishing was rich media. It's a fancy name for audio and video content on the Web and it is the new must-have for progressive publishers. We jumped in feet first with our Re:ID Podcast series, Government Smart Card audio coverage from the monthly IAB meetings, and our video segments from major identity-related conferences and events.

This year we had video crews onsite at CTST 2008, the Smart Card Alliance Annual Conference, the National Association of Campus Card Users Annual Conference, the Biometric Consortium Expo, and Smart Cards in Government. Next year we will do our best to be 'everywhere you want to be,' bringing you coverage from the events that are shaping our industry.

Checkout coverage online of the many industry-leading companies. Select "Videos" from the list of Article Categories on the left side of the page at any of our suite of ID technology publications.

NACCU 2008
Blackboard
CardSmith
CBORD
Color ID
Datacrd Group
Digion 24
Digital ID Soloutions
Dynamic Card Solutions
Hearltand Campus Solutions
HID Global
Identification Systems Group
Mac-Gray
Millennium Group
NuVision Networks
Off Campus Solutions
Persona
Pharos
Sequoia Retail Systems
SmartCentric
Vision Database Systems

CTST 2008
ACT Canada
Advanced Card Systems
CLEAR
CPI Card Group
Datacard
Datastrip
Gemalto
GlobalPlatform
INSIDE Contactless
Mühlbauer
Oberthur
Smart Card Alliance
Texas Instruments

Biometric Consortium Conference & Technology Expo
AOptix Technologies
Aware Inc.
Cogent Systems
Daon Inc.
Identica Holdings Corporation
IdentiPHI Enterprise Security Solutions
Lumidigm Inc.
Motorola
SAGEM Morpho Inc.
Sarnoff Corporation

Look for our camera crew throughout the 2009 trade show season.
If you would like to be included in future events, or if you would like more information about how you can be included, email info@avisian.com.

Visa working with Nokia, Android to deliver more mobile payments services

Visa contactless payments, money transfers and more are being added to Nokia's next generation NFC-compliant handsets beginning in October while at the same time Visa also announced plans to link with Google's new Android-powered handsets to make some mobile payment services available, first to Visa Chase cardholders.

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

The first set of services that Visa is planning to develop for Android will enable Chase Visa cardholders to receive notifications to their mobile devices about transaction activity on their accounts; obtain offers from a wide array of merchants; and use the built-in location-based technology developed by Google to quickly map nearby merchants where they can redeem Visa offers and locate ATMs that accept Visa.

During an introductory period, Visa mobile services that will be developed for the Android platform will first be offered to Chase Visa account holders. Following this initial launch phase, Visa plans to work with additional card-issuing financial institutions to extend availability of its mobile services for Android to their Visa account holders. Visa is also developing a payment application that will enable consumers with Visa accounts to make mobile payments in retail locations nationwide, or while on the go, over wireless networks.

"By developing these mobile services for the Android platform, Visa has taken a major step toward achieving our goal of combining two of the world's most powerful and ubiquitous consumer innovations, electronic payments and mobile technology," said Elizabeth Buse, global head of product at Visa Inc. "Through this effort, U.S. consumers will, for the first time, be able to download Visa mobile service applications directly to their handsets."

The Nokia 6212 classic includes integrated NFC chipsets which lets the mobile device behave like a contactless payment card. Nokia and Visa first demonstrated NFC technology in December 2005 with the launch of the first large scale NFC trial in the United States at the Phillips Arena in Atlanta.

This represents the next phase in an ongoing effort between Visa and Nokia to make mobile payments a reality for consumers around the globe. The long-term collaboration between Nokia and Visa has already resulted in multiple trials of Visa mobile payments enabled through NFC technology on four continents, including in the United States with Wells Fargo Bank; in Malaysia with Maybank and Maxis; in Taiwan with Chinatrust Commercial Bank and Chunghwa Telecom; and London with Barclays Bank.

Sesames finalists named

Thirty five finalists are in the running for 10 Sesames awards that will be presented during the 2008 edition of the CARTES & IDentification show Nov. 4-6 in Paris. At first there were 233 entrants, but the field has been cut to 35. It's a field which features some of the top names in the industry, including Gemalto, Oberthur, Giesecke & Devrient, NXP, Infineon and more.

The awards will actually be presented on the eve of the show's kick-off. Here are the finalists by category:

- Hardware: Infineon Technologies, SLE 78 Family with Integrity Guard; Infineon Technologies, SLM 76 Security Controller for Machine-to-Machine applications; INSIDE Contactless, MicroRead.
- Software: Gemalto, Smart Card Web Mashups; Hypercom, Hypersafe32; Oberthur Technologies, SafeSTIC.
- Identification: Identita Technologies International, ID-Touch; Motorola, Motorola Bio-Enrol; Motorola, Motorola Mobile AFIS; Smart Packaging Solutions, Antiskimming solution for e-Passport.
- IT Security: Gemalto, BioPIN-enabled Gemalto.NET smart cards; Giesecke & Devrient, StarSign Mobility Token; GO-Trust, GO-Trust SD Solution; Privaris, plusID 75.
- Transport: Giesecke & Devrient, Touch & Travel; Oberthur Technologies, WebSTIC Fly; Smartsoft Information Technologies, SmartCity.
- Banking/finance/retail: Thales, Thales SafeSign Pilot Package for mobile authentication; XIRING, BioPass; XIRING, Xi Sign wallet.
- Health care: gematik - Gesellschaft fA 1/4r Telematikanwendungen der Gesundheitskarte, Mobiler Konnektor; Hypercom, medCompac; NXP Semiconductors & Austrian Research Centers, KeepInTouch-NFC solution; Oberthur Technologies, HealthSTIC.
- Mobile: Neowave, Weneo-NFC; Oberthur Technologies, GIGANTIC WUAOW; Oberthur Technologies, WebSim Local Advertising.
- E-transactions: Atos Worldline, Fast booking on ATM; EtherTrust & Sagem Orga, TLS-Tandem; Immigration Department (ImmD) of the Hong Kong Special Administrative Region (HKSAR) Government, e-Passport Self-service Kiosk; SafeNet, SafeNet ViewPIN+.
- Loyalty: Contactless Data, MobiFetch; Experian, Come&Tap; garanti Payment systems, Flexi Card; ViVOtech, ViVOnfc 3.0.

Giesecke & Devrient opens R&D center in India

Giesecke & Devrient (G&D), one of the world's leading providers of smart-card solutions, is opening a new development center in Pune, India.

The center's approximately 80 employees are developing products based on smart card technology for applications in mobile communication, electronic payment and public administration. Over the next few years, the center intends to double the size of its workforce to 150 by recruiting other IT specialists.

The Pune facility is one of three G&D Development Centers – alongside those in China and at Group headquarters in Munich, the latter being responsible for controlling all R&D activities. Already in 2007, the German security technology group boosted its research and development expenditure by 25 percent to more than $145 million.

Bid aims to take Oberthur Technologies private

François-Charles Oberthur Fiduciaire (FCOF) is attempting to buy out its minority shareholders and take subsidiary Oberthur Technologies private, according to a company spokesperson. FCOF already owns 70% of Oberthur Technologies shares.

FCOF is offering $9.81 per share, which would end up costing the company more than $294 million to take the smart card and security company private. A board meeting is scheduled for Sept. 26 to take a final position on the offer, according to documents released by the Oberthur Technologies.

Dublin selects IBM for citywide smart ticketing system

Dublin's Railway Procurement Agency has chosen IBM to create and implement the infrastructure for a public transport ticketing system in the greater Dublin area. The payment system will enable commuters to use a single pre-paid contactless card similar to London's Oyster, for travel on all buses, trains, trams and coaches in the city.

This next generation automatic fare collection solution has the capacity to process up to two million transactions a day and can be extended to include other value-added services such as reloading the card via the Internet and retail payments.

The new system, part of Ireland's "Transport 21" project, is the largest investment ever in the country's transport system. Ireland plans to invest a total of $50 billion until the year 2015, to deliver world class transport to its citizens.

The ITS system eliminates the need to carry cash to pay for tickets, and enabled fast, secure and convenient transactions. The smart card is simply "re-charged" as needed. The integrated IBM back-office system will provide ticket and smart card management, central reconciliation and settlement services to all public transport providers.

The ITS Solution to be implemented in Dublin will use IBM's platform running Integrated Ticketing application software from MSI Global from Singapore. In 2006, Singapore chose the IBM technology platform to support its customized smart card e-payment infrastructure and enable the long-term growth of the public transport ticketing system.

In addition to working with the city of Dublin, IBM is also assisting the cities of London, Stockholm, Singapore and Brisbane, to meet traffic management and congestion challenges. IBM has established a team of professionals working on a range of technologies and solutions, including researching, testing and developing new Intelligent Transport system management capabilities.

Work on the Dublin project begins immediately and a phased deployment of the live system will will begin in late 2009.

Datastrip's mobile devices now available with TETRA

Datastrip, a developer of biometric identity solutions, has announced that they are now offering their mobile biometric device, DSVII, with Motorola's Terrestrial Trunked Radio Communication (TETRA) capabilities.

TETRA is a digital radio standard developed by the European Telecommunications Institute and will enable users of Datastrip's DSVII devices to access remote databases securely via its own communications or WiFi 802.11, Bluetooth, GSM and GPRS.

The DSVII devices are designed for mobile identification authentication by using a contactless smart card reader and/or fingerprint reader. The DSVII is designed as a biometric solution for military, border control and law enforcement needs in the field.

Daon unveils UnifiedID

Daon announced that it would unveil its new UnifiedID product at the Biometric Consortium Conference Sept. 23-25 in Tampa, Florida. UnifiedID is a system that provides secure biometric enrollment, verification, and provisioning to logical and physical access systems.

With UnifiedID, users can enroll a person's biographic information, fingerprints, and photograph in one place and have it available for accessing secure physical areas as well as computer networks. The system is built on the Daon platform, providing vendor neutrality, scalability and security.

The UnifiedID product can be seen at BCC in expo booth # 201, along with Daon's latest release of DaonEnroll (version 2.2) and a number of partner solutions demonstrating the integration of devices and algorithms with the Daon biometrics platform.

Staples' Canadian stores to accept contactless and EMV cards

The 300 Canadian stores of office retailer Staples will soon be accepting contactless credit cards, including those that are EMV compliant, as the country transitions to the more secure chip and pin technology.

Staples will begin installing MasterCard PayPass-enabled readers and chip card terminals in its Staples Business Depot and Bureau en Gros stores across Canada beginning early next year.

Credit and debit cards are being upgraded with chip technology in order to enhance the security of payments. The way you complete a transaction with your MasterCard chip-enabled card will change, but the card will continue to function as a normal credit card with all the same features. In the future, instead of swiping a card that has a magnetic stripe on the back, cardholders will insert a card that has a computer chip embedded on the front. Instead of signing to verify a payment, cardholders will enter a PIN.

In addition to better security protection, the chip system can be used to provide new payment features like MasterCard PayPass. Signatures are not required for purchases under $50 (Canadian) and receipts are always available. Purchases over $50 (Canadian) will still require a receipt signature.

In addition to the EMV features of the card, Canadian MasterCard cards will also continue to carry magnetic stripes in order to be compatible at retailers who have not yet upgraded their payment terminals to accept the new chip cards as well as in other parts of the world where chip technology is not available.

New York State issuing enhanced driver licenses

De La Rue Identity Systems is supplying the New York State DMV with the solution to issue its new enhanced driver license. The new document includes a combination of advanced anti-counterfeit and security technologies.

The new document can be used in place of passports for travel by land or sea to Canada, Mexico, the Caribbean and Bermuda. The EDL will be issued from Sept. 16 to U.S. citizens with New York State residency. The state expects to issue around five million of the EDL and existing license documents per year.

The EDL includes a range of pre-printed security features on both the front and back of the card and incorporates an RFID tag and antenna. The EDL will be issued alongside the existing New York State driver license which is also supplied by De La Rue Identity Systems.

Southwest Airline pilots undergo biometric screening

More than 200 Southwest Airlines pilots will participate in a biometricscreening program at Baltimore Washington International Airport over the next two months. The SecureScreen program is using biometric and identification technology from Chicago-based Priva Technologies.

Southwest pilots participating in SecureScreen undergo enrollment using Priva's Cleared Security Platform, which stores their fingerprints, photograph, and other protected security information on a ClearedKey. The ClearedKey data can only be accessed by TSA at a security checkpoint, where the reader verifies the pilot's fingerprint and also provides an additional layer of security by showing the TSA agent the pilot's photograph. After positive identification, TSA clears the pilot to proceed into the secure area to report for flight duty.

SecureScreen was jointly developed by the Southwest Airlines Pilots Association (SWAPA), Southwest Airlines (SWA), the Coalition of Airline Pilots Associations (CAPA), Maryland Aviation Authority (BWI), officials from TSA, and Priva Technologies. ClearedKey utilizes commercially available, biometrically enabled microchips with the government's FIPS 140-2 Level 3 certification.

SecureScreen addresses the congressional mandates in H.R. 1 (Public Law 110-053), implementing the recommendations of the 9/11 Commission, which requires TSA to enhance security by properly identifying authorized airline flight deck and cabin crew members at screening checkpoints, granting them expedited access through screening checkpoints and to integrate biometric identifiers into airport security access control systems.

Next gen IC chip will be faster, more functional

Shawn Rogers, director of secure RF products Texas Instruments, says the next generation contactless smart card chip will be faster, have greater memory and use less power. Rogers made the comments during the Future of Secure Documents 20008 conference in Chicago Sept. 8 through Sept. 10.

They also won't cost any more than then integrated circuit chips available now. "If you're walking into an existing market you have to deal with the price constraints already in place," he says.

The need for greater memory and speed is necessary as more electronic passports are used at border crossings. U.S. Department of Homeland Security Sec. Michael Chertoff says he wants the passports to be read in loess than five seconds.

Now it takes five to eight seconds for the transaction to be processed with passports using basic access control and eight to 14 seconds for passports with extended access control. That might not seem like a lot of time, but it can add up when hundreds of people are in a line waiting to get past a customer checkpoint.

Texas Instruments is working on next generation technology that will increase the speed and functionality, Rogers says. The newer chips will use 16-bit microcontrollers while current chips use 8-bit processors.

There's also a new type of memory that Texas Instruments is working with: FRAM – Ferroelectric Random Access Memory. Chips using this type of memory can write 1,000 times faster than traditional EEPROM memory and read three times faster. They technology also sues less power, 1.5 volts compared to 10 to 14 volts for EEPROM.

Rogers says these new chips should be available in 2009.

Dynamic Biometric Systems launches distance learning authentication solution

Nevada-based Dynamic Biometric Systems has introduced a series of student authentication products based on its Bio-Pen hardware solution to help schools comply with the recently-passed Higher Education Opportunity Act, which requires educational institutions offering distance learning courses to be able to verify that students who receive credits actually do the class work and take the exams.

The Bio-Pen hardware combined with the Dynamic Signature software and Private Lock Infrastructure application enables the educational institution's software to periodically require that students verify that they are actually in attendance for required classes and that they are the person taking tests or submitting other relevant information or class work.

Verification is accomplished by simply signing his name using the Bio-Pen. Since the verification can be random, and/or the administrator can require an immediate response to signature requests, the student must be present and able to provide the requested authentication.

One Bio-Pen benefit is that the student's personal data is still kept private. Only the student knows how he signs his name, or secret phrase, and because of the nature of behavioral biometrics, only the student will be able to sign the signature or phrase using the same motions that the student used when registering.

No training is necessary to implement the DynaSig verification system. If the student can write, the student can use a Bio-Pen. A Bio-Pen can plug into any computer using a USB port. The student only has to register and be

verified by the school once during enrollment. After that, his biometric template is in the system to be utilized for future verifications.

RFID technology encourages healthy lifestyle among children

Freiker Inc., a bike-to-school program based in Boulder, Colo., received a grant from Trek Bicycle Corporation to help fund its Frequent Biker program among area elementary schools.

The program was founded to encourage children to ride bikes to and from school by tracking their progress and rewarding them based on the number of times they rode their bikes to school. Rides are tracked using RFID tags mounted to the riders bike helmets and are read by RFID sensors placed near the school grounds. Their progress is wirelessly uploaded to the Freiker Web site, where participants can go to track progress towards their riding goals.

The program has been implemented at five Boulder area schools and has expanded to Madison, Wis. and Bend, Ore. In addition to promoting exercise among children, it also encourages safety, since the tags must be adhered to bike helmets in order to be registered in the program.

Japanese hotels moving to unmanned check-in processes

A new project to develop unmanned hotels in Japan may soon eliminate front desk check-ins.

A consortium of five companies, including the trading company Itochu and consumer credit provider Orico, are working to develop a network of hotels that rely on an online reservation and payment system. The contactless smart card-enabled Orico credit cards will serve as keys, and contactless-enabled door entry locks.

When hotel guests reserve a room online with their credit card, a "key" is assigned to the card. Since the credit card is the key, guests can bypass the check-in process and proceed directly to the room at the allotted time. The door lock recognizes the IC chip embedded in the credit card, opening for the guest upon arrival. The system eliminates the need for front desk staff to remain on duty.

Other companies involved in the project are Kesaka System, who are developing the entry locks, as well as Espace Construction and Miyabi Estex, who are handling construction and development.

Japanese law requires hotels to maintain staffed front desks, so the unmanned hotels will not be completely staff-free. However, the hotels are expected to require only half the ordinary number of personnel. A dozen or so of these hotels are scheduled to begin operations nationwide in 2008.

New York City student ID cards work at 50-plus restaurants

Students attending the New York-based Laboratory Institute of Merchandising, the College for the Business of Fashion, can now use their ID cards at more than 50 restaurants throughout the city thanks to a program implemented by Off-Campus Integration, a company designed to help colleges expand their preexisting card programs to include off-campus capabilities.

Off-Campus Integration, headquartered in New York City, was founded in 1994 at the University of Massachusetts and currently serves more than 50 institutions nationwide.

"When we received a call from LIM asking us to employ technology that is generally used for campuses with more than 25,000 students, we jumped at the opportunity and challenge to employ the same technology, with the same features, at a college with approximately 1,300 students," says Michael S. Hauke, President of OCI. "We set up the system last year and have seen our numbers double not only with LIM, but also with other New York City students."

Not leaving any students behind, OCI also offers the Off-Campus Meal Plan or OCMP card for students who live in New York City but do not go to LIM.

"We wanted to roll out our OCMP card in New York City because there was a growing demand for meal plans. LIM is one of many colleges in New York City that do not have facilities to provide students with a cafeteria-style meal plan. We have hundreds of students on the OCMP program that are here for a semester abroad, taking summer session courses, or going to other schools which do not provide cafeteria-style dining facilities, or that use OCMP as a supplement to their on-campus meal plan," said David Diana, CEO of OCI.

IDetect introduces low-cost handheld ID verification scanner

Saint James, N.Y.-based IDetect has released a new age verification scanner ideal for use on college campuses. The portable, ruggedized IDetect LITE ID Scanner can also scan driver licenses and corporate IDs.

While it can scan 3D bar codes and magnetic stripe IDs, if the license or ID can't be scanned, IDetect will take a picture of the license which can help bar owners or liquor store operators avoid fines or license revocations.

Automatically upon an identification scan, the entrant's picture is taken and saved with entry information. The picture can be used to locate any individual in seconds. IDetect's exclusive license picture function also takes a picture of an ID that is not able to be scanned.

