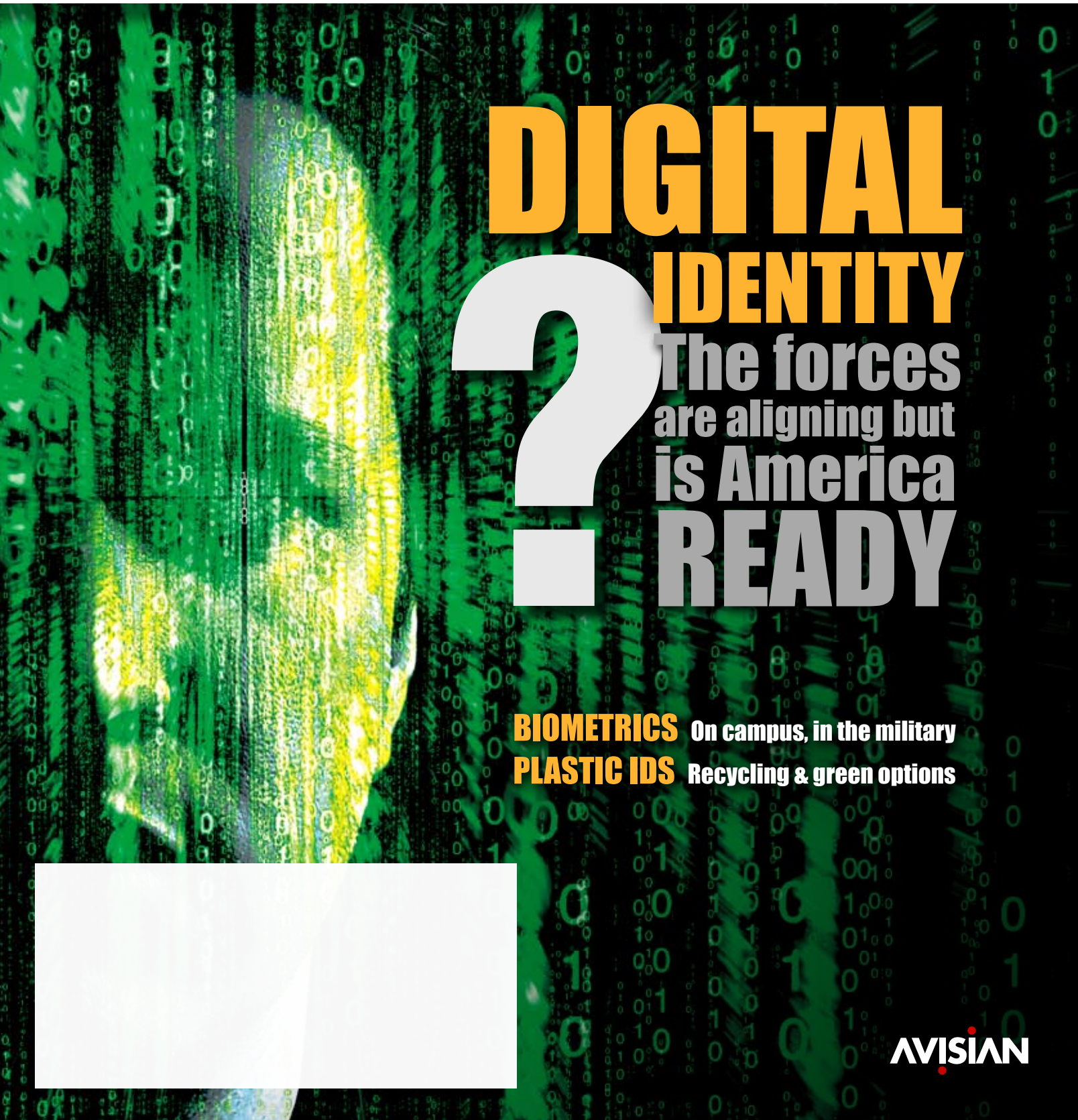
re:ID

Fall 2009

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



DIGITAL IDENTITY

The forces are aligning but is America READY?

BIOMETRICS On campus, in the military

PLASTIC IDS Recycling & green options

AVISIAN

CoreStreet

We Make Credentials Work

CoreStreet PIVMAN Solution for TWIC Compliance

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

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

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

No network connections. Just grab a handheld and go!

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

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

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

Resolve the **national identity crisis**

A trusted credential is essential to resolving the national identity crisis.

The ever increasing need to prove your identity requires a secure, personalized ID. Gemalto's smart card based solutions offer two factor authentication, enhancing your privacy in both the real and virtual world. Demand a secure credential and resolve the national identity crisis.

Learn how to own your identity at: **www.justaskgemalto.com**

www.gemalto.com

gemalto
security to be free

Contents

18
Online Identity
Strong authentication and identification may be just around the corner

26
First Responders
'Spring Ahead' demonstrates many technologies

34
Driver Licenses
New driver license legislation proposed

52
NFC
NFC aims to keep Pakistani children healthy

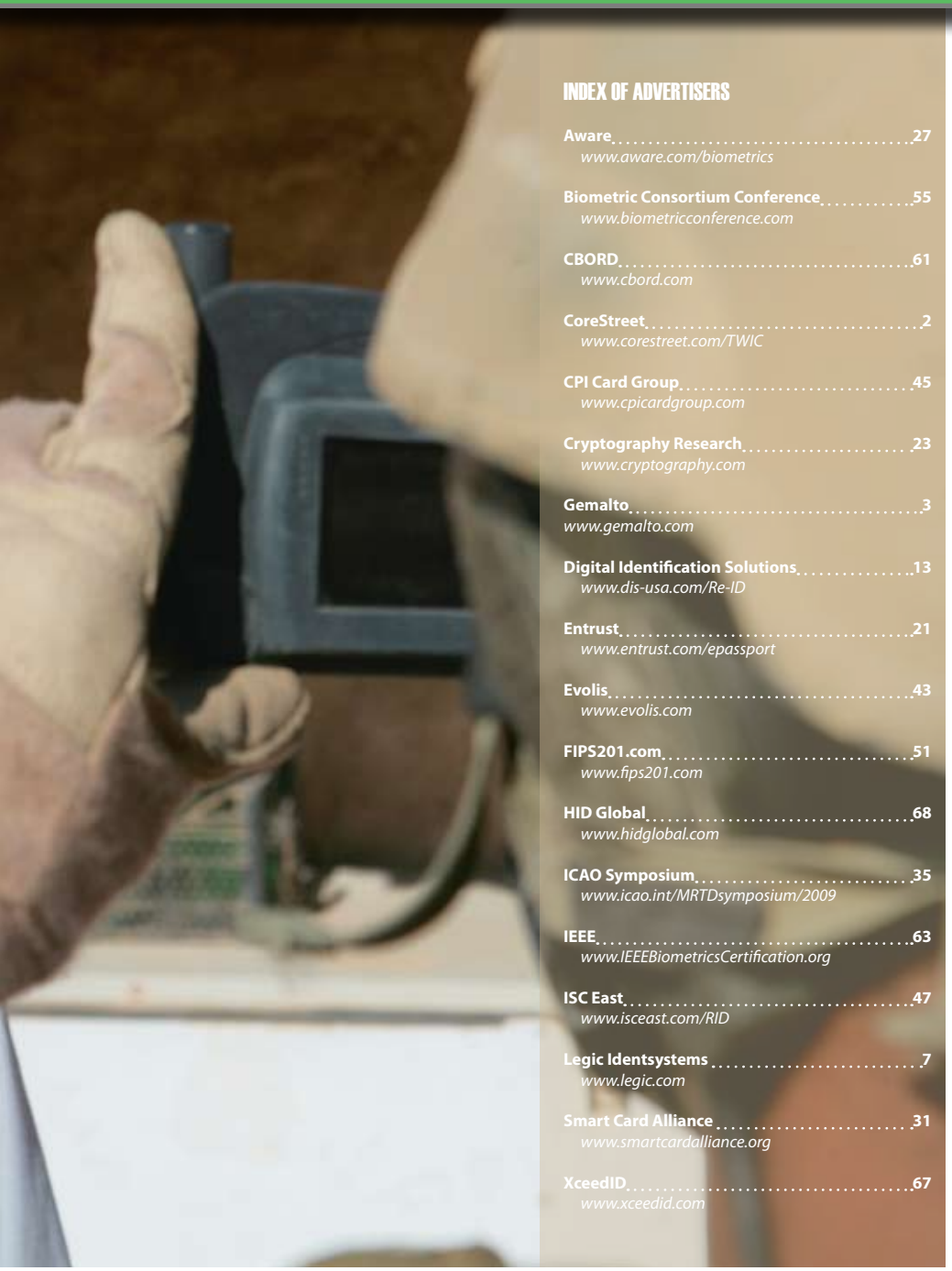
62
Biometrics
Biometrics and the Department of Defense