This feature, coupled with the automatic picture of the entrant, and the IDetect ID scanner's time and date stamp history feature, is a strong defense and proof of diligence against fines and state authority investigations. IDetect's License Scanners also flag an ID that is fake, tampered with, shared with another entrant, or banned for any reason, all in less than a second.

IDetect ID Validation Systems have been utilized for more than 15 years in night clubs, universities, casinos, military bases, office buildings, rental car agencies, festivals, banks and liquor stores throughout the United States, Canada and Mexico.

California's community colleges select Blackboard for mass-notification service

California's 110 community colleges now have the ability to instantly communicate with its 2.6 million students via the Connect-ED multi-modal mass notification service from Blackboard Inc., a provider of educational enterprise technology.

Under the agreement, Blackboard has provided a special pricing structure to members of the Foundation for California Community Colleges that will provide them with the technology to quickly reach its students, faculty and staff, with time-sensitive information.

Recently, Blackboard announced a similar agreement with the Oregon University System to make the Connect-ED service available to any public or private campus in the state, including community colleges.

Blackboard's Connect-ED mass notification service supports enrollment management, time-sensitive notification, and campus outreach efforts through a direct communication channel with students.

Built exclusively for post-secondary institutions, the Connect-ED service enables campus leaders to schedule, send, and track personalized voice messages at up to six phone numbers, two e-mail addresses and one text address per student and staff member.

2008	2009
NOVEMBER	**JANUARY**
NACAS 40th Annual Conference November 2 – 5, 2008 Hyatt Regency Chicago; Chicago, Illinois	**RFID in Health Care 2009** January 22, 2009 Rio All-Suite Hotel & Casino; Las Vegas, NV
CARTES & IDentification 2008 November 4 – 6, 2008 Paris-Nord Villepinte Expo Ctr.; Paris, France	**MARCH**
Active RFID, RTLS & Sensor Networks November 5 – 6, 2008 Dallas, Texas	**16th Annual NACCU Conference** March 8 – 11, 2009 Disney's Coronado Springs Resort; Orlando, FL
ID WORLD Intl Congress 2008 November 18 – 20 2008 Milanofiori Congress Center; Milan, Italy	**APRIL** **ISC West 2009** April 1 – 3, 2009 Sands Expo & Convention Ctr.; Las Vegas, NV
Maritime Security Expo November 18 – 19, 2008 Long Beach Convention Ctr.; Long Beach, CA	**Expo Seguridad México** April 21 – 23, 2009 Centro Banamex; Mexico City, Mexico
Building Tech Americas 2008 November 19 – 20, 2008 Hotel Crowne Plaza; Bogotá, Colombia	**ASIS Intl European Security Conference** April 26 – 29, 2009 Montreux, Switzerland
Voice Biometrics Conference London November 19 – 20, 2008 Hilton London Tower Bridge; London, UK	**RFID Journal LIVE! 2009** April 27 – 29, 2009 Disney's Swan and Dolphin; Orlando, FL
Mobile & NFC Payment Strategies November 24 – 27, 2008 Corinthia Grand Hotel; Budapest, Hungary	**MAY** **CTST 2009** May 4 – 7, 2009 Ernest Morial Convention Ctr.; New Orleans, LA
DECEMBER	**JUNE**
RFID Journal LIVE! Canada 2008 December 1 – 3, 2008 Toronto Congress Centre; Toronto, Ontario	**RFID Smart Labels USA 2009** June 9 – 10, 2009 San Francisco, California

The next generation electronic passport

Inspection systems and extended access control are next hurdles

Zack Martin
Editor, AVISIAN Publications

More than 100 million electronic passports have been issued in the two plus years since governments initiated production of the new travel credentials. The U.S. State Department alone has issued almost 15 million of the contactless documents.

But while there are many e-passports in circulation the inspection systems used to read them have not been widely deployed at border crossings. Putting these systems in place, while not adversely impacting wait times, will be the next challenge for countries.

European Union countries have that and another obstacle to hurdle as well: extended access control (EAC). Since EU countries are storing fingerprint images on e-passports they are using the more advanced security of EAC, a public key infrastructure scheme that secures the biometric data. EU countries are supposed to start issuing passports with EAC by next June.

Even the U.S., the initiator of the move to e-passports after the terrorist attacks of Sept. 11, hasn't deployed many inspection systems. The U.S. Department of Homeland Security's Customs and Border Protection (CBP) has requested funding for 5,000 e-passport readers to deploy at 372 air, sea and land border entry points, said Warren Burr, director of the fraudulent document analysis unit at Customs and Border Protection. The new readers would replace the current devices that just read the machine readable zone on the passport.

But so far only 500 of the readers have been purchased and less than half of those, just 247, have been installed, Burr said. The concern is that using the new scanners will adversely impact wait times.

The readers in the field are at the 33 U.S. international airports, which covers 97% of visa waiver country travelers entering the country, Burr says. CBP is analyzing how to deploy e-passport readers to all border entries and assess how it will impact wait times. Burr made these comments at the Future of Secure Document 2008 conference in Chicago.

There are concerns around how long it will take to process travelers with the e-passports. With the older documents customs officials would swipe the machine readable zone, check a few other items in the book and ask the traveler some questions.

E-passports require a little bit of extra finesse, says R. Michael Holly, director of international affairs for passports with the U.S. State Department. "They need to get the inspectors prepared and familiar with how to deal with the new documents," he says. "They have to deploy full page scanners and you need to let them sit awhile so the data can be accessed."

The State Department is working on getting sample e-passports to border officials so they

can test the systems and train officers, Holly says. When the U.S. introduced e-passports they also changed some of the physical security in the book as well and officers need to be able to spot the different features.

Already, use of the new documents is rising rapidly. Between Oct. 1 and Dec. 31, 2006 Customs and Border Protection scanned 165,921 electronic passports, Burr said. In all of 2007 1.4 million were checked and in the first half of 2008 CBP officers had scanned more than 1 million e-passports.

Inspection challenges trump issuance challenges

But the challenge to deploy these inspection systems is what most countries are facing. The change was evident in September at the E-Passport EAC Conformity and Interoperability Tests in Prague, says Mike Bond, security director at Cryptomathic. "The guys from the inspection side outnumbered the guys on the issuing side," he said. "Their money has been spent and the project is done, now it's time for the border control guys to come in."

The European border control officials have quite the task in front of them. Extended access control is a PKI scheme that secures biometric data on e-passports. EU countries decided to store fingerprint and iris biometrics on the passports as well as the photo and other data. This biometric information is stored as images, not templates, so countries want to take extra steps to make sure the data is protected.

In order to view the biometric on the passport and match it with the traveler the other country will have to have the proper PKI certificate so the data can be unlocked. Vendors and border officials are still trying to figure out how these certificates will be exchanged and read while also making sure that systems from different vendors are interoperable.

While EU countries have to start issuing e-passports with EAC by next June there is no deadline to actually read the biometric data from the passports, Bond says. "With regards to inspecting we're 18 months away from starting pilots. The UK was talking about initial inspection by the end of 2009, scanning the full biometrics of some people, but only about 1% of travelers, and moving to 30% by 2016."

There are numerous reasons for the seemingly long timeline. First and foremost, governments don't know how it will work. This was a reason for the Prague conference in September.

The purpose of the test was to enable European countries to verify the conformity of e-passports using EAC and fingerprint biometric data. A related target is verification of the cross-over interoperability of different EAC inspection systems and e-passports. In addition countries attempted to verify interoperability of EAC PKI infrastructure for national border inspection systems, including official exchange of EAC certificates.

The tests went well, but were not without issues. "Overall results are that not all passports worked with all readers," says Neville Pattinson, director of government affairs and marketing, identity and security at Gemalto.

Four of the countries participated in a test that put in place a fully-operational PKI infrastructure, says Tim Moses, director of advanced security technology at Entrust, one of the participants. Entrust is supplying the PKI infrastructure to the UK and Slovenia.

Considering it was the first time the infrastructure was checked, the test was pretty successful, Moses says. "There were a few minor issues on the certificate exchange but we resolved them." Full results from the conference are not expected until December and another test will be scheduled before the June 2009 deadline.

Moses emphasized that countries are going to have to work to make sure EAC is done properly. "The EAC environment requires a lot of interaction among countries," he says. "The PKI system must be built to manage the trust; it's not just a set of tools."

Added security likely to add further delays at inspection points

One of the larger issues with EAC is the time it's going to take to process travelers. Pattinson says it can take anywhere from two to 15 seconds for the information to transmit.

Cryptomathic has released a new product it claims will accelerate the speed of inspecting electronic passports by a factor of four. The product uses a different type of caching mechanism, a storage area that holds an encrypted version of the e-passport biometric data.

When the e-passport has its initial contact with the border control station, the biometric data is transferred from the chip into the inspection system, and at the same time a unique key is calculated from the e-passport chip which is used to encrypt the stored data.

The storage key is then deleted from the memory of the border control system to make it impossible to retrieve the stored data. In order to recreate the decryption key for the record and view the biometric data, the original e-passport document must be connected to the inspection system.

Long lines at border control points is the fear when countries start deploying inspection technologies for e-passports, Bond says. He saw one presentation at the Prague conference that said wait times at some busy airports during peak times could be as long as 90 minutes.

And some countries are making the problem worse because they're not standardizing the biometric, Bond says. For example, most EU countries are storing the index fingerprint images on the passport, regardless of the quality of those fingerprints. But Germany is taking the two best quality fingerprints from passport applicants; it may be the index, but it also may be the thumbs.

This may lead to slow-downs at border crossings. German travelers won't remember what fingerprint image is stored in the book or a border control agent may be asking for the index when he needs the thumb. "When the delays start to happen they'll either pull the plug or soldier on," Bond says. He expects a few false starts. Countries will roll out systems and then roll them back and reconfigure as problems arise.

One solution that could potentially alleviate wait times are self-serve kiosks, says Gemalto's Pattinson. (See Global Entry story, page 21) "The consequence of EAC is more automated kiosks for border control," he says. "Have the document authenticated by the kiosk instead of manual inspection."

While the focus shifts from issuing e-passports to inspecting them, lines at international border checkpoints may be interesting over the next couple of years as travelers and officials get used to the new documents.

Future of the U.S. passport

The U.S. may have been the driver behind electronic passports, but officials have no plans to use the new, more secure extended access control on the travel documents, says R. Michael Holly, director of international affairs for passports with the U.S. State Department. "We don't envision using another biometric for e-passport issuance," he says.

The U.S. does use basic access control with its e-passports, Holly says. In order to read the data stored on the chip the machine readable zone on the data page must be swiped first. The front cover and spine of the U.S. book also has a metallic paint, which creates a faraday cage, which prevents unauthorized reading of the chip.

But there are other plans for the travel documents, Holly says. He doesn't expect needing more memory, but hopes the processing power of the chips improves to speed up transactions and he may look for greater security as well.

There are other items being considered, Holly says. Multifunction chips that enable a third-party to write to a secure portion of the chip are being looked at. This would enable countries to issue visas electronically instead of on paper.

There's also the possibility of using multiple chip schemes in the U.S. passport. For example, the State Department started issuing the Pass Card this summer, which used long-range RFID technology for land and sea border crossings.

"We're thinking about using both technologies in one travel document so our customers could use the book for international travel and at land borders," Holly says. "It's just something we're punching around." E-passports can still be used at land border crossings, the books just can't take advantage of the expedited crossing.

Any modifications to the chips used in U.S. e-passports would likely occur at the point when current contracts expire. Gemalto and Infineon currently supply the microprocessor chips to the State Department and U.S. Government Printing Office, the agency that actually prints the books. These contracts expire in 2010 and 2011.

There are also changes to the physical security of the e-passport, says Keith Bruce, document design officer for e-passport services at the State Department. Future versions of the document are going to use laser perforation that produces a hole by burning through the paper. "You can have different diameter holes that look very different and unique and would be difficult to counterfeit," he says.

Self-service kiosks expedite e-passport processes

One concern the public has about electronic passports is knowing what information is stored on the chip. Governments tell citizens what information is stored on the chip, but unless the document holder can actually see it he's never really sure.

To try and combat this problem the UK Identity and Passport Service agency has deployed kiosks that enable e-passport holders to view the data stored on the chip. The agency tapped Minnetonka, Minn.-based DataCard Group for the project.

The Datacard e-passport reader kiosk uses an intuitive graphical interface that requires no language skills or data entry. It automatically senses the presence of an e-passport and displays chip data and the facial image on the screen, which is cleared when the passport is removed.

It is designed for unattended public use and has a patent pending on the method of integrating electronic IDs and e-passport machine-readable zone capabilities in a single device.

The kiosks also are fitted with privacy filters, which black out views on either side of the monitor without blurring or distortion. The filters comply with Data Protection Laws and the kiosks themselves meet all requirements of the UK Disability Discrimination Act.

Norway is using kiosks too, but they are being used to enroll citizens. Motorola has been chosen to supply the enrollment kiosks to the Norwegian Ministry of Foreign Affairs and the National Police Computing and Material Service for Norway's biometric passport and visa program.

The kiosks from Motorola, called Bio-Enrol Stations, will enable Norway's agencies to enroll the 500,000 passport applicants and 150,000 visa applicants they receive annually. The kiosks they have been designed to enable people, regardless of language fluency and literacy level, to easily navigate the system via pictograms.

The contract with Motorola follows a successful trial of the technology that saw eleven kiosks setup in Norway with another five in embassies abroad. The implementation of the stations began this month and is expected to be finished by June 2009.

E-passport kiosks from a variety of vendors are helping countries to expedite service delivery – from enrollment to verification. Pictured here is a device from Datacard (left) and Motorola (right).

Are e-passports vulnerable to forgery?

Tim Moses
Director of Advanced Security, Entrust Inc.

In July the TimesOnLine reported a demonstration by a security expert that the integrity of electronic passport systems around the world were compromised. "Potentially devastating" is how the report described the announcement.

The article strongly implied that there is a flaw in the passport readers used at ports of entry around the world that will enable terrorists to impersonate genuine passport holders and thereby travel freely to any country.

When researchers discover security vulnerabilities there typically is a standard protocol for handling these situations: responsible disclosure. When a security expert discovers a flaw in a product that can be unsafe for its users, he provides the supplier of the product with the necessary details to develop a fix. Provided the supplier cooperates, only once the fix has been made available will the expert publish the details of his or her discovery. Those details have to be sufficiently complete that other suppliers can identify similar problems in their own products and the same mistake can be avoided in future products.

The product containing the supposed flaw in this story is the Golden Reader tool, which is software designed to be used with a contactless smart card readers for reading the contents of e-passports. It was developed in 2004 under contract to the German Federal Office for Information Security (BSI) and it has been used in several international interoperability trials. It is considered the functional reference implementation for communications between e-passports and readers.

No patch was announced for the Golden Reader tool in the days or weeks leading up to the TimesOnLine article. So, either the security expert is not following the responsible disclosure protocol or the consequences aren't "potentially devastating" after all.

The report vaguely describes how the security expert programmed an uncommitted contactless smart card chip with the biographical data of a genuine passport holder and the biometric data of an impostor, signed – not by the UK Identity and Passport Service – by the security expert himself.

It goes on to describe how the Golden Reader tool apparently accepted the bogus document as genuine. If this is true, then there is a problem with the software in that it was either designed, configured or operated to bypass one of the most elementary safeguards in any system based on digital signatures: verifying the chain of credentials from the signatory to a priori source of trust.

The principal victim of this type of attack is the accepting country itself. So, it's hard to imagine why, in an operational setting, such an elementary step would be missed.

The Golden Reader tool is not in widespread use at ports of entry around the world. It is a functional reference implementation. Its purpose is to help ensure that the products that actually are, and will be, deployed by governments for reading passports will work with all the passports that they may encounter.

The passports in question are first-generation e-passports, also know as "Basic Access Control" (BAC) passports. They offer their holders protection against unauthorized viewing and eavesdropping, or skimming, and they offer accepting countries protection against forgery.

The second generation of e-passports, known as Extended Access Control (EAC) passports, will extend the protection for accepting countries to include impersonation attacks, through the use of advanced biometrics, and the protections for passport holders will be extended to cover misuse of their biometric data.

Unlike first-generation e-passports, second-generation e-passports will include a private key that cannot be read out through the RF Interface. The passport must be able to prove that it knows its own particular private key without revealing it.

This is how forgery and cloning attacks can be overcome in the upcoming technology.

While it may be possible to program an uncommitted chip with the desired biographical and biometric data, it will not be possible to convince a passport reader that it knows the private key that has been authorized by the appropriate issuing authority.

EU regulation No 2252/2004 requires member states to start issuing second-generation passports by mid 2009.

So, what can we learn from this report? First of all, it is possible to implement, configure or operate a perfectly sound security solution in such a way that its safeguards are ineffective. That isn't news.

Secondly, first-generation e-passports, if used as they were designed to be used, offer protection against forgery. They may not be impervious to all forms of attack. Second-generation e-passports will contain a number of features that address a broader range of threats.

And finally, I see no good reasons to deviate from the well-accepted protocols of responsible disclosure. If the development is actually newsworthy, then there is all the more reason for adhering to the protocol. If it isn't newsworthy, then let's not try to sensationalize it.

International trusted traveler program ramps up

Standing in long lines at customs and border checkpoints is a hassle, especially after sitting on an airplane for what was most likely half a day.

The U.S. Department of Homeland Security and its Customs and Border Protection agency are trying to alleviate the wait times for some of those travelers with the Global Entry Trusted Traveler Program, says John Wagner, director of the program at DHS. The program is based on the Nexus and Sentri programs that expedited U.S. and Canadian citizens border crossings. "It's a risk management approach to process frequent, low-risk international travelers," he says.

The program, still a pilot, is in place at Los Angeles International, Hartsfield-Jackson Atlanta International, Chicago O'Hare International, Miami International, George Bush Intercontinental Airport in Houston, John F. Kennedy International Airport in New York and Washington Dulles International Airport.

The eventual hope is to roll it out to all international airports and have reciprocity so U.S. citizens can participate in similar programs with other countries, Wagner says. Agreements have already been signed with the UK and the Netherlands with others in the pipeline. "Both countries do the vetting on their citizens," he says.

Travelers interested in the program undergo a voluntary background check, Wagner says. It begins by filling out an online application and paying a $100 fee, which is good for five-years' enrollment in the program. The application seeks basic demographic data and asks questions about past international travel.

At that point the individual's information will be checked and after a couple of weeks he will be conditionally approved or denied, Wagner says.

Change to domestic registered traveler on the horizon

While the international trusted traveler program may be lifting off, there are questions surrounding the domestic registered traveler program in the U.S.

The U.S. Transportation Security Administration announced that is was eliminating the $28 screening fee associated with the program. The TSA felt that it was redundant and no different from the TSA watch list checks already performed daily at airports around the country.

The elimination of the fee has made some observers question the security value of the program. "If a background check isn't performed what makes this a security program?" asks one Washington-based security advisor.

There may be changes coming to the cards that participants use as well. Clear, the largest registered traveler program, issues a card that includes the contact smart chip and the cardholder's name.

But RT operators may have to start issuing a card that includes a photo and other information to comply with the physical security guidelines outlined in the Real ID Act, the law calling for stricter identity vetting for state driver licenses. The background check that individuals undergo may also be similar to that called for in Real ID.

The TSA shut down Clear registration at one point in late summer after a laptop containing personal information for 33,000 customers was stolen from a locked office at San Francisco International Airport.