6 | OPINION | Now is the time for U.S. to issue high-assurance credential to public

8 | PODCAST | Conversations on the Kantara Initiative, PASS ID Act, Laser Engraving IDs, and Four Bridges Forum

10 | ID SHORTS | Key news items from AVISIAN's online ID technology sites

Fall 2009



INDEX OF ADVERTISERS

Aware 27
www.aware.com/biometrics

Biometric Consortium Conference 55
www.biometricconference.com

CBORD 61
www.cbord.com

CoreStreet 2
www.corestreet.com/TWIC

CPI Card Group 45
www.cpicardgroup.com

Cryptography Research 23
www.cryptography.com

Gemalto 3
www.gemalto.com

Digital Identification Solutions 13
www.dis-usa.com/Re-ID

Entrust 21
www.entrust.com/epassport

Evolis 43
www.evolis.com

FIPS201.com 51
www.fips201.com

HID Global 68
www.hidglobal.com

ICAO Symposium 35
www.icao.int/MRTDsymposium/2009

IEEE 63
www.IEEEBiometricsCertification.org

ISC East 47
www.isceast.com/RID

Legic Identsystems 7
www.legic.com

Smart Card Alliance 31
www.smartcardalliance.org

XceedID 67
www.xceedid.com

17 | CALENDAR | Industry events from the identity and security worlds

18 | COVER STORY | Online identification is coming, sooner than you may think

19 | DIGITAL SECURITY | Obama's Plan for securing the Internet

24 | ONLINE ID | Four Bridges Forum building bridges to identity

26 | FIPS 201 | PIV I enables states, others to issue high-tech credentials

26 | FIRST RESPONDERS | 'Spring Ahead' demonstrates interoperable credentials from federal and state issues

29 | CASE STUDY | Federally interoperable credentialing in Illinois

30 | LOGICAL SECURITY | Securing Macs with smart cards in a Windows environment

32 | REGISTERED TRAVELER | Does CLEAR's demise signal the end of Registered Traveler?

34 | DRIVER LICENSES | New legislation proposed to change REAL ID to PASS ID

36 | EDLs | How do EDLs fit in with new PASS ID bill?

37 | REAL ID | Some states on the way to REAL ID compliance

38 | ISSUANCE | Laser engraving IDs catching on

42 | TECHNOLOGY | Searching for 'green' card stock

44 | ENVIRONMENT | Card recycling has yet to take off

48 | TRANSIT | Riding Seattle's rails, ferries, buses, ORCA style

50 | OPINION | FIPS 201 and India National ID, interoperability anyone?