The information on the stolen laptop included applicant names, addresses and birth dates. The computer also contained driver license numbers, passport numbers and alien registration card numbers for but no credit card information, Social Security numbers or biometric information. The company said two levels of password protection secured the information.

Registration was halted while encryption software was installed on all computers and the customers whose information was stolen were notified of the theft.

The RT program also had issues in the Washington area. Clear CEO Steve Brill refused to guarantee that members of its rival provider FLO would be able to use the registered traveler gates at Reagan National and Dulles International airports.

FLO announced that it had partnered with the Washington Redskins to offer expedited entry into FedExField as well as touting the registered traveler program at the Washington-area airports.

Clear runs the registered traveler gates at Regan and Dulles airports. Brill said it isn't fair that FLO members have been able to use the company's lanes, which are two-thirds of the company's operating costs, free of charge, according to news reports.

Brill told news agencies that it might block FLO users if they don't start paying for its members to use the Clear lanes. The company runs the lanes at 17 of the 19 airports. Luke Thomas, executive vice president of FLO, said if that happens Clear members won't be able to use the FLO lanes at Reno-Tahoe International Airport.

This is most likely the first volley in what is going to be a competition that is just heating up. The TSA has lifted the cap that limited the fast lanes to 20 airports and said registered traveler operators, like FLO and Clear, must remain open to all operators for the next 12 months. After that it's anybody's game.

If approved the traveler will have to go to an enrollment center, which is typically located at his home airport, Wagner says. The applicant will have his fingerprints taken, passport scanned and be interviewed by a Customs and Border Protection official.

If everything checks out the individual is typically approved on site and his registration in the program is completed. The traveler is then shown how the kiosk will work when reentering the country.

From there, whenever the traveler is coming back to the U.S. he can use the kiosk, which is similar to an ATM or airline self-check in kiosk, Wagner says.

The traveler confirms enrollment by scanning his passport and authenticating with a previously enrolled fingerprint biometric. A camera on the kiosk then takes the traveler's picture and he fills out the declaration on the screen.

While the traveler is answering these questions the system is running queries in the background to confirm airline and other information. Once successfully processed the traveler can claim his bags as he leaves the airport.

Using the kiosk takes about two minutes, compared to the three minutes it takes a customs official to check a traveler through, Wagner says. But the more significant time savings comes from not having to wait in line to see the officer.

The traveler can use either an old passport or a new electronic passport with the program, as long as it has the machine-readable zone on the data page, Wagner says.

Global Entry is still in pilot but Customs and Border Protection wants to deploy it at all international airports. "Our target audience is people who travel internationally four or five times a year," Wagner says. "At three of our pilot sites about 140,000 people fit into that category and ideally we would like to get 75% of those."

As of late September, 3,500 travelers have enrolled in Global Entry and more than 1,100 members have used kiosks at the three existing pilot locations since the June 10 opening date.

To drive membership in the program Wagner is working with the airports and airlines to get the word out. This includes ads in trade publications, some airlines marketing it to their members and signage at the airport, Wagner says.

But the best message may be when travelers are waiting in line to see a customs official and they see others using the kiosks and getting on the way much quicker.

ID

How the global supply chain can benefit from biometric technologies

James M. Anzalone
Compliance Assurance LLC

Supply chain security is a term that was practically unheard of prior to the terrorist attacks of September 11, 2001. Since then, numerous initiatives have been launched both in the U.S. and abroad to secure the global supply chain – that is, the logistics, cargo and transportation systems – against threats of terrorism, pilferage and piracy.

Globalization has significantly proliferated the links and nodes in the supply chain including shipping points, consolidation points, surface and air transportation carriers, agents, brokers and distribution facilities. Each of these opens an opportunity for a security breakdown. The aim of supply chain security initiatives is to plug these holes and create an integrated and secure process. The global supply chain stands to benefit greatly from the adoption of biometric technologies such as fingerprint, iris and similar technologies that provide the security necessary to secure people, property and information at international borders.

Supply chain security activities typically include background checking and credentialing individuals with access to the supply chain; screening and validating cargo being shipped; sending advance notification of shipment information to the destination country; ensuring the security of the cargo in-transit; and inspecting cargo upon arrival at destination. Each of these activities requires people to perform particular tasks. Therefore, the securing of the people component is the first priority in securing the supply chain.

In November of 2007, ABC News reported that federal authorities arrested more than 20 people, all believed to be illegal immigrants, after agents found they were allegedly using fake and expired security badges that allowed them unlimited access to commercial aircraft at Chicago's O'Hare International Airport. This serious violation could have been prevented if the workers were properly screened, credentialed and verified using biometric access devices such as fingerprint readers.

While federal law requires fingerprint and background checks for workers with access to secure areas of the airport, such checks could be incorporated into all links in the supply chain including loading, warehousing and transportation.

Screening and validating the cargo being shipped involves screening both the shipper and the physical goods. The Transportation Security Administration has established the Known Shipper Program whereby passenger and indirect air carriers are required to vet individuals and companies tendering cargo to an airline, with the goal of eliminating anonymous shipments aboard passenger aircraft. While this program relies

upon the air carrier's check of the shipper's name, physical location and other factors to verify a shipper's identity, the program does not guarantee that an individual has provided tamperproof identification or valid documentation. A background check including a criminal history fingerprint check would help prevent the use of fraudulent identification in the process of vetting known shippers.

The remaining elements of the secure supply chain involve the use of computerized systems to book, manifest and screen cargo for communication to government agencies, forwarders, brokers and others on the destination side of the shipment. Unauthorized access to such data is a critical security risk as potential terrorists could easily alter information about a potentially sensitive shipment. In addition to physical security, secure supply chain initiatives require a high level of information security.

Many companies and government organizations are already using biometric devices in addition to the usual user ID and password to gain access to computer systems. This is a significant opportunity for the players in the global supply chain to secure the transaction data for the millions of shipments crossing international borders each day using proven biometric technologies.

What are the specific opportunities for the use of biometrics in the global supply chain?

There are numerous initiatives both in the U.S. and abroad, some of which have been in place for several years. For example, the TSA requires a security threat assessment and fingerprint-based criminal history records check that ensures that anyone with access to airport cargo areas do not have a disqualifying criminal offense. Since then, numerous other security initiatives have come into being for other modes of transport as well as other links in the supply chain. These programs include:

- Transportation Worker Identification Credential,
- Certified Cargo Screening Program (CCSP),
- Customs and Trade Partnership Against Terrorism (C-TPAT),
- Authorized Economic Operator and the World Customs Organization (WCO) SAFE program,
- International Ship and Port Facility Security Code (ISPS),
- International Organization for Standardization (ISO 28000:2007).

The following are brief summaries of these programs with links to the official websites and justification as to how the use of biometric technologies can benefit each program.

U.S. Programs

The Transportation Worker Identification Credential is a mandatory program administered by the TSA and U.S. Coast Guard. TWIC enrollees must provide biographic and biometric information and pass a security threat assessment conducted by the TSA. The resulting TWIC cards are tamper-resistant biometric credentials that will be issued to workers who require unescorted access to secure areas of

ports, vessels, and facilities. It is anticipated that more than 1 million workers including longshoremen, truckers, and port employees will be required to obtain a TWIC by the end of 2009. As of late September more than 335,000 credentials have been issued.

TSA's TWIC Web site can be found at *www.tsa.gov/what_we_do/layers/twic/index.shtm*.

The Certified Cargo Screening Program (CCSP) is a new voluntary program under which the TSA will certify facilities to screen cargo before it is tendered to aircraft operators for carriage on passenger aircraft. The program, expected to be deployed in 2009, will enable the TSA to meet the 100% cargo screening requirement by 2010 as mandated by the 9/11 Act.

Under the CCSP, facilities upstream in the air cargo supply chain such as shippers, manufacturers, warehouses, and third party logistics providers may apply to the TSA to become certified cargo screening facilities (CCSFs). CCSF employees and authorized representatives will be required to successfully undergo TSA-conducted security threat assessments which include background checks using biometric technologies.

Before being certified, the CCSF will be required to undergo examination by a TSA-approved validator. The secure facilities will also be subject to random inspections by TSA cargo inspectors to ensure their adherence to CCSP requirements. For the latest information on the CCSP, visit the TSA Web site at *www.tsa.gov/press/happenings/air_cargo_screening.shtm*.

Customs and Trade Partnership Against Terrorism (C-TPAT) is an existing voluntary government-business program established in 2001 by the U.S. Department of Homeland Security's Customs and Border Protection in an effort to address the threat of a terrorist attack on the global supply chain. C-TPAT establishes minimum-security criteria which vary depending upon whether the participant is an importer, broker, forwarder, carrier or foreign manufacturer.

In general, all applicants require security to be documented and validated in the following areas: business partner requirements, container security, container inspection, physical access controls, personnel security and information technology. The use of biometric technologies for background checks and physical and information security are not required for C-TPAT but such technology is ideal for meeting these security objectives.

For more information, visit the CBP C-TPAT Web site at *www.cbp.gov/xp/cgov/trade/cargo_security/ctpat/*.

International programs

The World Customs Organization (WCO) members have developed a framework of international standards to secure and facilitate global trade or "SAFE" program which establishes minimum-security criteria for WCO members. Like U.S.-based programs, SAFE seeks to employ a layered, risk-based approach to address security threats.

The program enables manufacturers, importers, exporters, carriers, warehouses and the like to become Authorized Economic Operators (AEOs) by adopting strict security assurances with respect to their role in the supply chain. Like C-TPAT, the SAFE criteria addresses measures to prevent unusual or undocumented goods entering the global supply chain; physical security of facilities used as loading or warehousing sites; security of containers and cargo; personnel vetting; and protection of information systems. Each of these criteria can be most effectively secured through the use of biometric security devices to verify backgrounds and identity and secure access and information systems.

The WCO has detailed information about the SAFE program on its Web site at *www.wcoomd.org/home.htm*.

Put into effect in 2004, the International Ship and Port Facility Security Code (ISPS) is part of the International Maritime Organization (IMO) and provides a common international framework with which to assess security vulnerabilities and threats, implement security measures, and facilitate international cooperation between the contracting governments of the Safety of Life at Sea Convention. Requirements of the ISPS include a ship security assessment, security plan, and designation of a security officer, recordkeeping, training and verification. Guidelines for carrying out the ISPS elements are voluntary but state which measures should be carried out at various levels of security threat. The ISPS program is a broad opportunity for the utilization of biometrics applications to improve security in the maritime industry.

For more information visit the IMO Web site at *www.imo.org/*.

The International Organization for Standardization (ISO) has released a set of security standards in ISO 28000:2007 which specify the requirements for a security management system, including those aspects important to ensure supply chain security including manufacturing, transportation and warehousing.

Like other ISO standards, ISO 28000:2007 seeks to assure conformance with stated management policies, demonstrate such conformance to others, make a self-determination or seek certification/registration of its security management system by an accredited third party certification body. This adoption of ISO 28000:2007 may create the most significant opportunities for the use of biometrics due to the widespread global adoption of ISO standards.

Visit the ISO Website for ISO 28000:2007 at *www.iso.org/iso/catalogue_detail?csnumber=44641* for more information on this set of international standards.

Addressing individuals and countries' security is shifting some from troops, tanks and guns to civilians, ships and commercial aircraft. More importantly, responsibility for addressing global security threats is shifting from governments to individuals and businesses.

Many of the supply chain security programs currently in place are voluntary but it is not likely that they will become mandatory if the global threat of terrorism continues to escalate. Biometric technologies, once a tool primarily for law enforcement, have become key to ensuring the security of individuals, property and information. The use of biometric technology to reinforce supply chain security is in its infancy and the near-term opportunities to benefit the global supply chain are as numerous as the number of links and nodes in the chain.

James Anzalone is the president of Compliance Assurance LLC, a firm specializing in global trade compliance solutions.

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

DOD secures document scanning with smart cards

Using smart cards to secure computer login, emails, encrypt files and access networks is becoming commonplace. But a serious hole exists in the network security if output such as scanning and printing is not secured as well.

"It's the weakest link in terms of security," says Enrique Barkey, worldwide director of the public sector at Hewlett-Packard Development Company, Palo Alto, Calif.

This fact, coupled with the U.S. Department of Defense wanting a way to better secure its multi-function printers, led the printing giant and Fremont, Calif.-based ActivIdentity Inc. to come up with a solution that enabled the Common Access Card to be used to authenticate individuals before they could scan documents. Eventually the products also may be used to authenticate individuals before they print documents as well.

Barkey says the DOD approached HP to come up with a solution to the problem. HP then approached ActivIdentity to provide the middleware. ActivIdentity has provided middleware for the Common Access Card from the start of the program.

Now when a CAC cardholder wants to scan a document to either email or have as a file they must be authenticated first, says Simon Wakely, vice president of business development at ActivIdentity. The employee places the document on the device and hits the scan button. The multi-function printer would then ask for the employees' CAC and PIN.

The digital certificate stored on the card is checked and verified and if the certificate is good he can proceed with the scan, Wakely says. The scanned document can either be emailed to someone or saved in a folder on a server to be accessed later.

The DOD is considering the addition of secure printing in the future, Wakely says. Before an individual would be allowed to print a document he would have to authenticate with the credential as well.

Private sector implications too

While this application was born out of the public sector, HP and ActivIdentity say it has implications for the private sector as well. "We're seeing many large global entities deploy smart cards," Wakely says.

Printers and scanners are often the most overlooked devices when it comes to security, says HP's Barkey. "HP has invested a lot of money and resources around this, not just around the authorization, but other capabilities as well," he says

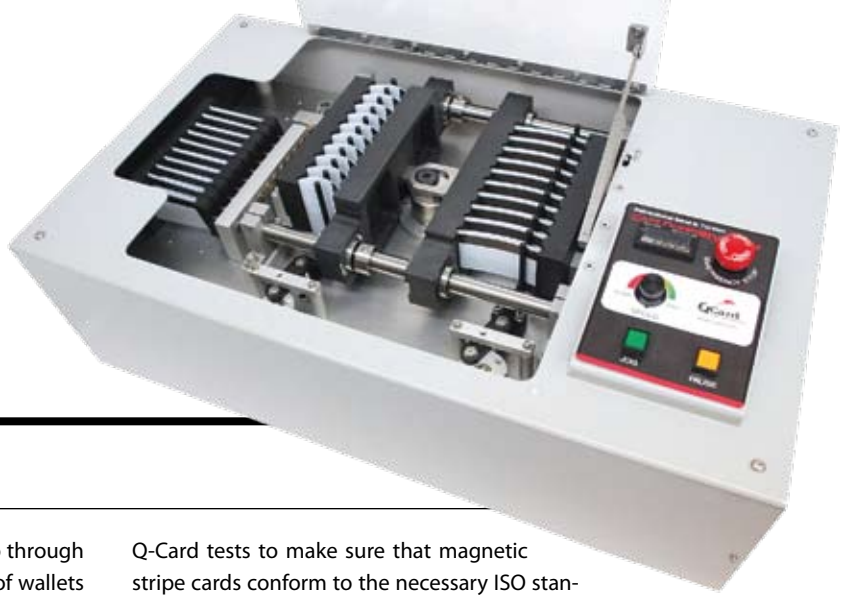
HP has come up with the "four As" for multi-function devices: authentication, authorization, accounting and auditing. HP's system is also able to say how much individuals are printing and who's printing and scanning what documents.

HP has come up with solutions for all four of these with an added bonus: being green. "By having a secure environment you can also control how much is being printed," Barkey says.

Smart cards also aren't the only form factor that can be used for securing the multi-function printers, Barkey says. HP has seen applications that use biometrics or proximity cards as well.

Whichever technology is being used, it has multiple functions. "It's a lot more efficient to have one card that opens the door and accesses the network," Barkey says.

Testing companies make sure ID cards can stand test of time



Angela Tweedie
Contributing Editor, AVISIAN Publications

Imagine the stresses credit cards, ID cards and debit cards go through on a daily basis. Between constantly being taken in and out of wallets and purses, subjected to heat, and even run through the washer and dryer, the durability of plastic cards are put to the test every day.

But what most people don't see are the rigorous tests that cards are put through before being placed in a wallet or purse. A battery of tests ensures that the product leaving the card manufacturer facilities is working properly and is in optimal condition.

Many card manufacturers purchase equipment that enables them to conduct the testing in-house, while others choose to go to a third-party testing facility to ensure that the testing is done in an unbiased environment with properly calibrated machines in good working order.

Sunsbury, Pa.-based Q-Card sells machines for card manufacturers to do their own testing but also performs the tests for the manufacturers. "A lot of the larger card manufacturers come to us to do their testing procedures," says Ric Jones, a representative for Q-Card. "It helps keep the company honest and proves to the consumers that their products really are safe and have been properly tested. Both sectors of our business, the actual testing facilities and the testing equipment sales, are growing rapidly."

Business is booming internationally as well. Q-Card opened an Asian division in 2007 to keep up with the growing Chinese manufacturing markets. "China is really an emerging market for manufacturing. We now offer equipment in both English and Chinese in order to accommodate the demand," says Jones.

Q-Card tests to make sure that magnetic stripe cards conform to the necessary ISO standards. The company manufactures the equipment and technology used to produce the magnetic stripe reference cards. These cards are used to calibrate magnetic stripe analyzers during the manufacturing process of cards and tickets. The company also tests contactless smart cards.

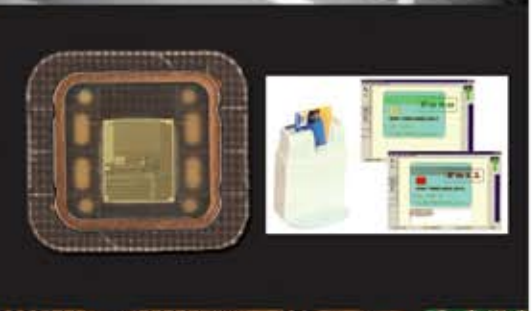
After the cards are produced and encoded card manufacturers pull some cards and send them to a testing facility to see if they meet the necessary specifications. "There are no minimums for testing at Q-Card, so some tests are performed on only one card," Jones says. "The testing facilities are secure, and all the testing is done in-house to ensure that it has been conducted properly."

Often when there's a problem with a card, finger pointing will ensue. "You have a situation where all three entities – the manufacturer, the testing service, and the distributor – can all blame the other party, so test labs and equipment can ultimately determine where the fault really lies," says Jones.

Another company involved in card testing is the Netherlands-based Collis. It offers services for testing, including EMV, contactless, near field communication and Single Euro Payments Area consulting and services. "Our activities are based on our TestGoal test philosophy and method, which includes the full spectrum of test activities: test design and implementation, quality and test management, and reviews, inspections and audits," says Valentyna Romanenko, marketing and communications officer for Collis."

Collis offers several different testing schemes, based on timelines, price and individual customer needs, Romanenko says. The company offers testing in its own facilities, testing in customers' facilities, or a combination of the two.

In addition to smart card testing, Collis also specializes in electronic identification testing, including e-passports, e-ticketing, and e-health programs. Collis also offers consulting services that aid in implementing e-ID programs, Romanenko says.



Exponent®

Exponent, Inc., a U.S. company with a staff of over 800 engineers and scientists, offers a wide range of testing and evaluation services to improve the durability, reliability, and performance of identification devices, cards, equipment, and processes. We offer:

- Independent testing (physical, electrical, interoperability)
- Design analyses
- Reliability studies
- Technology evaluations
- Failure analysis
- In-depth engineering support.

We evaluate smartcards, e-Passports, machine readable travel documents, and other identification devices and associated equipment in accordance with FIPS201, ISO, ANSI, ICAO, and other relevant standards. Exponent is certified to ISO 9001.

For more information, contact Brad McGoran, P.E.
650-688-7013 • mcgoran@exponent.com

www.exponent.com/smartcard_testing_capabilities/

Another player in the test market is the U.S.-based Exponent Inc. The scientific and engineering consulting firm performs testing on smart cards, e-passports, bank cards, and a host of other products that use mag-stripe and IC technologies. Exponent has collaborated with the GSA to test smart cards as a part of the FIPS 201 program.

"We test cards both pre-issuance and post-issuance on behalf of companies. When a product fails to work properly or fails to meet certain requirements, we run it through a suite of compliance testing. On the post-issuance side we examine any card that defaults before the three-year lifespan," says Brad McGoran, senior managing engineer for Exponent.

The smart card testing part of the business was established in 2000 when Exponent was supporting the U.S. Department of Defense on system and evaluation testing. A project had gone over budget and over time, and Exponent was called in to assist. The interest from other groups heightened, and Exponent was tapped to provide support on the DOD Common Access Card (CAC) issuance – which it has been doing for eight years.

On the pre-issuance side, Exponent runs the cards through a number of ISO and ANSI tests on the smart card chip. The company also performs tests on the durability of the card as well.

On the post-issuance side, Exponent looks at any CAC that fails before its three-year lifespan. The company analyzes the card and finds out why it failed and determines if any steps need to be taken to make sure other cards don't fail.

Q-card says most of its tests are performed in just a few minutes' time. The standard tests run on contactless cards are performed on test validation and personalization. Other examinations include heat and flexibility testing, demagnetization, distortion, and data encoding testing on the cards.

"The main focus in mag stripe testing is various things that can introduce 'jitter' in a card, which causes failed transactions. It's basically caused by magnetic particles being improperly coded in the magnetic stripe," says Jones. Jitter is commonly caused by day-to-day activities or dirty magnetic reader heads, but is also caused by defects in the encoding process, which can be determined before the card hits the market.

While the actual testing may only take a little bit of time, the next step is to create a report to send back to the card manufacturer. "The process is generally about three weeks for a complete testing and submission of a report," says McGoran.

While it may seem a bit mundane, the role of the testing companies is crucial to identity management programs. After all, once the cards are approved, they are sent out to issuers and become driver licenses, bank cards, and transit cards … and they become constant companions in our wallets and purses.

Testing the ISO way

A series of specifications and standards define minimum acceptable levels for ID card performance. Documents issued by the International Organization for Standards (ISO) form the basis for testing but other requirements may be added above and beyond these specs by issuing organizations or other bodies.

ISO/IEC 7810 is one of a series of standards describing the characteristics of identification cards and establishes many of the requirements for the physical card stock. Major areas of concern include:

- dimensions and tolerances,
- construction and materials,
- physical characteristics such as stiffness, flammability, dimensional stability, warpage, resistance to heat, surface distortions and more.

ISO/IEC 10373 defines specific test methods for different card technologies.

- Part 1: General characteristics tests
- Part 2: Cards with magnetic stripes
- Part 3: Integrated circuit cards with contacts and related interface devices
- Part 4: Contactless integrated circuit cards
- Part 5: Optical memory cards
- Part 6: Proximity cards
- Part 7: Vicinity cards

Retailer experiments with facial recognition

It really does sounds like something out of the film "The Minority Report." Walk up to a kiosk to place your order and have an advertising message tailored to your demographic segment appear on a monitor next to the cash register.

All this because the monitor has a camera that uses facial recognition technology to determine an individual's sex and age in order to try and give them an offer the customer something they may want.

The technology is from YCD Multimedia and is being tested in Dunkin' Donuts stores operated by franchisee, Kainos Partners in Buffalo, N.Y. YCD and its partners have come up with playlists, different marketing messages that play at different times of day, that appear in the stores.

Customers walking into select stores walk up to a 15-inch digital screen and, depending on when they walk into the store and which store it is, the content will be different. "The content on that screen will be highly targeted and precisely scheduled," says Barry Salzman, CEO of YCD Media, New York.

Some of the stores are using facial recognition technology to capture an image of the individual, make some decisions on his demographic, and then tailor an offer specifically to him, Salzman says.

The technology is basically being used to identify the gender and age of individuals. Depending on those factors and whether or not the retailer is trying to target that demographic a special offer may appear on the monitor. "When someone fitting the demographic bucket stands in front of the screen it will override the standard playlist in real time and give another option," Salzman says.

The pilot has been designed to meet four objectives for Kainos Partners' Dunkin' Donuts stores: drive awareness and trial of Dunkin' Donuts' healthier menu offering; increase sales for the new "Oven Toasted Menu" product line; promote Dunkin' Donuts coffee; communicate the Dunkin' Deals value proposition.

"We're also trying to extend the business into lunchtime as well as promote the healthier menu items," Salzman says.

YCD Multimedia also is working with Technomic, a research partner, to provide analysis of real-time transaction data. With this feature the parties will be able to update and modify promotions in real time, based on actual sales data of promoted products and special offers.

Smart cards in health care making small steps

Credentials have the potential to solve some of industry's bigger problems

Imagine trying to find a patient record for Juan Gonzalez at a hospital in the middle of New York City and having nothing other than the name to go by. It's not easy.

This was just one of the challenges faced by Mount Sinai Medical Center and its affiliated hospital in New York, says Paul Contino, vice president for IT at the medical provider. Trying to properly match medical records to the patient is critical. Finding out about previous conditions and medication can impact how a patient is treated and literally mean the difference between life and death.

Smart cards can help solve this, along with other problems in health care. Mount Sinai was one of the early adopters of smart card technology in the U.S. and has an aggressive project in the works that would eventually issue 100,000 smart cards to patients in New York City.

It started in 2004 with Sinai's affiliate Elmhurst Hospital Center, Contino says, when the hospital started issuing 14-kilobyte contact chip cards to patients visiting its clinic. The chip holds a small text file containing a portion of the patient's medical record.

The program is successful because 96% of patients returning to the clinic would have their cards and thus could be properly identified, Contino says.

But the card only contained data from Elmhurst so if the patient saw a specialist at another provider the information would not be reflected on the card, explained Contino. "There wasn't the ability to show results across multiple institutions."

Elmhurst, Sinai and eight other New York-based institutions decided to build a system that could be used at all their hospitals and clinics, Contino says. The institutions would standardize the data model and technology and issue cards to patients that contain portions of their medical record as well as demographic and health insurance information.

Instead of storing a patient's entire medical record on the card it was decided that a snapshot would be best, Contino says. The most recent medical activity and lab results would be on the card along with current medication, allergies and an overall problem list. Giving physicians the entire medical record on the card wasn't practical, as they wouldn't have time to review the whole thing. "It gives doctors up to three really good pages of medical data, a summary that is up to date," he says.

The model for the card was built around an emergency card. Clinicians decided that it was important to have the most recent information available to a doctor if the patient is brought into the emergency room, Contino says.

The emergency room physicians had one other request, a recent baseline echocardiogram. Contino says they were able to compress the EKG image to sit on the 64K card without any issues.

The cards are being issued at the hospitals. Before the patient receives the card there is some identity vetting performed. "They need to present another ID and insurance information," he says. The card also includes a photo of the patient and a medical record number.

Three hospitals have started issuing the card, Contino says. Contino estimated that around 5,000 cards have been issued so far and each of the 10 institutions will issue 10,000 cards.

Identity technology is key to a wide range of health-related needs

Contino says smart cards are still emerging in the health care market but can provide a solution to a big problem. "We see a real opportunity to improve patient identification," he says. "You need to be able to identify a patient quickly and efficiently."

Proper identification of a patient leads to the administrative staff getting better information which can then impact insurance claims and the amount of money coming into the hospital, Contino says. Being able to accurately identify a patient also means being able to accurately charge the patients and the health insurer.

Smart cards can also decrease the possibility of duplicate patient records, a big cost for hospitals, Contino says. "Most hospitals have some level of record duplication, whether it's 2% or 15%," he says.

Contino says Mount Sinai has spent millions of dollars over the past six years to clean up duplicate and co-mingled medical records. That compared with spending between $4 and $7 per card may be a bargain in the long run. "We're investing money in smart cards so we don't have to do massive record duplication," he says.

There may be other applications for the cards down the road as well. Health care organizations are starting to invest in regional health information organizations (RHIOs), which enable those participating to share medical record information when necessary.

Part of the problems with RHIOs has been patient identification. The smart card could act as a secure token to identify the patient, Contino says. "Instead of doing a probabilistic match you could enhance the match by using smart cards," he says.

Randy Vanderhoof, executive director of the Smart Card Alliance, says organizations are working on standards for this information as well, which may accelerate the adoption on smart cards in health-related fields. The U.S. Department of Health and Human Services is working to create interoperable standards for electronic medical records.

The ability for consumers to carry around a personal health record is catching on as companies like Google and Microsoft start entering the field and offering different products to consumers, Vanderhoof says. "There's a lot of little bowling pins starting to fall," he says. "It's raising awareness at the consumer level that putting the information into a personal heath record has some value."

Identity with equality for all

Stephen P. Howard
Thales e-Security Inc.

Identification in the U.S. is fundamentally broken. How do we fix it and why does it need to be fixed? And what do we mean when we say "Identification is fundamentally broken"?

In discussing this, we need to outline a few key issues:

- The decline of "Practical Obscurity"
- Financial fraud vs. true identity theft
- Long lasting ID numbers
- Equality
- Options to address the issue

We will take this in order to enable us to understand our conclusion: we must get to solutions that enable individuals to protect their own identity. Enabling protected identities for all will require new thinking. And this requires specific action by government agencies, legislators and the private sector.

Practical Obscurity

On August 12, 2008, National Public Radio's Kojo Nnamdi show led a discussion on Practical Obscurity *(Technology, Privacy and "Practical Obscurity" - www.wamu.org/programs/kn/08/08/12.php)*. The thesis of this session, as copied from NPR's Web site, was:

> "It's the kind of personal data most people would prefer to keep private: an old speeding ticket or a check written to a presidential candidate. But new Web sites are making this data available to prying eyes, potential employers, and curious acquaintances [sic]. Tech Tuesday explores how information technology is ending the days of "practical obscurity."

In the recent past, prior to the ubiquitous Internet, public records were hard to get. To investigate someone's criminal history, you had to know how to go to the federal, state, county or local jurisdiction, physically walk into the office and request the records in paper form. Essentially, this process defines the concept of Practical Obscurity. It isn't very practical to search for identity and personal information using this method.

With this in mind, using static identifiers (such as a Social Security Number) to enable indexing of records is not really a problem. Hence EXECUTIVE ORDER 9397, NUMBERING SYSTEM FOR FEDERAL ACCOUNTS RELATING TO INDIVIDUAL PERSONS, signed by President Franklin Delano Roosevelt on November 22, 1943, did _not_ create a privacy risk to citizens. EO9397 mandates the use of the Social Security Number as the primary index for all federal information, mitigating an extremely expensive set of duplicate identifiers and management processes within every federal agency.

The Internet has dramatically changed this model. If you do listen to the audio of the NPR story, you will hear about *www.criminalsearches.com*. This is a new *free* service. Just type in a name and you will see all known information that is published electronically for all federal, state, county and local criminal databases. This service makes money through advertising. It is a direct challenge to organizations like ChoicePoint or LexisNexis, who charge for access and tightly control the information.

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**.

Join the Smart Card Alliance at these upcoming events:

Smart Card Alliance

CARTES 2008 — 23 Years Supporting the Smart Card Industry

November 4-6, 2008
Paris-Nord Villepinte
Exhibition Center
Paris, France

ctst 2009 THE AMERICAS — Smart Card Alliance

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

FOR EVENT INFORMATION VISIT WWW.SMARTCARDALLIANCE.ORG

WORLDWIDE OUTREACH

UNRIVALED EDUCATION

TASK FORCES & REPORTS

CONFERENCES

NETWORKING

Services like CriminalSearches have their flaws: data on that Web site is not certified and confirmed to be full, complete and accurate. You still must go to the official source to "ground proof" the information and confirm it. If you don't, buyer beware.

Regardless, the notion of Practical Obscurity that is an underpinning of our society to "rely on secret identifiers" for identity is quite completely broken.

Financial fraud vs. true Identity Theft

As we move forward in time, it will be useful to delineate better what the lay term "identity theft" actually means. The all encompassing view is that identity theft is use of any identifier to commit crimes or fraud against an individual. But this is way too broad.

There are really two major categories of identity theft:

- Financial Fraud
- True Identity Theft

In the financial fraud case, the criminal uses static information about you. Examples of static information include skimmed credit card numbers, your home address, your name, mother's maiden name, etc. From there, they proceed to use Internet stores and buy stuff in your name, using your line of credit. In the United States, we have Visa and MasterCard supporting the Truth in Lending Act. As such, you are not liable for these fraudulent charges.

True Identity Theft is much more frightening. In this case, the perpetrator may be an illegal alien who purchases static information about you, such as your Social Security number, address, date of birth, birth certificates, etc. They then seek employment using your identity. They then seek a mortgage to buy a house in your name. They may sell the house they bought, or even your primary residence out from under you, and take the cash. They may or may not pay taxes in your name. They then fake a death against your name. They then try to claim your life insurance.

In the true identity theft model, they act with impunity to become you in a holistic sense. You may not find out about it until the IRS contacts you or the new buyer for your house asks you to move out so they can move in. This type of attack is extremely difficult to undo. It may take years, legal fees and lots of personal time to correct.

The core underpinning of all these events is that practical obscurity is no longer legitimate insurance or protection against attack. Open records are the reality of our current situation.

Long lasting ID numbers

ID numbers that represent us are not really a true threat. The Social Security number, vilified as a source of ID theft, is not really the problem. The problem is that it is static and it can be used by people it without authenticating the individual presenting it for that use.

The SSN is not much more than a User ID. That's all well and good but would anyone ever login to a computer where all you needed was the User ID and not the password? Typical Web services or IT resources require a minimum of User ID and password as a threshold. If they do not require this, then the notion is that the data is public, such as a brochure published on the Internet.

There is a substantial effort underway for FIPS 201 and the Personal Identity Verification program throughout the federal government to move to even stronger means of electronic access to information and network resources. Specifically, this program assists in migrating away from User ID and password towards PKI and smart card tools. The User ID is no longer the valuable static bit of information. As an identifier, it is harmless. Used in combination, the User ID and PKI login is very effective. And that long-lived static identifier, your User ID, is rendered unimportant and less useful to the attacker.

Equality

As we move forward in time, we must look to systems that address identity theft on the whole, and how these solutions affect various populations. There are many issues and programs to consider. The following is an incomplete list of various ID programs and the populations they serve:

- Driver's license – anyone that passes the State's driver test
- Real ID – any legal individual
- Proposed Guest Worker ID card – legal aliens
- Green Card – legal permanent resident aliens
- FIPS 201 PIV credential – vetted executive branch employees and contractors
- First Responder Authentication Credential (FRAC) – vetted emergency responders
- E-passports – U.S. Citizens and any other foreign nation's citizens
- Employment Authorization Document – legal aliens
- Social Security card – any legal individual
- Alien Registration Number – legal aliens

As we look at these programs and technologies, they break into two categories: electronic vs. static printed media. From a technology perspective, the e-passport, FRAC and PIV credentials all provide electronic tools to ensure that only the individual that was issued that ID can legitimately use the credential. The others are static printed documents, easily copied, forged or acquired through Internet services.

There is a real challenge to our nation when evaluating these programs. A classic case is Real ID vs. Guest Worker Card. For Real ID, the law requires a strong identification vetting, very much like FIPS 201 PIV part I. We will have high confidence that the individual is legally in the United States. Then we issue a static printed plastic card, which kind of defeats the purpose of the vetting. For the Guest Worker ID, the early discussion was to use an e-passport or PIV like electronic ID credential that is tightly aligned with the individual using biometric identifiers.

So what are the challenges of equality? If this proceeds apace, we will set up a caste system … Guest Workers vs. US Citizens for employment. As an employer, how do we avoid discrimination when we determine who is a citizen with right to work, who is a guest worker with right to work, as opposed to a perpetrator of ID theft with no right to work or be in the country?

The perpetrator simply needs to continue to behave as a US Citizen by buying static information and presenting legitimate fraudulent documents to the employer. Without equality in the strength of mechanism for authentication of who is presenting the document, the whole house of cards comes down and the perpetrator wins the battle.

Options to address the issue

Remarks by Homeland Security Secretary Michael Chertoff at University of Southern California National Center for Risk and Economic Analysis of Terrorism Events is a very well reasoned and thoughtful approach to address identity issues in our nation *(www.dhs.gov/xnews/speeches/sp_1219162986509.shtm, Release Date: August 13, 2008)*. He states, "I'd suggest to you that identity is at the heart of a number of other very significant elements of our social fabric."

This quote is the basis of this article. As we move forward in time, we must enable everyone and anyone to have an equal means of proving identity. All ships float on a rising tide. Our objectives must be to enable all employers and employees, all citizens and non-citizens alike, to share identity information that can be trusted and verified as accurate and current.

Real ID achieves some positive results: strong vetting processes to prove the identity of an individual. Yet it has a weakness in that the credential issued does not use secure electronic technologies. The Green Card has strong vetting and also uses insecure technologies to represent the individual.

We must achieve equality in how we treat citizens and noncitizens alike. And the tools we use must support our national interests. To start this process, legislators and regulators need to take action to ensure identity policy reaches all populations equally. Private industry needs to use stronger authentication models that align with these new legislative and regulatory solutions.

PIV, e-passports, FRAC and similar programs provide the way forward. One potential solution is to enable and empower any organization to stand up and issue a certified credential according to best practices and standards such as FIPS 201. This will mitigate the risks of true identity theft, and not require the U.S. government to issue a National ID Card, which so many fear.

We hope to see more use of FIPS 201 and e-passport technologies in the future. They are the way forward.

Stephen P. Howard serves as vice president, business development-identity management, for Thales e-Security, Inc. and has over 24 years of information technology experience. He led the technology tiger team that developed the FIPS 201 recommendations to NIST, and is experienced in systems and operations of smart card technologies inclusive of silicon fabrication, manufacturing, cryptography, contactless, and biometric methods.

Chertoff: Control of identity critical in 21st century

Protecting identity is critical and is only going to become more important as time goes on, says U.S. Department of Homeland Security Sec. Michael Chertoff.

In a speech at the University of Southern California National Center for Risk & Economic Analysis of Terrorism Events in August, Chertoff talked about how important identity can be.

"It lies at the core of a great deal of what we do protecting our financial security, our personal security, and our reputational security," Chertoff said. "And what I'm referring to is how we manage and protect our personal identities because I'm going to submit to you that in the 21st Century, the most important asset that we have to protect as individuals and as part of our nation is the control of our identity, who we are, how we identify ourselves, whether other people are permitted to masquerade and pretend to be us, and thereby damage our livelihood, damage our assets, damage our reputation, damage our standing in our community."

Identification online is also becoming important as more business is transacted over the Web. "Identity, more and more particularly with the use of the Internet for purposes of transacting business, lies at the heart of our entire financial and market system," Chertoff says. "If we don't know who you are, if we don't know whether you are accurately representing your assets and your intentions over the Internet or even transacting business face to face, we introduce an element of risk into that business model."