52 | NFC | NFC aims to keep Pakistani children healthy

53 | PRODUCTS | New Nokia phone heralds commercial NFC deployments

56 | LOYALTY | Loyalty goes high-tech with advanced ID technologies

58 | CONVERGENCE | The changing market for converged security products

60 | CAMPUS ID | Clap your hands for access

64 | BIOMETRICS | Biometrics and the Department of Defense

66 | BIOMETRICS | Facial recognition in Apple's iPhoto

Perspective

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

EDITOR
Zack Martin, zack@AVISIAN.com

ASSOCIATE EDITOR
Andy Williams, andy@AVISIAN.com

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

ART DIRECTION TEAM
Darius Barnes, Ryan Kline

ADVERTISING SALES
Chris Corum, chris@AVISIAN.com
Sales Department, advertise@AVISIAN.com

SUBSCRIPTIONS
Regarding ID is available for the annual rate of $39 for U.S. addresses and $87 for non-U.S. addresses. Visit *www.regardingID.com* for subscription information. No subscription agency is authorized to solicit or take orders for subscriptions. To manage an existing subscription or address, visit http://subscriptions.avisian.com and enter the Customer Code printed on your mailing label. 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.

Copyright 2009 by AVISIAN Inc. All material contained herein is protected by copyright laws and owned by AVISIAN Inc. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopy, recording or any information storage and retrieval system, without written permission from the publisher. The inclusion or exclusion of any does not mean that the publisher advocates or rejects its use. While considerable care is taken in the production of this and all issues, no responsibility can be accepted for any errors or omissions, unsolicited manuscripts, photographs, artwork, etc. AVISIAN Inc. is not liable for the content or representations in submitted advertisements or for transcription or reproduction errors.

EDITORIAL ADVISORY BOARD
Submissions for positions on our editorial advisory board will be accepted by email only. Please send your qualifications to info@AVISIAN.

Now is the time for U.S. to issue high-assurance credential to public

Zack Martin
Editor, AVISIAN Publications

There are a number of steps that can be taken to secure the Internet and stem the rising tide of identity theft. Offering citizens a high-assurance credential would be one step in the right direction.

Some interesting proposals are being floated around in Washington DC. Sen. Chuck Schumer (D-N.Y.) wants to create a system that would identify citizens for employment eligibility. He definitely wants to use biometrics, but whether or not a card would be involved hasn't been decided.

During a Senate Judiciary subcommittee hearing Schumer said if any type of system were put into place it would be mandatory and only used for verifying employment eligibility (See page 20).

Creating a credential that can be used as an extra security factor online, as well as employment verification, could help stop some of the rampant fraud and help individuals secure their identities.

While Schumer's plan has yet to be fully detailed, using just biometrics, making it mandatory and limiting its use to one thing would be mistakes.

Biometrics should be a component of the project Schumer is proposing, but using it alone isn't enough. Fingerprints, the most tested and widely deployed technology, still experience slight error rates. And while it may be a small fraction of a percent when it scales to more than a hundred million people there are going to be problems.

The project should use a smart card in conjunction with biometrics. The fingerprint template can be stored on the card, maybe even matched on the card, for a quick authentication and then checked against a database to confirm employment eligibility.

Making any type of identification system mandatory in the U.S. is going to run up against huge opposition from privacy advocates. REAL ID has been blasted as a national ID program by these groups and appears likely to be either repealed or severely watered down (See page 34).

Just mentioning a mandatory ID program in the U.S. will raise a red flag that people won't be able see past. By making the program voluntary the government can avoid the national ID label. Those who opt not to get the credential will have to show additional proof of identity in order to verify employment eligibility.

Still, verifying employment eligibility isn't enough to get people to buy into a voluntary credential. There must be something in it for the individual. Including a digital certificate on the card for identification online could be just what it takes to attract people.

Identity theft is a major concern among consumers and there's only so much that can be done to counter it without some type of viable digital identification. Offering this the government will be able to get buy in, show that the system works and offer a benefit that translates to wider acceptance from the public.