This eventually could impact the economy. "The entirety of our economic livelihood in the 21st Century is going to turn in large measure upon our ability to verify identity for those who want to transact business, and, finally, our reputation and our privacy depends on our ability to control our identity. If people can pretend to be us, if they can speak in our name in an unauthorized way, they can do great, perhaps irreversible, damage to our privacy or to our reputation and this again from a personal standpoint suggests that identity is increasingly going to become the asset that we have to be most careful to protect in the 21st Century where the ability to get information, move it around the world and store it indefinitely creates greater and greater risks to personal reputation and personal privacy."

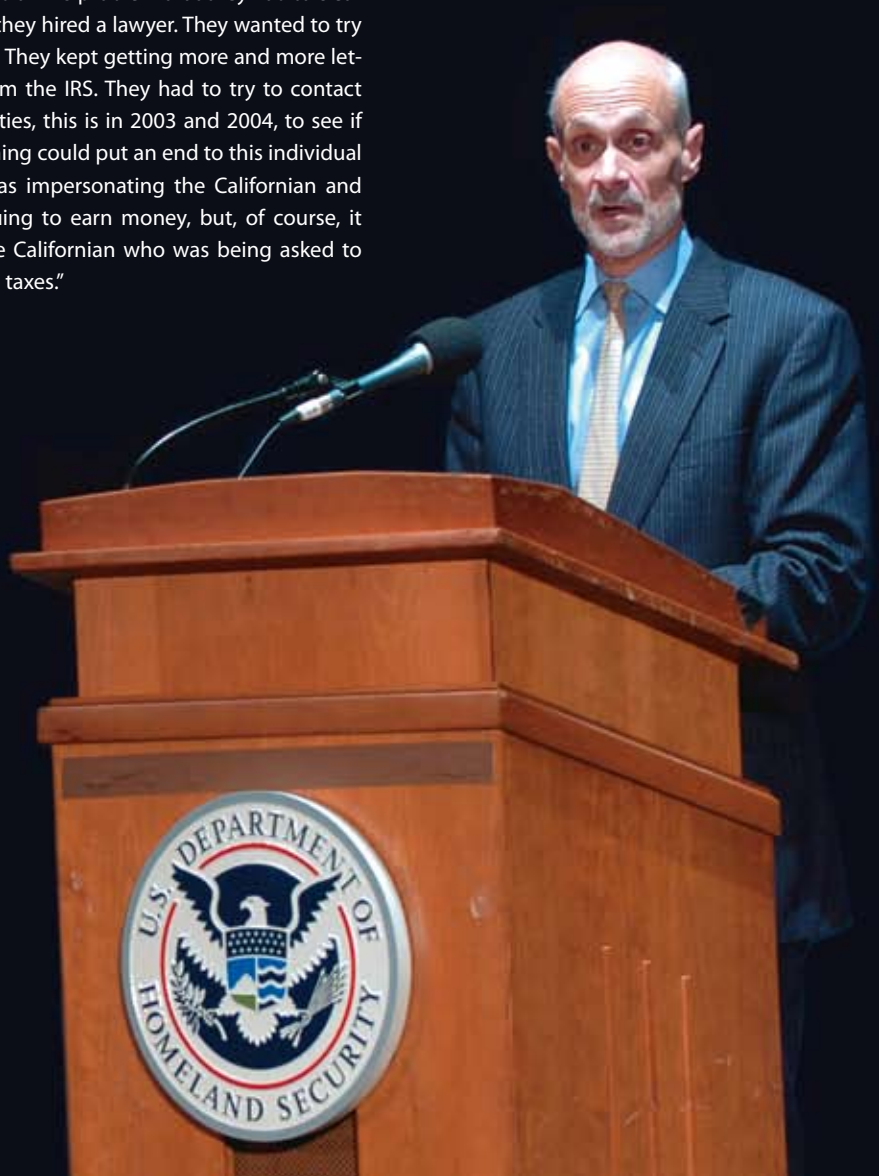
Chertoff gave some examples where identity theft-related issues have caused individuals and companies trouble. Illegal aliens making up Social Security numbers and working in the country illegally have caused problems. He cited one individual who received a letter from the IRS regarding $18,000 in unreported income.

"This person, however, had never worked in the company in question," Chertoff said. "In fact, the company was on the other side of the country in North Carolina, and all of a sudden, they had an IRS problem that they had to clear up. So they hired a lawyer. They wanted to try to fix it. They kept getting more and more letters from the IRS. They had to try to contact authorities, this is in 2003 and 2004, to see if something could put an end to this individual who was impersonating the Californian and continuing to earn money, but, of course, it was the Californian who was being asked to pay the taxes."

Chertoff says authenticating identity in different scenarios is going to become necessary. How do we know who people are online? He points to the Social Security number, passport and driver license as ways individuals are identified now, but there needs to be more.

"I like to say that the issue of identity authentication, determining that you are in fact the person you claim to be, really rests potentially on what I call the three Ds: description, device, and digit."

Description is a piece of information known only by the individual. Device, in today's world, would most likely be some type of card, but it can refer to other things as well. "A cell phone could be used as an identification device," Chertoff says.



As for digit, Chertoff says fingerprint biometrics are the third factor. "Your digit is unique. Your fingerprint is unique and the ability to use that as an identifier, as we do, for example, throughout the criminal justice system, gives us a third powerful tool that we can use in order to make sure that we can separate real people from impersonators."

The future is using all three of these "Ds" together to authenticate identity. "The way forward is to work with all of these tools in combination, to take the ability to use some descriptive information, like a PIN, or some private information, a device like a card or perhaps a cell phone or other electronic device, perhaps with a token, and a biometric, like a digit which is easily used and concurrently be captured on a whole host of mobile devices, to combine these together, and I can envision a time in the not-too-distant future where, in order to authenticate yourself, whether it's for purposes of getting on an airplane, whether it's for purposes of transacting business at a bank, whether it's for purposes of gaining entry into a student dormitory, that you will have some kind of device; it may be electronic, that will combine two or three of these three Ds, as I call them, to increase the ability to be secure in the knowledge that nobody else can duplicate your ability to identify yourself."

The solution may not be perfect, but it's better than what exists now, Chertoff says.

"There will be some people who will be so good that … they'll steal your device, they'll find a way to get your fingerprint and fabricate it and then they'll somehow ferret out the piece of information and having assembled all these things, they'll be able to impersonate you." Chertoff says

"But, you know, nothing is perfect. If the test of any movement forward in a system were that the new system has to be perfect, we wouldn't have airbags in automobiles. After all, the airbag is not perfect. If you run headlong into an 18-wheel tractor-trailer, that airbag is not going to help you. But in a lot of accidents, it will help you. So I'm arguing this is a 99% solution and in real life that's a very good solution." ID

HSPD-12 Roundup

Most agencies will miss HSPD-12 deadline, but progress has been made

By the time you read this, the Oct. 27 HSPD-12 deadline, when government agencies were supposed to have completed issuance of credentials to employees, will have passed.

But progress has been made, says Mike Butler, program manager for the managed service office at the General Services Administration, though he is hesitant to estimate how many credentials will be out there. "Not everybody will be done, but everybody did get the message and they are working on it, the numbers will show that," he says. "I know they're out there because when I get on the Metro you can see the cards hanging on people's necks."

The GSA, which is handling credentials for 70 agencies, is supposed to issue around 800,000 credentials. All told, including the U.S. Department of Defense that has till 2011 to issue the new IDs, 4 million total credentials are expected to be issued to all federal employees. As of late September the GSA had activated 96,489 credentials and enrolled 287,512 government employees.

Even though the number of credentials activated might not be where some want it, Butler says the move forward is significant. "This is a huge project and to get a working credential into the hands of government employees is no small thing," he says. "It may not be pretty but it's getting done."

As of early October the GSA was focused on activating credentials more than enrolling employees because it was the activation numbers that the White House Office of Management and Budget, the agency overseeing the program, would be looking at, Butler says. "We're enrolling around 2,000 people a day," he says.

Butler says there are many agency success stories when it comes to issuing the credentials. The United States Department of Agriculture has activated 16,338 credentials and is getting its employees new laptops so the cards can be used for logical access, Butler says. The agency is also using the card for physical access control in some of its buildings, too.

The U.S. Treasury Department is another that has stepped up, Butler says. The agency has sponsored more than 88,000 employees and activated more than 23,000 credentials. The U.S. Department of Energy has made strides, enrolling more than 42,700 and activating 22,644.

The progress of credentialing has picked up tremendously this summer, but the systems still have problems, including vendor issues. "I wish the vendor community had their act more together than they do," Butler says, adding that the government remains the quality control medium to impact vendor performance.

The next steps are deploying systems that use the credential, especially for network access, Butler says. ID

Featured FIPS 201 Products

ACR38
Advanced Card Systems LTD

The ACR38 smart card reader/writer is a USB full speed device designed for use in the PC environment today. This reader has an optional built-in Security Access Module (SAM) slot that supports various high security applications. It is ideal for use in network security, electronic payment systems, electronic identifications as well as other advanced smart card applications.

Secure Badgeholder DuoLite for ID cards
Identity Stronghold, LLC

The new Secure Badgeholder DuoLite™ is now available for users that need to shield two contactless cards. One side of this holder accepts the card from the side which also allows easy access to magnetic stripe cards. The other side accepts the card from the top. This combination allows the wearer to choose which combination suits their needs. It's lightweight, durable, and small. You won't even realize it is there.

Newly approved FIPS 201 products

Electromagnetically Opaque Sleeve
No Access Passport Holder
Sports Prescriptions Inc

No Access Men's Wallet
Sports Prescriptions Inc

Secure Badgeholder DuoLite for ID cards
Identity Stronghold, LLC

Skim-SHIELD RIGID-2, 2-card, top-load badge holder
Logic First, LLC

PIV Middleware
Athena IDProtect PIV Middleware
Athena Smartcard Inc.

Template Generator
STARTEK ANSI/INCITS 378 Template Generator for PIV
STARTEK Engineering Inc.

Template Matcher
STARTEK ANSI/INCITS 378 Template Matcher for PIV
STARTEK Engineering Inc.

Transparent Reader
ACR38
Advanced Card Systems LTD

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.

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

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.

AN AVISIAN ID TECHNOLOGY RESOURCE

NFC is more than just payments

Ticketing, physical access and information sharing take off

Andy Williams
Contributing Editor, AVISIAN Publications

Mention near field communication and most think mobile payments. That's probably because the next generation technology is being touted as a replacement for contactless cards or potentially even the next wallet. NFC will enable a phone to carry all your credit cards, loyalty cards, maybe eventually even your driver license.

But what makes NFC so attractive is the wide range of applications it can support, whether it's opening a door, logging into your computer, signing on to the Internet, or using your phone like a PDA stylus, touching points on a map or other display to gather further information or directions.

Near field communication, co-developed in 2004 by NXP Semiconductors and Sony, is a short-range wireless technology that evolved from existing contactless technologies, according to the NFC Forum, a non-profit association created in 2004 by NFC's founders and which now includes some 150-member companies. NFC is supposed to simplify the way consumer devices interact with one another, helping people speed connections, receive and share information and even make fast and secure payments.

Gerhard Romen, director at Nokia, a manufacturer of NFC-compliant phones, estimates that 85% of NFC applications have nothing to do with payments. He cites ticketing as one example of the many applications possible. Ticketing applications are already underway with pilots in New York City's Metro system and San Francisco's Bay Area Rapid Transit system. In both cases, NFC-compliant phones are being used as transit tickets similar to how contactless smart cards are used.

A CONVERGING CONTACTLESS LIFE

PAYMENT

TRANSIT

ACCESS

ID

make the move

inside CONTACTLESS

www.insidecontactless.com

But the NFC Forum wants people to know there is much more you can do with NFC besides making a contactless payment or riding a transit system. To encourage development of "cool" NFC applications, the organization has conducted an annual contest to encourage out-of-the-box developments.

The winners in this year's competition included an NFC-enabled lock for hotel rooms that enables guests to bypass the check-in process and unlock their hotel room doors using their phones. The other winner was an interactive prototype designed by the UK's Lancaster University that can be applied to a tourist guide. (See related story, Page 48.)

Both are prime examples of NFC's versatility, but they're not the only ones. Some are even in commercial use today. "When you look at non-payments, the first thing that comes to mind is access control, whether for buildings, offices, or even for hotel elevators or hotel rooms," says Martin Buehrlen, secretary of the NFC Forum and senior manager of marketing programs at NXP. "But access can also mean access to computers, such as logging into your PC by touching your mobile phone to the computer."

With access control and NFC it's difficult to say how many pilots are underway because those operate on a relatively small scale, he says. "You don't do it with thousands of people," Buehrlen says. "Usually you do it in tens or hundreds."

One of the advantages of NFC is that companies already using contactless smart cards for access control won't need to change the infrastructure.

Hotel room keys on your phone with NFC-enabled locks

VingCard Elsafe of Norway took first place in the commercial category of the NFC Forum's "Touching the Future Competition" for its Signature RFID electronic locking system for hotels that enables hotel guests with NFC-enabled phones to bypass the check-in process and unlock their hotel room doors using their phones.

The research track winner was the UK's Lancaster University for its Touch & Interact system. The project uses NFC technology to enable mobile phones and public information screens to share display space, overcoming the screen size limitations common with cell phones.

The hotel locking system from VingCard, an Assa Abloy company, isn't new. It has been around since 2006 and what's unusual about it is that, despite lack of cell phones to really make the system work, hotels continue to install these NFC-compatible locks.

"We were somewhat surprised we were selected for the NFC Forum award," says Pascal Metiver, VingCard president for Europe, the Middle East and Africa. "I think they were most impressed by the fact that even with the lack of phone availability, it was still functioning in 100,000 hotel rooms, that hotels are buying the locks to use NFC because they understand the business case, they see the value."

Metiver says the system is designed to address important elements in the hotel industry. "One is its common knowledge that hotel guests don't like to stand in line to check in or check out. That's an absolute burden for most guests. As a result, chains have been trying to streamline this process. The second aspect is that chains are looking at getting more control over their distribution channels. For a hotel, it's more lucrative to sell you a room through its Web site. If you combine those two factors, you bring a unique service to the guest."

Hotels could make the NFC service available only to guests who are members of its loyalty program. "Once they're registered, they have the option to receive their room key prior to arrival at the hotel, on their NFC cell phone via a text message. And if the phone is GPS-enabled, they can even find the hotel easier," he adds.

The room key is encrypted and secured by the SIM card inside the phone. To prove the usability of the concept, Metiver adds, some hotels are even loaning guests an NFC phone when they check in.

When it comes time to leave, guests can use the NFC phone to check out through the NFC-enabled TV in the room or an NFC-enabled kiosk. Guests receive their invoices either through text message or printed out at the checkout kiosk.

Metiver expects commercial releases in 2009 and 2010. "We're working with numerous carriers, and some will be announcing commercial launches of NFC applications then," he adds.

Still, he doesn't think NFC acceptance has been slow. "If you take a normal technology cycle, it's typically seven years. We're probably reaching year three and a half to four years now on a global basis," he says. "The hotels are building the infrastructures to reap the benefits of NFC as soon as the phones are released."

Empowering Bluetooth

Another major non-payment use of NFC is its capability to manage Bluetooth devices. Bluetooth is a wireless communications protocol, which some may say is similar to NFC, which enables multiple devices to communicate with each other. One of the problems with Bluetooth, however, has been setting up the pairing without conflicting with other nearby Bluetooth devices.

"In the home your phone and Bluetooth devices are the only two present, but in an office when you have to identify which is your device, your headset and your PC – because you have 10 phones and 20 PCs in the area – it's pretty difficult to configure," says Buehrlen. "You want one headset linked to your phone and not your colleague's. You need a one-to-one link between the headset and the phone, otherwise incoming calls could go to the wrong person. NFC technology makes it easy to pair two Bluetooth devices."

With an NFC phone, all you need to do is put your headset and mobile phone together and they instantly pair. "You don't need to go to complicated menus in the phone to activate this pairing. When you do the Bluetooth pairing now, the phone needs to select from the entire list of available Bluetooth devices. If you have 20 others, it could be a trial and error phase," says Buehrlen. "But with NFC, you just touch them together for less than a second and the two devices get introduced to each other. Then maybe you have to push one button on your phone to confirm. It's much easier to do."

Smart posters, products and services

One of NFC's most hyped applications is its ability to retrieve information from different sources. "You might see a poster at a bus station informing you about the latest movie and you're interested in finding the closest theater, watch a trailer or even make a ticket reservation. Touch a smart tag on the poster with your mobile device and you pick up all this information from the poster or via the Internet."

Beyond smart posters, products can be tagged to expedite access to key information. Pharmacists and drug manufacturers are considering affixing a tag to the pill container. A new washer and dryer could be tagged and provide access to the owner's manual or details about its operations.

"As we've seen in the NFC Forum competition, there is no end to what you can do with NFC technology," says Nokia's Romen. "I have seen blood pressure measurement devices where you can touch your NFC phone to the device and your blood pressure results can be sent, via a text message, to your doctor, allowing the doctor to easily adjust your medication."

In the Netherlands, 10,000 nurses are using NFC to track their visits to patients' homes, says Romen.

After arriving at the patients' home they use the NFC device to identify the patients and what needs to be done during that visit. "It also serves as a digital signature so insurance will pay for the health care and can also see what health service was provided," he adds.

The service is provided by NEDAP, a Netherlands-based ID security company, using Nokia phones. The project was introduced two-years ago and has undergone rapid growth since then, says Romen.

In the UK, a security service that provides guards for vacant buildings, places NFC-style tags throughout the buildings. A guard, when he enters, taps his NFC phone against a tag that is then read and transmitted back to the security office. The guard has to make it to the next point in his security sweep in a set amount of time to tap the next tag or the office it notified that there may be a problem. "You never know who's around the corner in these vacant buildings so this is for the guard's protection," says Romen.

In Frankfurt, you can touch your phone to a city guide and get a map of the town and in Monaco, you can tour the Grace Kelly Memorial Trail and, with an NFC phone, touch several points along the route to see information about the former film star's life, says Romen.

Size does matter

Lancaster University's Touch & Interact, addresses the limited screen size of mobile phones. It won the NFC Forum's award for best application in the research category at the 2008 "Touching the Future Competition."

Because of the small screen size, current mobile phones may still fail to fully address the requirements of map, multimedia and information browsing applications.

Touch & Interact uses mobile phones like a stylus on a PDA. One of the Lancaster researchers probably put it best: It's like using a touch screen, but the cell phone replaces the finger.

You touch the display, such as a map, with your NFC-enabled device at any position to call up selections. During the interaction, both the phone and public screen share the display. This shared display can be useful for separation of public and private information by presenting sensitive information only on the phone. A tourist map application was used to test the project in a real world environment.

Enrico Rukzio, academic fellow and lecturer in the computing department at Lancaster, says the cell phone interacts with the larger display, but they don't show the same thing. "In the prototype shown at the NFC Forum, the big display showed high-resolution map information and the mobile phone displayed contextual information, for example, details on selected points of interests.

For the Touch and Interact demonstration, a projection screen was used. "Our vision is that one will find NFC enabled LCD/plasma/projection-based displays at public spaces like train stations, airports, supermarkets, shopping malls or tourist offices," says Rukzio. "The user could then use his/her mobile phone to interact with various points or tags on the screen at any position."

He says the University of Lancaster developed Touch & Interact as part of an industry-sponsored research project funded by NTT DOCOMO, Japan's largest mobile operator.

Peer-to-peer possibilities

NFC also makes information sharing possible between devices, says Buehrlen. Two NFC phones in close proximity to each other can communicate with one another. "It's like exchanging business cards, only you just need to hold the phones next to each other and the information is passed from one phone to the other."

Another example is what Buehrlen calls peer-to-peer. "This was one of the purposes of NFC in the beginning, so that it can run in mixed infrastructures." In his example, an NFC phone can do double duty as a card reader. "You can use your phone as a value checker for contactless cards. When you have a contactless card or a bus ticket, you can check how much value is left on the card."

What has helped spur NFC development to date are the standards the NFC Forum has produced, such as how this information is to be stored in the tags, says Buehrlen. "The specifications and compliance programs in the NFC Forum are materializing and being launched. It is clear for device manufacturers what they have to do and how to achieve interoperability of the devices and to have consistent uses and experiences for the consumer," says Buehrlen.

The industry has needed the standards. When Nokia first introduced its so-called NFC-compliant phone, it was an accessory says Buehrlen. "The next phone from Nokia, the 6131, was sold in quantities but was not globally promoted and not sold outside of areas where trials were conducted. The latest Nokia phone is being sold to everyone. It shows that manufacturers are betting much bigger stakes on this technology."

Something holding NFC back is the fact that existing mobile phones can't be upgraded to accept NFC. "NFC hardware involves a chip which runs the RF protocol, the RFID interface," says Buehrlen. "This transceiver chip translates the RF interface into a protocol understood by the microprocessor."

Nokia's Damien Balsan, business development for the Americas, believes 2009 will be there year that NFC starts to gain traction. "You're going to see carriers and transit authorities finally getting along together to get this to work."

Buehrlen agrees. "For the past few years, we have always put out the message that next year NFC will take off. Now I believe it is really going to come about."

Balsan says while some are "looking for a killer app," the vast majority of applications at first will be simple.

He says Nokia is working with lot of companies who provide applications that will be ready when there's a national rollout of NFC. Nokia's 6212, the next generation NFC phone, will be out en masse by the fourth quarter of 2009. "That phone is really made for Europe and Asia, but we're working to have a number of these phones for pilots in the Americas," he adds.

But the big holdouts are still the mobile operators. "At the end of the day, nothing can be done without the carrier," says Balsan.

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

HID takes the next big 'logical' step

Announces support for iCLASS® contactless cards in Dell laptops, plus new HID on the Desktop logical access control solutions

"Never before has it been so easy to have convenience meet security at the desktop."
— Denis Hébert

Physical and logical access on a single credential … We have been talking about it for years using the industry buzzword convergence but it has been more difficult to achieve than most ever imagined. But this may be changing. Recent announcements from HID Global outline how to access both your building and your computer from the same contactless card.

At a press conference during the September ASIS International Conference in Atlanta Denis Hébert, HID Global's president and CEO, announced that new Dell Latitude E-Family laptops have a contactless smart card reader built into the palm rest that supports iCLASS cards.

When using an iCLASS® card, laptop users will be able to use Dell's pre-boot authentication functionality which helps to secure the data on the laptop. When first turning the laptop on, a user will present an iCLASS card to the contactless smart card reader. A valid card presentation will enable the laptop to boot up and take the user to the Windows operating system.

In the future, users will be able to experience secure, two-factor authentication with the ability to present their card and a PIN to securely authenticate to either Windows XP or Windows Vista. This conforms to Microsoft's strategic direction to deploy smart cards for secure authentication.

A good password management system has been one of the major barriers to computer authentication, Hébert said, quoting Microsoft founder Bill Gates that "passwords are the weakest link in the system." Hébert said this is what HID can help resolve.

Plus with this new system, a single iCLASS card can both get an employee into the building and access his computer. "We're accelerating the requirement for convergence of security solutions by enabling a single credential for physical and logical access," says Hébert.

More importantly, this makes logical and physical access control more accessible, in this case to small- and medium-size businesses, something that because of cost and complexity may have been out of reach before.

Another logical step in convergence

HID also announced what Hébert called "the next logical step … logical access on the desktop." HID on the Desktop is a set of logical access control solutions including both hardware and software.

On the hardware side, HID cards or tokens and a series of OMNIKEY® card readers are available. The newest addition to the series is the OMNIKEY 6321 USB dongle reader that can both read and write to both a 13.56 MHz contactless smart card and virtually any SIM-sized contact smart card. It instantly adds contactless capability to any USB-equipped computer and is ideal for mobile users. "It provides a transition between machines that incorporate smart card reader technology in them and standard machines as they exist today," says Hébert.

On the software side, HID's new naviGO™ software enables an organization to use its existing physical access control cards for strong two-factor authentication at the desktop, says Hébert. "It provides logical access control that makes computer access as easy as building access."

The opportunity here, whether with the Dell Latitude E-Series laptops or any machine with an smart card reader, is to let small- and mid-sized organizations achieve convergence … enabling the use of a single credential to control logical and physical access.

Europe moves toward standard, contactless student ID card

If Eugene McKenna at Waterford Institute of Technology in Ireland has his way, in the not too distant future one identification card is all students will need to access services at most European institutions of higher learning.

As McKenna, chief executive of campus services, explains, today a student who wants to transfer from one university to another has to carry with him "a folder containing all his academic credits and qualifications."

That's about to change. With the pilot program that's ramping up, one student card is all that's necessary. "It'll be a student's secure key to access the information on the server, (the key) will be common to all universities," says McKenna, who has been one of the driving forces behind this project.

That's the eventual plan. But first up is the two-year pilot program, expected to kick off in January 2009. The pilot will test the validity of standardizing the type of campus card used in European universities.

The standardization project is known as the European Education Connectivity Solution and the1.5 million euro (US$2.1 million) project was approved for funding by the European Union, which will put up 75%. The remainder will come from a consortium of five companies specializing in campus card systems, says McKenna.

"We are in the process of validating the companies which are acceptable before EU will release the money," says McKenna. He explained that only small and medium sized enterprises (SME) are eligible to participate in the EU funded project so this, among other eligibility requirements, is being vetted.

Europe-wide standardization of campus cards is the brainchild of the European Campus Card Association (ECCA) that was 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. "When it was founded in 2002, its main goal was to get standards in place," says McKenna.

The European campus card system is obviously still in its infancy. "We're maybe 15-years behind the U.S.," he says. But Europe has been "more aggressive in utilizing advanced technology, such as contactless" as opposed to its U.S. brethren. "When we think of contactless chips, it's generally accepted that Europe is ahead in that area."

And while the technology may be more advanced, there aren't any standards. "Some of the more successful campus card projects in Europe are home-grown," says McKenna. "Every campus is developing its own system. There is no such thing here as an off-the-shelf campus card system. We don't have the Blackboards or CBORDs (companies that supply large numbers of campus card systems in the U.S.)."

In the trial phase, students from Waterford and the Technical University of Lodz in Poland, two members of the consortium, will become like exchange students. "They'll be able to use the same card. That's part of the pilot project," he says.

To prove the successful completion of this pilot it will be necessary to have a live test environment involving a higher education institution in two separate European countries, says Kate Kelly, OneCard Solutions, Ireland. OneCard is one of the five card providers involved in the consortium.

The card will be based on NXP Semiconductors' Mifare technology. "If the trial is successful, the system will be licensed to card systems around Europe for various integrators to use," says McKenna.

If all works out as expected, Mifare will be the standard but that doesn't mean colleges will have to adopt that standard, says McKenna. It will simply be a recommendation.

Why Mifare? "It was chosen because it dominates Europe," says McKenna. "One of the first tasks was to establish a standard card and we recommended Mifare, although it's quite possible we'll use other systems too."

He doesn't feel security is a problem. "We'll never place money on the chip. It's just a secure key that will be used to access the system in the back office. (The chip) won't include any personal information that someone else can use. It will have a unique student number that goes on the card and the Mifare chip will have security in place to protect it," he adds.

But universities will be able to add other applications to the card, says McKenna. For example, if a student wants access control and meal plans on the card, "he brings it to the university and the university will program it for their system."

Besides Waterford Institute and Lodz, the University of Zagreb in Croatia is the third university involved in the consortium. All three schools are deemed research centers. "We wanted to get a group that's spread all over Europe," says McKenna.

One campus card provider and a consortium member that has a head start is OP Team in Poland. It has already issued one million student ID cards to 450 universities, colleges and high schools across the country. A reseller of Gemalto products, many of the universities are also issuing cards that can be used at other schools in Poland.

The pilot project aims to prove that standardization works and possibly jumpstart other initiatives across Europe, adds McKenna. "I do believe a European standard will have a great benefit for the card programs across Europe," says McKenna. "Quite a number of universities have been waiting for standards. When you don't have standards, you don't have successful card systems. I also believe that development of a standard might lead to development of bigger (campus card) companies."

Kelly concurs. "This type of project is vital both for the mobility of students across Europe and also for the business potential of campus card vendor companies. The standard product will create huge business potential for campus card vendors across Europe."

Making the switch to contactless

Switching out a physical access control system can be an intimidating process. The switch from 125-kHz proximity technology to 13.56 MHz contactless smart card technology can seem daunting.

But as prices have come down and the advantages of the technology increases, corporations have more reasons to look at migrating to new technology. Two physical access control experts give their tips on making the switch.

Jack Bubany, director of product marketing, credentials and physical access control for HID Global, realizes there is a "natural fear" by some of contactless technology. "They don't fully understand how it works or the level of security it actually provides," he says. "Globally, most people have explicit confidence in contactless technology. In fact, many markets outside the U.S., such as China and Latin America, moved directly to using contactless technology for physical security, bypassing magnetic stripe (and prox) altogether."

But there are still problems for those who have an installed base of prox card users, says Roger Roehr, manager of the government vertical with Tyco Fire & Security's Access Control and Video Systems business unit, Reston, Va. "What I see in the corporate world is not so much making a switch to contactless as them saying, 'hey, we're going to unify our ID management system and put both 125 KHz prox and (13.56 MHz) contactless capability on the same card," says Roehr. "They'll reserve that mostly for biometrics because only contactless technology can store a template."

Companies looking to transition to a contactless access system need to consider not only their older applications but also how to integrate the newer systems and what system to choose.

That's why any conversions will take time and should be done in an orderly fashion. "The key to moving to contactless is to have a viable migration plan," says Roehr.

One transition plan might simply be to replace legacy readers with the newer multi-technology ones as existing readers go bad, says Roehr.

Then corporations need to look at what Bubany calls "the next frontier" which involves making the move to more processing power. That "will further drive the convergence of multiple applications on to a single card," he says, "keeping user information, financial data and company networks secure through multiple layers of identity verification."

When it comes to deciding whether to go with multi-tech cards or readers, Roehr thinks there are cases when one makes sense over the others. "You have to look at the deployed base and move on from there."

There are instances when both solutions are needed, says Roehr. "If you were a corporation moving into a brand new building and you rebadge all your people in that building, but you want to let your employees in from other buildings with older systems, then it makes sense to have multi-readers so they could use their legacy cards." Still those cards would be for those in low-risk areas.

Numbers matter as well. "The number of employees and amount of facilities requiring physical access control really determine which solution would be best for a company," says Bubany. "Many times we are seeing the use of both multi-technology cards and multi-technology readers deployed within the same company, tailoring the migration to the needs of each individual facility."

Making the switch can be tough, but the increased security received from contactless smart cards should be worth it. One of the major difference between prox and contactless is that every transmission with the contactless card is encrypted.

"If you have true encryption you eliminate the ability to do a replay attack," says Roehr. "With any other, you're passing the same information each transaction so you're replaying the attack, while encryption, made possible with contactless, supplies a random answer each time." It's the same philosophy behind contactless payments and why its proponents say it's so hard to capture a transaction since it changes each time the card is used.

But it's about more than using 13.56 MHz technologies for security, says Bubany. "Since the introduction more than 30 years ago of magnetic stripe technology to physical access control, it has provided the market with basic access control. In the 90s with the addition of prox, customers embraced hands-free operation and maintenance-free readers. With the turn of the century and evolving customer needs, the 13.56 MHz smart card technology addresses the convergence of multiple application solutions on a single card, providing security and privacy, for both the company and the individual user."

"People using 13.56 MHz contactless technology are looking for solutions that provide a higher level of security and privacy," says Bubany.

Whether the war is over or there are still some battles to be fought, the eventual outcome seems to be a world of contactless access control … it's just a matter of when.

Going INSIDE Contactless

Company has come a long way from seven guys wanting to make their own contactless chips

Andy Williams
Contributing Editor, AVISIAN Publications

INSIDE Contactless might never have seen the light of day had Gemplus 13-years ago accepted the suggestion of some of its engineers to begin producing its own chips. Gemplus, which later merged with Axalto to become the largest smart card producer in the world, said no and seven of its people walked away in 1995 to create their own company.

Didier Serra, INSIDE's executive vice president of sales and managing director for North America, was one of those seven. "You have to be a bit crazy sometimes. If you're not crazy you don't take the risk."

Serra might have been a little crazier than the others. He was just 25 at the time, his wife was pregnant and he had just bought a new apartment.

Still, Serra and his six compatriots were firm in their commitment – "passionate" as he later described it – to begin creating their own contactless chips.

Serra had been at Gemplus about two years when he made the suggestion to one of his co-workers, Jacek Kowalski, that the company should start making its own contactless chips. "We were buying contactless chips from this company and they weren't working very well. Kowalski said 'why not,' and we began developing our own chip after hours. We worked together for a few months and came up with a mini-business plan to present to Gemplus management," Serra recalls.

"Gemplus didn't believe we would be able to develop a contactless chip. They basically told us, 'no guys, we can't do it,' and they continued buying chips from the same supplier," Serra says.

So Serra, Kowalski and the rest – in fact, the whole design team – left Gemplus to form a new company.

What's in a name?

In the first few months of this company's existence, the seven struggled with what to call it. As Serra recalls, after some "brainstorming, we came up with INSIDE." It's always displayed in all capitals because it represents an acronym of sorts: IN is for "innovative," SI for "silicon" and DE for "device," as in "innovative silicon device." But it can also represent technology that's "inside" any object, he says. In fact, that was the company's name for the first few years, INSIDE Technology, which gave way to "Contactless" in 2002.

After the company was created, Serra said the seven worked "day and night" to develop the technology, validate the chips to make them work and to have a product to demonstrate at the CARTES show in 1997, two years after leaving Gemplus. That first product was called Incrypt, "a memory product having a dual interface where you could read and write to the memory using either a contactless or contact interface," says Serra.

It was meant to serve as an "interim step" between contact and contactless to help with the migration from the older technology to the newer one that was just making itself known. "We're a strong believer in contactless technology and our idea was to eventually convert all the contact cards to contactless," says Serra.

While products, or at least a product, started to flow, the money wasn't. As with any new startup, cash flow was tight, Serra admits. "The first year, we started with our own money. We went back to our families to get all the money we could get," said Serra.

They quickly realized it would take more money than what they could raise among themselves, which meant seeking out investors. But with the pedigree behind INSIDE Contactless, finding investors wasn't a big problem.

inside CONTACTLESS

"We're a strong believer in contactless technology and our idea was to eventually convert all the contact cards to contactless,"

Didier Serra
INSIDE Contactless

INSIDE's first venture capitalist was Alta Berkeley, a European technology investor that is still with the company today. Other INSIDE investors are quite well known in the industry, such as Nokia Growth Partners, Visa Ventures, HID Global, Motorola Ventures and Samsung Ventures.

"We all left Gemplus and we've always been very, very close. When the market wasn't there, you had to be close to go through the good and bad to keep the company alive. We had tight cash flow and we had to sell our story to investors and tell them why they should believe in us. You can only make this happen if you're passionate. We worked together … cranking away to make it happen. Did we ever anticipate it would be successful? Absolutely yes. Right from the start we were all certain."

Remy de Tonnac, INSIDE's current CEO and another Gemplus veteran, came on board two-years ago to replace Kowalski. de Tonnac was INSIDE's chairman at the time because he was a partner in the venture capitalist firm Vertex Management Funds, another of INSIDE's investors. Prior to joining Vertex in 2001 de Tonnac was with Gemplus, where he held several positions, including CEO of the company's Americas operation and CEO for Gemplus Asia Pacific operations.

The original seven

INSIDE's original founding members include: Bruno Charrat, chief scientist and vice president of the NFC product line; Didier Serra, executive vice president of sales; Eric Bouyoux, IC design senior engineer; Michel Martin, design manager; Sean Commercial, platform support manager; and Olivier Adjemian, CAD (Computer Aid Design) and network manager. Jacek Kowalski, INSIDE's CEO, left two years ago to create another company, Twinlinx, geared towards development of near field communications projects.

The products still being sold today

In the beginning, INSIDE wanted a product it could sell. While it took a couple of years to get the product to market, getting it used – or sold – was another matter.

"Initially we were thinking we would be successful even faster then we eventually were because we believed then that if we had a product that works we could sell millions," says Serra. "But we quickly learned that if you don't have bigger corporations deploying your technology it's difficult to sell the product."

What helped INSIDE was its ability to align itself with some key companies in the industry, such as HID Global and credit card giants MasterCard and Visa.

After Incrypt, which is no longer around, INSIDE in 2000 developed PicoTag, an ISO 15693 chip designed for access control. But in an industry quickly moving towards the shorter read range 14443 standard, INSIDE realized it had to keep pace. That led to the development in 2002 of PicoPass, a chip compliant with both 14443 and 15693 standards. "The same chip can handle both protocols," says Serra.

Standardization was also important. "Back in 1997 we decided to align ourselves with ISO standards, because if you're not, you'll do nice in a niche market but you'll never go mainstream," says Serra.

When PicoPass came to market in 2002, INSIDE landed that first big company, HID Global. "We signed a license agreement with HID, base lining their iClass line on PicoPass."

PicoPass securely manages up to 16 independent applications from a single platform. Besides its use in HID's iClass access control cards, the platform is also usable in transit, identification, ticketing and other applications.

MicroPass came online in 2005 and shot INSIDE to the forefront of the payments market. Developed about the time contactless payment technology was starting to take hold, MicroPass is a microprocessor-based product with greater flexibility and more memory, says Serra.

Support for multiple payment brands – MasterCard's PayPass, Visa's payWave, and Discover – were built in. It has been so successful that 80% of contactless products in the U.S. are based on it, says Serra.

R2R or NFC?

Also during this time INSIDE had developed its Microreader technology that would enable a cell phone to become a payment device as well as a reader. INSIDE called the technology reader to reader, or R2R, Serra says. At the same time Sony and NXP were touting near field communication.

"In the past couple of years we've combined our reader technology into one chip called the Microreader," Serra says. "We have one of the patents on this technology and that was before NFC came to market."

For a time there were two competing standards – the one offered by INSIDE and the other developed by Sony and NXP. "The market did not need two," says Serra. "We stopped promoting R2R and since then we've worked a lot with the NFC Forum to develop this standard and all the protocols." But the philosophy behind INSIDE's R2R technology remains. "Our concept was for it to behave like a reader or a card," says Serra.