Function creep makes me laugh

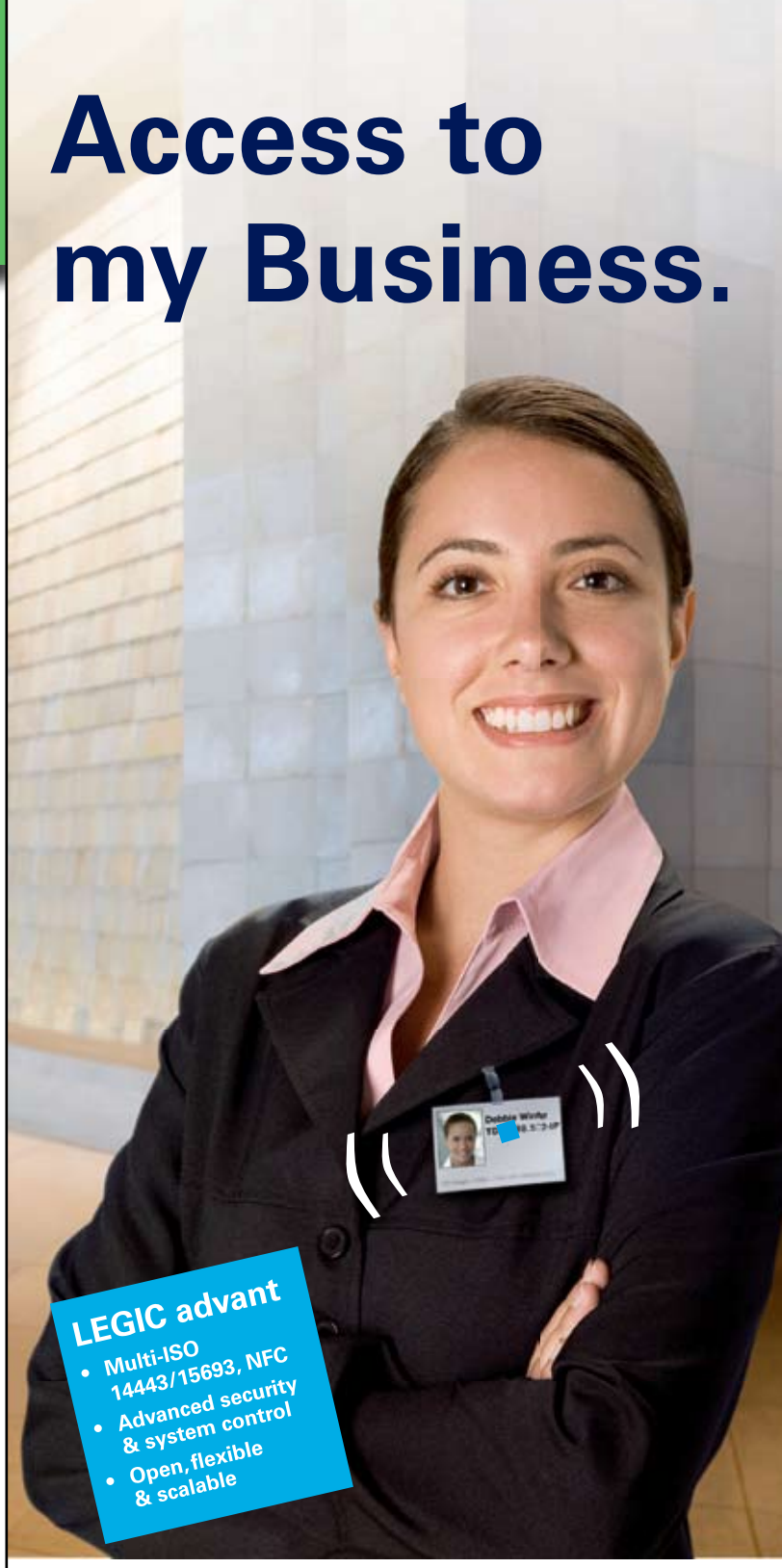
Politicians may want to limit the role of this credential for fear of function creep, where something is created for one purpose and it eventually is used for much more, i.e. state-issued driver licenses and Social Security numbers.