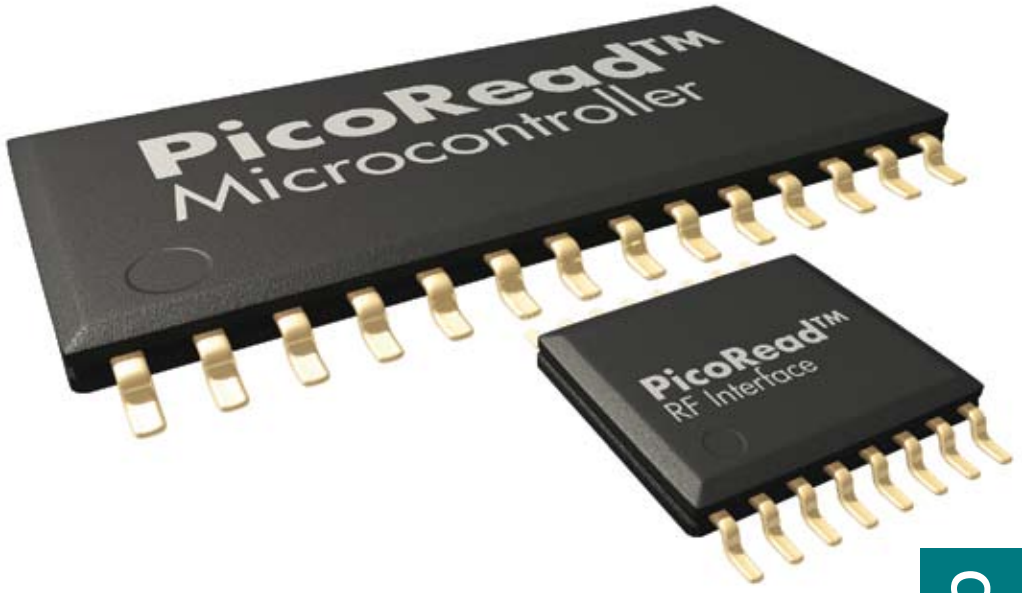
Last year, INSIDE's MicroRead, the company's third-generation NFC platform, was launched. MicroRead includes the microprocessor, operating system, and application in a secure and compact footprint.

By 2005, INSIDE realized it had to rein in its operations, to focus on its core markets. Charles Walton, INSIDE's executive vice president for payments, was brought in to help transition the company "from operating in a lot of markets to a company focused on fewer big markets," says Walton.

One of those markets is in the payments arena, which INSIDE pretty much owns, Walton says. And he see several challenges ahead for INSIDE in this area. "The U.S. payments market is growing and it has always been a challenge

"Our chips are optimized for payments, but what we're starting to see is a need for a lower-end chip for an ID, for driver licenses and border crossing cards,"

Charles Walton
INSIDE Contactless



to keep the quality levels up," he says. "We see a lot of applicability to this platform such as transit and access control markets and our challenge is growing our business into these converged markets."

He says INSIDE has also been toying with producing a contactless sticker, about one inch by two inches, for cell phones as an interim step until more NFC-compliant phones are released. "We're starting to hear from issuers that they are interested in the sticker," says Walton. "We've provided stickers to some issuers to play with and we're in the midst of commercializing it with a card manufacturing partner."

With EMV technology taking hold in Europe, Canada and Mexico, INSIDE is also deploying a chip for those markets. "But it's a little different, it will have a contact and a contactless interface," says Walton.

Lightweight identity

While INSIDE has shied away from traditional government ID programs, such as passports, the company has seen an area in this market that may be under-served. "We choose three or four years ago to focus on payments because passports generally require more storage," says Walton. "Our chips are optimized for payments, but what we're starting to see is a need for a lower-end chip for an ID, for driver licenses and border crossing cards," he says.

INSIDE calls it an "ICAO-lite" version, after the International Civil Aviation Organization which set standards for e-passports and e-visas based upon the use of contactless chip technology. INSIDE's MicroPass can create a mid-range series of ID cards and documents that meet ICAO standards, but don't include as much data storage, which means they won't cost as much.

"It's a new area for us, something we're starting to look at now," says Walton. INSIDE in late September, made the first announcement about its light identity version.

A view from the INSIDE

Today, INSIDE holds 55 international patents and is still headquartered in Aix-en-Provence, France where it was founded. The company also has locations in Warsaw, Singapore, Seoul, Shanghai, Silicon Valley and Boston.

INSIDE, a privately held company, doesn't release revenue figures but just looking at its most recent milestone – the delivery of 100 million chips – it's obviously growing. INSIDE and its 150 employees have worked directly with manufacturers' customers to pilot new contactless products and drive adoption of contactless technology. It has partnered with some of the largest handset manufacturers to integrate INSIDE's NFC technology into their handsets. NFC trials using NFC chips, are currently underway in Australia, France, Ireland, Korea, Malaysia, Norway, the Philippines, Singapore, Taiwan, Turkey and the U.S.

INSIDE is also an active participant in several industry alliances including the NFC Forum and the European Telecommunications Standards Institute aiming to develop standards to assist in NFC adoption and deployment and a member of the Smart Card Alliance.

It has received recognitions from research and consultant company Frost & Sullivan, including its 2008 North American Contactless Smart Cards Growth Excellence of the Year Award for INSIDE's role in shaping contactless payment technology, for contactless innovation in 2007 and for the best contactless product, MicroPass, in 2006. It also received technology magazine Red Herring's Top 100 most "Most Promising" Companies Driving the Future of Technology honor in 2007 as well as the Sesames innovation award for best hardware, MicroPass.

All this goes to show that INSIDE has come a long way from that day 13-years ago when seven men left the security of a paycheck to start a company that, while they had no doubt would succeed, they knew deep down that that optimism was probably their "passion" talking. It was all they had at the time. But it was obviously enough.

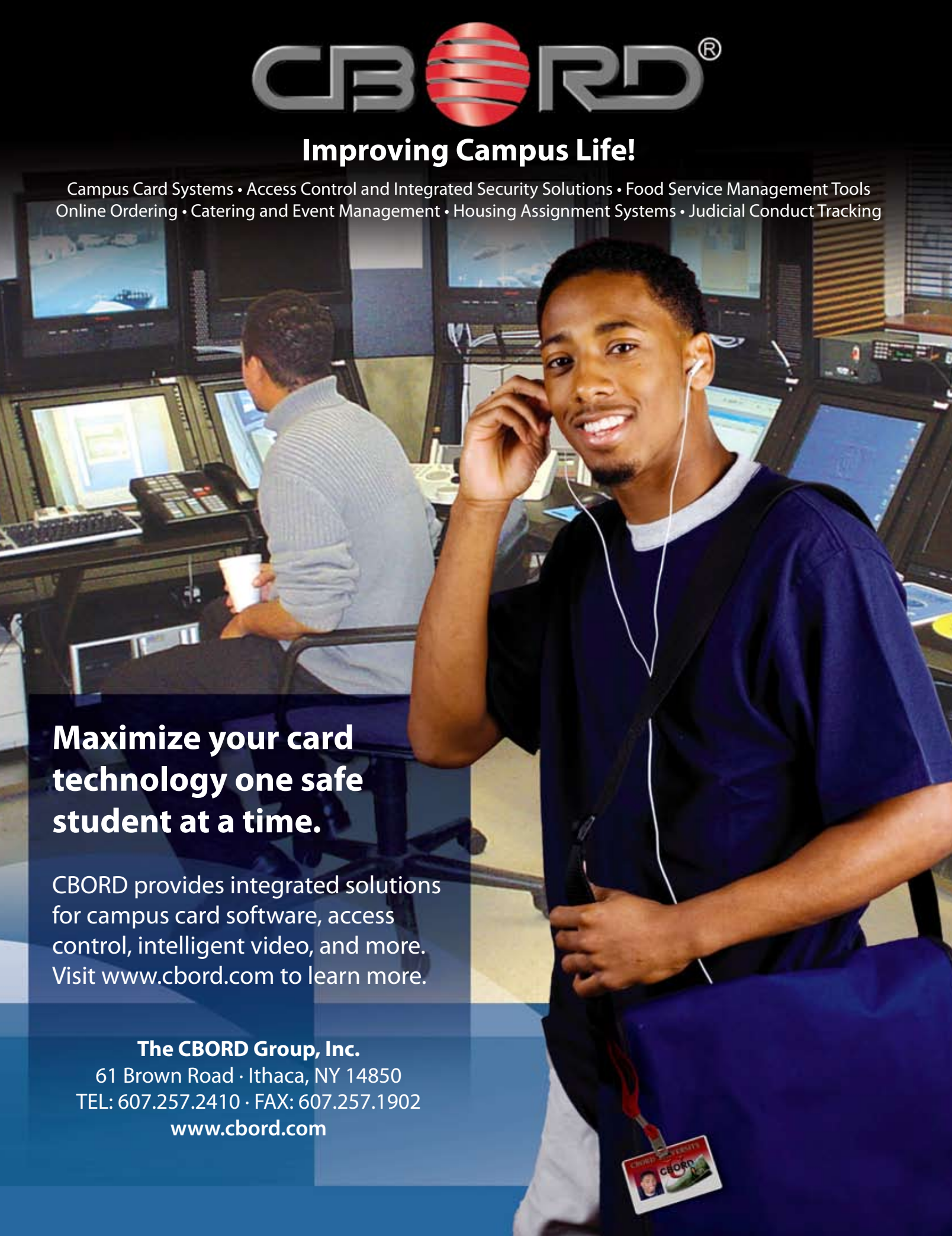
PCI regulations cast shadow over campus payments

Universities need to be aware of security requirements for payment card data

College and university campuses need to be aware that different portions of their computer networks may need to be secured because of requirements from the payment card industry. Payment Card Industry Data Security Standards (PCI DSS) are often overlooked by campuses, but the pressure to comply is mounting.

PCI DSS pertains to anyone who accepts credit or debit cards and governs how transaction data is stored and transmitted. If organizations don't protect payment card information and a breach occurs it could result in fines from the card associations. That is what J. Ashley Ewing, director of information security and compliance at the University of Alabama, told participants in a recent PCI web conference hosted by the National Association of Campus Card Users. In 2006 alone Visa issued merchant fines totaling $4.4 million across all industries.

The fines from the payments card associations aren't the only costs associated with data breaches, Ewing says. A small breach can cost an institution $1 million, with the average cost reaching $182 per impacted account. This includes the cost of notifying those affected, paying for credit monitoring and unauthorized charges. "There's also the additional cost of unfavorable publicity and significant brand damage to the institution," he says.


CBORD®
Improving Campus Life!
Campus Card Systems • Access Control and Integrated Security Solutions • Food Service Management Tools
Online Ordering • Catering and Event Management • Housing Assignment Systems • Judicial Conduct Tracking
Maximize your card technology one safe student at a time.
CBORD provides integrated solutions for campus card software, access control, intelligent video, and more. Visit www.cbord.com to learn more.
The CBORD Group, Inc.
61 Brown Road · Ithaca, NY 14850
TEL: 607.257.2410 · FAX: 607.257.1902
www.cbord.com

12 Steps to PCI Compliance

Build and Maintain a Secure Network
Requirement 1: Install and maintain a firewall configuration to protect cardholder data
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data
Requirement 3: Protect stored cardholder data
Requirement 4: Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program
Requirement 5: Use and regularly update anti-virus software
Requirement 6: Develop and maintain secure systems and applications

Implement Strong Access Control Measures
Requirement 7: Restrict access to cardholder data by business need-to-know
Requirement 8: Assign a unique ID to each person with computer access
Requirement 9: Restrict physical access to cardholder data

Regularly Monitor and Test Networks
Requirement 10: Track and monitor all access to network resources and cardholder data
Requirement 11: Regularly test security systems and processes

Maintain an Information Security Policy
Requirement 12: Maintain a policy that addresses information security

Source: PCI Security Standards Council

Educational institutions seem to be particularly vulnerable to some of these breaches. Thirty-three percent of reported data breaches occurred at educational institutions, Ewing says. "There's a lot more businesses out there than educational institutions," he says. "We have a disproportionately high hit rate."

There are a number of ways campuses can be impacted by PCI, Ewing says. Anyone or any system that deals with payment cards must know how to handle the information. Not only do the point-of-sale terminals in cafeterias need to be secured but the individual taking donations over the phone from alumni also needs to know how to securely handle payment card data. "Everyone who takes credit cards on behalf of the institution is affected by PCI," he says.

Depending on the type of ID the campus issues, it could fall under PCI too, says Joel Weidner, director of information systems for Penn State University auxiliary and business services. If the card has a MasterCard or Visa logo PCI standards must be met. If a campus ID is tied to a bank account but a PIN is necessary – in other words it is not an MasterCard or Visa branded product – the regulations are different and PCI does not apply.

But even if it doesn't, PCI may pertain to areas where the student ID is used, Weidner says. If a point-of-sale terminal accepts both student IDs and credit and debit cards PCI regulations need to be followed. "Understanding your environment is critical to compliance," he says. "Campuses need to understand what parts of the infrastructure need to be protected."

Even if a campus outsources all of its card processing, officials need to make sure that vendors are complying with PCI regulations or they can still be held liable, Ewing says.

Campuses that enable students to use IDs at off-campus merchants need to perform due diligence too, Ewing says. Those vendors need to be questioned on how they handle payment card information to make sure they comply with security standards or the university could be held liable if there's a breach.

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

Standardizing the issuance of non-standard card sizes

If you want to print to a standard CR80 plastic card – your average campus ID card or credit card – there are plenty of printers from which to choose. But what about a non-standard size cards, say an oversized CR100 or a smaller CR79 card?

CR100 cards are 3.88 inches by 2.63 inches (98.5 mm x 67 mm). Compare that with the industry standard CR80 ISO standard card, which is 3.370 inches by 2.125 inches (85.6 mm x 54 mm). Shave a couple of millimeters off that card and you have a CR79, 3.3125 inches by 2.0625 inches (84.150 mm by 52.400 mm), also considered non-standard but which can be handled many times by existing card printers if they can be adjusted to print to the slightly smaller card.

What's considered a non-standard card? "Anything that's outside the industry standard 30 mil PVC, CR80 card. That means thin cards, CR100 cards, rewritable cards and adhesive-backed cards," says Apryl Erickson, senior channel marketing manager for Fargo products at HID Global.

While the choice of printers is diverse for the standard CR80 cards, if you want to print a CR100 card, you really have just two options: buy a printer that's specifically designed for that type of card or outsource the job.

HID has a Fargo printer that produces CR100 cards, which are 42% larger than CR80 cards. "The HDP600 prints standard sized cards, but to reliably print an oversized CR 100 card, we modified the print engine to accommodate and produce the HDP600 CR100 Printer with a larger card path," says Erickson.

The need for these printers are in markets where it's necessary to quickly and easily to view the information on the card. "The demand is definitely coming from niche markets," says Erickson. "The main applications we see are largely event-driven, like political conventions, concerts or golf tournaments, and also the airport market where it's helpful to quickly and easily verify that personnel belong there."

An airport needs more than just a larger than average card. They need security on that card as well. Adding a secure holographic overlaminate to the CR100 card with the Fargo HDP600 provides protection from forgery.

In addition, the High Definition Printing technology used by the HDP600 CR100 makes any tampering with the oversized badges evident. If someone tries to alter a badge by peeling apart its layers, the printed image is destroyed, because it is sandwiched between the card and film.

The HDP600 CR100 can also print on both sides of a badge in one pass. Dual-sided printing can be an important security feature since counterfeiters don't often get a good look at both sides of a card.

"There are other oversized printers, some of which you can send a larger card through, but you're only able to print onto a smaller area of the card," says Erickson. "The card is still large, but the printing area is not. With the Fargo HDP600 CR100, you can make the print or photos as big as the card. Because printing is over the edge, there is no printless border."

Event management firms also have interest in the CR100 cards. Big events are also an attractive target for ID badge counterfeiters. But with Fargo's optional lamination module, the HDP600 CR100 can add a holographic over-laminate for additional protection from forgery, tampering and routine wear and tear. An overlaminate can also make badges more durable, which can reduce the costs of rebadging.

For example, two years ago Iowa State University hosted the Special Olympics. "We provided them a CR100 card printer from Fargo because that was the only printer that could print in a mass production way for thousands of kids, says Mark Degan, ColorID's corporate marketing manager. Football and other sporting events are also trying to use a CR100 card because it stands out.

Reusable, smaller cards

HID's DTC400e printer can also handle "breakaway cards". Usually printed on CR80-sized cards, breakaway cards become multiple cards that can be attached to key chains and are used by supermarkets or other retailers for loyalty programs. "Since these cards are smaller in size, it's more likely the patron will carry the card with them and thus more likely they'll take part in the loyalty program, much to the delight of the issuing organization," says Erickson.

Besides the DTC400e, which starts at $2,895, Fargo also offers an economical, entry-level version, the Persona C30e, which starts at $2,295. The main difference is that the DTC400e is equipped with a LCD screen. "Both printers combine a number of interesting features. You're able to

print thin cards, rewritable cards, adhesive-back cards, as well as print and encode smart cards," she adds.

Health care is the big market for thin cards, says Erickson. "We're seeing a lot of health care organizations moving from paper cards to a more durable yet still thin, plastic card."

The reason for the thinner cards is simple. They're more malleable and take up less room in a wallet. "Wallets are starting to fill up with CR80 cards, so organizations are smart to turn to thin cards for their various applications," says Erickson. Popular applications for thin cards include those used for transit passes, membership cards and loyalty cards.

While Fargo may hold a lock on the CR100 card printing, several companies supply printers that can handle other non-standard sizes, such as adhesive stock and CR79 cards.

Principally designed for non-permanent employee badges, adhesive-backed CR79 cards are used to personalize expensive technology cards, such as proc and contactless smart cards, that can then be reused. After printing is completed, that portion is removed and adhered to a technology card used for access control. After the temporary badge is done being used, the adhesive can be peeled off the base card and tossed and the technology card reused.

Another form of a non-standard card is defined by the material used to produce it, says Cunningham. DIS printers can print to biodegradable card materials, such as ABS, Polycarbonate, non-PVC coated corn cards and 100% polyester. "This gives our end users the ability to produce cards that can last up to 10 years without posing an environmental risk."

Evolis offers a single-sided card printer that can print on CR79 cards, says Jean-Charles Pichon, sales manager at Evolis. Priced at $2,310, the printer can also handle thinner cards, down to 10 mil, and adhesive backs.

However, he adds, such a printer has to be special-ordered to accept the smaller sized cards. "The modification is done in the feeder and the card guide located inside the printer," says Pichon. Regardless, he adds, the Pebble CR79 can still accept and print on regular CR80 cards.

As to who is buying these types of printers, Evolis' experience is similar to that of Fargo and DIS. "Our distributors are selling those printers to companies that need to print adhesive cards for access control applications," says Pichon.

"We do not have a printer that prints on cards larger than CR80, because the market for them is significantly smaller, and there aren't many (if any) oversized cards with embedded technologies, which is becoming our primary focus," says Shane Cunningham, marketing manager for the U.S. and Canada for Digital Identification Solutions.

DIS can print on CR79 sized cards, such as adhesive skins for clam shell cards, the thicker cards that contain a prozimity coil. "But since they are so easily removed and pose a legitimate security risk, we don't recommend them," he adds. "What's the point of adding security features in a skin that you can pull right off the encoded card body and replace with another?"

Cunningham points to the company's Professional Line printers that can handle thicker or thinner cards, instead of larger or smaller cards. "Our XID retransfer printers can print on cards as thin as 8mil and as thick as 78mil, which means we can print directly onto the surface of HID clamshell cards without the need for an adhesive skin, which could be peeled off and replaced at whim," says Cunningham.

"I often have prospects come to my booth at shows and tell me that they want to be able to print on skins that they can stick to their $20 HID cards, because it saves them money. Most of them have zero security features on the card itself and can have the simple logos, photos and data that are currently on their skins printed by any number of other printers. Once I tell them that I could take their cards, tear their adhesive skin off, replace it with my own and then be waiting for them in their office when they come to work the next day, they see that saving $20 by reusing the same clamshell card over and over again can cost them a lot more than a few dollars."

DIS printers can also print on cards that may be thicker due to multiple technologies being included on the same card, such as an RFID antenna, a contact chip, and a magnetic stripe. "We offer multi-function inline encoders that can handle all of the encoding/reading of those technologies internally during the same print process."

So, it's not just size of the card buyers need to think of when purchasing a card printer, thickness and materials matter as well.

Recent Advances in RFID

Jerry Banks
Co-author of RFID Applied

This article is based on a presentation made on June 5, 2008 at a kickoff meeting of a new RFID center. The author agreed to talk on the topic of recent advances in RFID. To accomplish the desired result, the RFID literature was monitored almost daily for the prior three months in search of advances in the technology.

First, we need to discuss what is and what is not an advance from the author's perspective. Advances are hardware or applications that seem out of the ordinary. So, one person can read the report of some new tag and not be surprised, while another person will be surprised. Or, the reverse of that situation can occur.

Advances in tags

With respect to tags, the most surprising occurrence in the past few months was that Mojix unveiled the details of a customer field trial program involving more than a dozen companies utilizing its EPCglobal Gen2- and FCC-compliant STAR reader system, which can read passive RFID tags from distances up to 190 meters. Some of the features of the STAR reader system are as follows:

- 100,000 times the indoor receiver sensitivity of previous RFID solutions
- 20 times the read range of conventional passive RFID readers
- 100 times greater coverage than conventional systems
- Verification of 100 percent of tags on RF-challenged goods
- Non line-of-sight read capability
- One multi-purpose system to read, locate and secure RFID tag data.

When the notion of a passive RFID tag being read at a distance of 190 meters was put to one of my co-authors of *RFID Applied*, he called it "bogus." That's a colloquialism for "fake" or "untrue." But, the Mojix system won 'Best in Show' at RFID Journal Live, held April 27-29, 2008 in Orlando, Florida. So, there must be something to it!

A popular tag is the Alien Squiggle. It has been mentioned in this series previously. We mentioned that it could be read at a distance of 19.4 meters in one test. So, you can see the relative difference in distances for a popular tag and for the Mojix system.

Recently, we were again experimenting with the Alien Squiggle tag. The best read occurred when the tag was perpendicular to the reader called 'face-on,' in this case the reader was a handheld Motorola device. The tag could not be read easily when it was on its side, or, 'edge-on.' But, the Avery Dennison AD-631 inlay is orientation insensitive, so it can be read in any direction (face-on or edge-on) which improves tag visibility in randomly oriented asset and

Exhibition & Congress

November 4-6, 2008

Paris-Nord Villepinte Exhibition Centre-FRANCE

- E-TRANSACTION
- SECURE SOLUTIONS
- ID MANAGEMENT
- CONTACTLESS
- STRONG AUTHENTICATION
- BIOMETRICS
- EID
- SECURITY
- ACCESS CONTROL

SECURE TECHNOLOGIES AND BIOMETRICS EXHIBITION

iD IDENTIFICATION

FOCUS USA NATION OF HONOR

Showtime for IDentification!

The widest international offer
Dedicated conferences

Co-located with

CARTES 2008 — 23 Years Supporting the Smart Card Industry

Participate in the major event of your profession

www.identification-show.com

Your FREE badge* on www.identification-show.com with this code: IDK01

AND PREPARE YOUR VISIT:

Exhibitors list & news • Special events • Congress registration • Practical information

* Pre registration fee: € 50 incl. taxes
On site: € 70 incl. taxes

The World Leading Event in Digital Security & Smart Technologies

An event organized by comexposium

CARTES & IDENTIFICATION 2008
70 avenue du Général de Gaulle
92058 Paris la Défense Cedex - France
cartes-id@exposium.fr

pallet tracking applications. Avery Dennison says that the tag provides also a longer read range yielding greater readability rates.

Another concern with tags is the amount of memory available. By the end of June 2008, Fujitsu announced that they would have a Gen2-standard RFID tag with 64 kilobytes of FRAM, which it claims is the highest-capacity Gen2 tag available. FRAM is Ferroelectric Random Access Memory (also referred to as FeRAM). FRAM uses ferroelectric film as a capacitor for storing data. Featuring advantages of both ROM and RAM devices, FRAM devices have high-speed access, low power consumption, and high endurance for numerous rewrites. Fujitsu is initially marketing the tag for aircraft maintenance applications.

Omni-ID now produces fully converted, ready-to-use RFID tags specially designed to perform well around liquids and metals. While an increasing number of tags have been introduced on the market that make the same claim, a key differentiator of Omni-ID's QinetiQ tags is that they perform well when *not* around liquids and metals as well. The tag has a conductive substrate that creates an electromagnetic field around the chip when the tag is interrogated.

In mid-February, 2008, STMicroelectronics announced that they had combined near field communications reading, processing, and memory functions into a single chip. The device has standardized NFC reading capabilities, 112 kilobytes of user ROM, 4 kilobytes of RAM, plus controller functionality and software in a single .13-micron chip that can function as both a reader and a tag. The product is intended for integration into cellular phone handsets and other devices. An example application is contactless payments.

Item-level tracking

We leave the discussion of tags to discuss item-level tracking, i.e. placing tags on every item. This is related to the section above, but we will return to that after we discuss this topic.

The concern about item-level tracking has been the cost of the tags. For example, is it a wise idea to put a $0.10 tag on a $0.90 can of beans? That excess can't be justified. Somehow, merchants have found, or are investigating the, economic justification in placing tags on every item. The items mentioned are all worth more than a can of beans, and some of the examples are older than three months.

Beginning in May of 2008, retailer American Apparel rolled out an item-level RFID inventory tracking system in its 17 New York stores. The roll out will be complete in July 2008. The inventory process typically occupies four employees for eight hours. At the RFID-enabled Columbia University-area store, it takes two employees just two hours to take inventory. This savings from 32 person hours down to four person hours is in line with other reports that have been received.

As previously reported German department store operator, Karstadt, with 86 department stores and 32 sporting stores, tagged selected items of men's apparel in a six-month pilot study that was launched in September of 2007. The tagged items were read at five points in the process:

- Upon receipt at the store
- Between the back room and the store floor
- On the shelves
- At the point-of-sale
- During inventory (by store staff using mobile readers).

Karstadt hopes that the pilot study will demonstrate:

- A dramatic reduction in the amount of time necessary to conduct store inventory
- Improved inventory accuracy, enabling misplaced items to be restocked faster
- Data about how often items are removed from their shelves
- Improved and automated shipment reporting, enabling errors to be discovered and corrected faster.

NP Collection from Finland expects full ROI in less than six months from a pilot program in which Gen2 tags were placed on 80,000 individual garments. The company plans to more than triple the number of garments tagged in 2008, add new inventory applications, and expand collaboration with suppliers and logistics providers.

METRO deployed an RFID system at their Galeria Kaufhof, high-end retail store, in Essen, Germany. It fully integrates many of the latest RFID retail applications including item-level tagging, supply chain visibility, back room inventory visibility, smart shelves, smart mirrors, point-of-sale information transfer and theft prevention. It is an end-to-end retail deployment all of which is based on Gen2 and related EPCglobal RFID standards.

As reported each individual package of fresh meat at the new METRO Future Store is labeled with a passive Gen2 RFID tag that keys applications to prevent the sale of outdated product and provide inventory information to drive replenishment and meat cutting operations.

Butchers at the store apply EPC Gen2 RFID smart labels to meat packages. Each package is identified and recorded when it is placed into the display case, which METRO calls the Smart Case. The implications for insuring the freshness of meat purchases and the taking of inventory with this system are vast.

Without going into detail on each of the latest RFID retail applications, we will discuss just one of them, smart mirrors. (Metro produced

a "gee whiz" video in 2002 that showed how many of these applications would operate.)

Let's say that a woman selects a black skirt and a white top, both RFID enabled, and takes it to a dressing room. She tries it on. She wonders how a purple top in the same style will work. She has logged her image into the mirror. Instead of changing back into her regular clothing, going out to find the purple top, returning to the dressing room (that could be occupied by someone else now!), and changing into the black skirt and purple top, she simply indicates that the mirror should reveal an image showing the black skirt and purple top. Voila! As if by magic, the image appears.

She can accept the combination (reject it, accept part of it, or, choose another combination) and the selected goods will be waiting for her at a designated location.

Organic ink

We are impressed with organic ink! We will be more impressed if it is implemented thereby saving much money for RFID tags. Parelec Inc. has developed ink chemistry that suspends the metallization in an organic carrier that decomposes after printing leaving a 99% pure metal coating. The company states that their organic ink is "3 to 10 times more conductive than polymer-based inks."

Kovio, a San Francisco firm, says that it expects to create printed-silicon high-frequency RFID chips by the end of 2008, paving the way to low-cost tags.

A*STAR Research, an institute sponsored by the government of Singapore, has developed capabilities in printed electronics. The Institute of Material and Research Engineering, a part of A*STAR Research, has received an injection of funding to further develop high performance functional materials for printed electronics such as semiconductors. SIMTech, another research institute sponsored by the government of Singapore, has developed capabilities in printing antennas for RFID tags. This is certainly an avenue for reducing the cost of tags.

In early March 2008, it was announced that a German government agency, the Federal Ministry of Education and five companies are jointly investing about $23.2 million in a three-year research project intended to develop better materials for printable RFID tags. The ministry provides almost half of the funds for the so-called MaDriX project with the remaining funds coming form German companies BASF, ELANTAS Beck, Evonik Industries, and Siemens.

Coradyn Biosystems is a smart sensor materials company developing responsive, conductive polymers for detecting biological and chemical analyses. In June 2008, the company announced licensing of responsive, conductive polymer technology from the University of Texas at Austin. Coradyn's preliminary results support the potential for use in molecular sensing devices in a wide array of applications including RFID and wireless sensing.

Real-time Location Systems

Aeroscout announced a series of partnerships and new software capabilities that use multiple real-time location system (RTLS) technologies in a single system. The technologies are Wi-Fi based RTLS and ultra-wideband RTLS.

A new mobility initiative from Cisco Systems includes support for features that enable real-time location systems (RTLS) to go beyond just reporting location to include information about a tagged object's work status, motion alerts, temperature, and input from other sensors. An application would be tracking infusion pumps in a hospital. The system would not only locate the infusion pumps (many do this already), but also determine if they are currently in use.

Securing RFID Systems

NeoCatena Networks plans to release a new product in June 2008 that will serve as a firewall to prevent fraudulent or malicious tag data from entering enterprise systems. The Silicon Valley startup was formed by a researcher who previously demonstrated that RFID passports could be cloned, and who maintains that most RFID systems used today are insecure. NeoCatena's core preventive product is RF-Wall, a firewall-like appliance, which integrates transparently into a given RFID system right after the RFID reader and in front of the backend (Edge Server or middleware). RF-Wall analyzes tag data before it reaches the backend and can block the tag if it poses a threat or let it pass through if the tag data is safe.

Applications

Now, we note some new uses of RFID. These applications don't necessarily use new technology; they just use existing technology in innovative ways.

- Ford's popular F-150 pickup trucks are now available with an RFID reader integrated in the bed to monitor cargo.
- The Army is testing an RFID-based sensor system to record and store how often the cannons on M1 Abrams tanks are fired. The data will support proactive maintenance operations and help the Army determine when the barrels approach their end-of-life and should be replaced.
- Engineers at Purdue University are creating a wireless implantable passive microdosimeter designed to be injected into tumors to tell physicians the precise dose of radiation received and locate the exact position of tumors during treatment. Clinical trials are scheduled for 2010.

Conclusion

RFID is advancing rapidly. As the literature is scanned, new items appear as if by magic. If this article is revised one year from today, its entire contents will be new.

This article is the tenth in an ongoing series that explains the principles of RFID. It was created for RFIDNews by Jerry Banks, Tecnológico de Monterrey, Monterrey, México. *The author is one of four co-authors of RFID Applied, John Wiley, 2007, ISBN-10 0471793655; ISBN-13 978-041793656.*

Casinos betting on RFID

From the gambler's perspective not much has changed. He walks up to the blackjack table, buys some chips and places a bet. But at 1,000 casinos in 20 countries there's a whole lot more happening on the back end.

More and more casinos are spending money to put radio frequency identification tags in gaming chips, says Bodo Ischebeck, vice president RFID and table management systems at Progressive Gaming International, Las Vegas. He expects 30 more casinos to begin using RFID chips in 2009.

"It's been difficult to track what's going on with the table games at any given moment," he says. "You only know how much you made by the amount of chips in front of the dealer at the end of the day."

Placing the RFID tags into the gaming chips enables a casino to track the revenue flow at any moment, protect against counterfeiting and internal fraud as well as help manage guest relations, Ischebeck says. He made the comments during a session in September at the Future of Secure Documents 2008 event in Chicago.

The technology used in the casino chip is a 13.56-megahertz PJM (Phase Jitter Modulation) tag invented by Australia-based Magellan Technology. Magellan licenses the technology exclusively to Progressive Gaming.

Tags are placed in each of the chips. Each table has a single RFID reader with antennas under each betting spot. Each table is also outfitted with a PC to monitor activity at the table, Ischebeck says. The system is able to monitor 1,000 chips per second. "It constantly scans the table to validate the RFID and track the chips' movements," he says. "It can track the chips in real time and the casinos know where chips are at any given time providing real time win/loss information."

The program also enables a casino to track players' bets, Ischebeck says. Most casinos have loyalty programs that reward players based on how much they bet and what games they are playing. The RFID-enabled chips make sure the player is rewarded accordingly.

The chips also make it possible for casinos to offer table jackpots and bonuses, Ischebeck says. "It offers higher entertainment and attracts more players to the tables."

The RFID-enabled gaming chips cost about $2 each, 40% of which is the RFID tag. But research has shown that casinos hit a break even return on investment in less than six months, Ischebeck says. □

INNOVATION REDEFINED

DATACARD® SP PLUS SERIES CARD PRINTERS DELIVER ENHANCED PERFORMANCE, SUPERIOR OUTPUT

NEW FEATURES

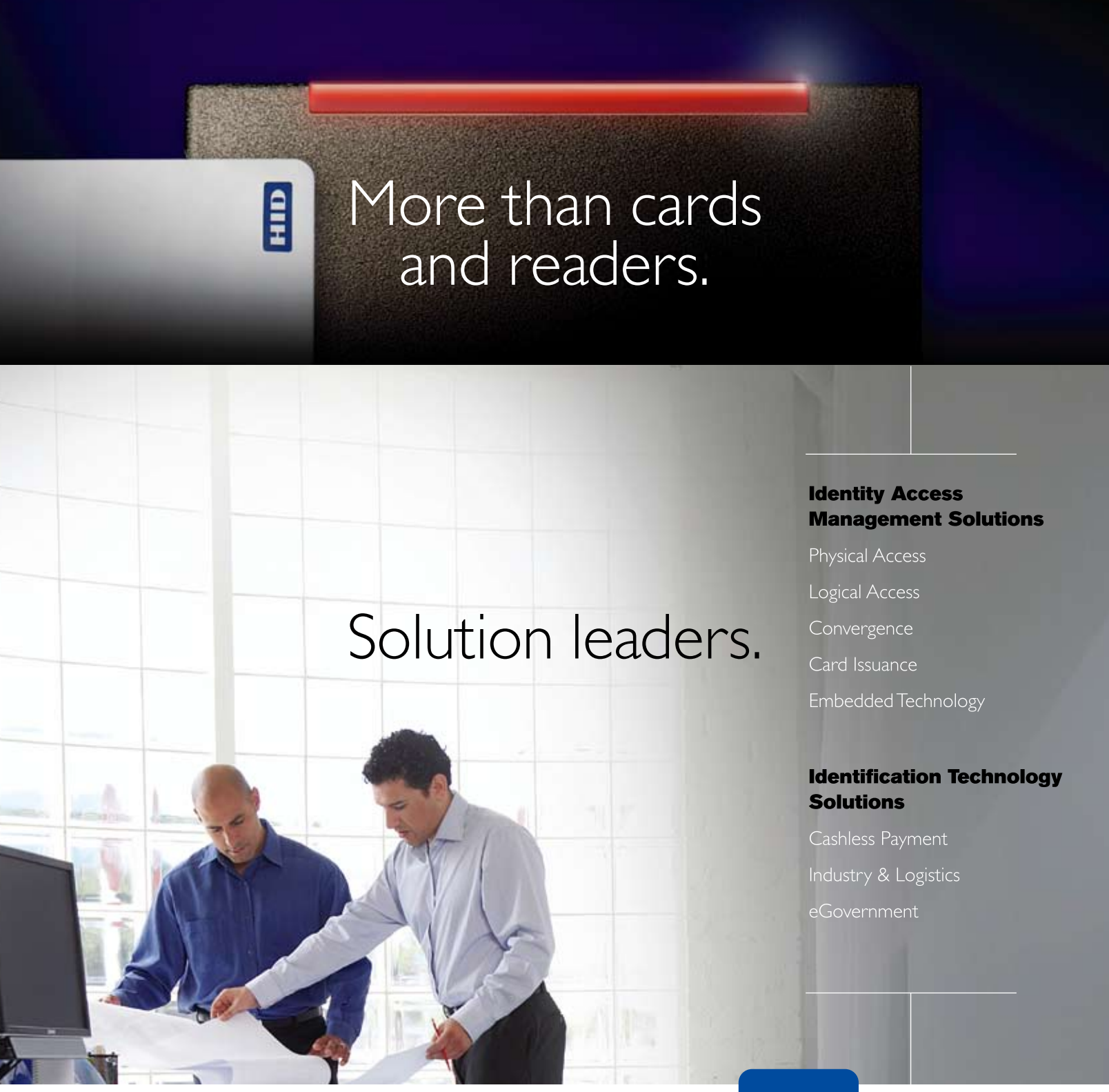
- FASTER OUTPUT
- SHARPER COLORS
- NEW SUPPLY CHOICES
- CLEAR CARD PRINTING
- EXTENDED WARRANTY

IMPROVE YOUR CARD PROGRAM

Datacard® SP Plus Series card printers provide outstanding reliability and superior card quality. This broad line of desktop card printers deliver proven performance, innovative technology and the capabilities you need to produce high-quality, secure cards for corporate, education, government, membership, retail and many other applications.

Learn more about the Datacard SP Plus Series card printers today.
Visit **www.datacard.com/spplus** or call **+1 952 933 1223.**

DatacardGroup
SECURE ID AND CARD PERSONALIZATION SOLUTIONS



More than cards and readers.

Solution leaders.

Identity Access Management Solutions

Physical Access

Logical Access

Convergence

Card Issuance

Embedded Technology

Identification Technology Solutions

Cashless Payment

Industry & Logistics

eGovernment

HID Global, the worldwide leader in access control cards and readers, now offers a comprehensive selection of secure identity solutions.

An innovator in access control technology, HID cards and readers are counted on every day by millions of people around the world. Now, we've expanded our offering to include everything from logistics technologies to the design and production of credentials to IP-based access control. We believe the future of secure access and identity lies in open platforms, "smart" technologies and rock-solid reliability. That's what our solutions deliver. So no matter what you need in secure identity solutions, you can count on HID to lead the way.

hidglobal.com

HID

ACCESS choices.