Both of those identifiers had very different original purposes than how they are used now. A person shouldn't have to show a driver license to get on an airplane or use a Social Security number to apply for a credit card but that's the way it is.

Instead of worrying about function creep give the credential additional functionality from the start. Creating a credential that can be used as an extra security factor online, as well as employment verification, could help stop some of the rampant fraud online and help individuals secure their identities.

Don't get me wrong, it will be an extremely difficult for something like this to happen. The American public will be skeptical, it will be expensive and there are challenges I haven't touched on … identity vetting? How will the credential work in an online environment? etc., etc.

But as the old saying goes, nothing worth doing was ever easy, right?



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

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

SPONSORED BY DIEBOLD

Episode 32: Online identity

Identity in the online world is difficult. Regarding ID podcast Editor Zack Martin spoke with Brett McDowell, executive director of the Liberty Alliance Project, about the Kantara Initiative, a plan to bring online identity projects together.

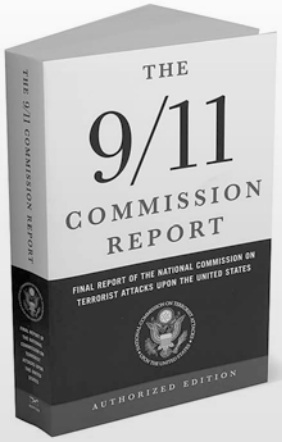
Highlights: "We're focused on interoperability at the protocol level. None of the solutions in the marketplace can solve the full Internet ID continuum," he says. "The stakeholder on any one solution is focused on solving that problem on his own and we now realize we have to work together to solve the problem."

"In the end the goal is for a person to assert their identity across the continuum. From your banks to your social network and working with the government and your employer."

Financial services companies will likely have a role in helping authenticate individuals. "You look at the banks and they authenticate everyone. They have an infrastructure and are regulated. Google and Yahoo have the users and they are authenticating people but they have no knowledge of who they are."

To listen, visit SecureIDNews.com/tag/Podcasts and select "Episode 32"

Episode 34: PASS ID Act



New legislation has been submitted in the U.S. Senate that would roll back parts of the REAL ID Act, including the identity vetting portion. Regarding ID Editor Zack Martin spoke with Janice Kephart, a member of the 9/11 Commission and director of national security policy at the Center for Immigration Studies, about the proposed law.

Highlights: "PASS ID guts the key element of the 9/11 Commission in regards to driver licenses, which is ID verification. PASS ID pulls the plug on people proving who they are."

"It's about creating an appearance of security without any real security," says Kephart.

"It pulls back on all significant areas of identity verification that REAL ID had honed in on. There's no cross checks to make sure people don't have multiple licenses in different states. The bill pulls back on all significant areas of identity verification."

To listen, visit SecureIDNews.com/tag/Podcasts and select "Episode 34"

Celebrating 150 Years of Innovation 1859 - 2009

Episode 35: Laser engraving ID cards

Often the focus is on how information is stored and secured in a card, but just as important is how information is secured on a card. Zack Martin, editor of Regarding ID magazine, sat down with Jonathan Bowen, sales manager at Digital Identification Solutions about its new desktop printer and its ability to laser engrave ID cards. The company is expecting to ship its first units this fall.

Highlights: "Those who have huge issues with forged and faked cards are our primary customers. Laser engraving makes it difficult to remove or alter the card information. The normal person who wants to fake the card won't bother with it, he'll move on to another target," says Bowen.

"It's also expensive enough to keep the criminal element away and technical enough to where if he got it he wouldn't know what to do with it," he adds. "When a state trooper pulls someone over and only has a few minutes to validate an ID the tactile feature is great. It's virtually impossible to forge on a desktop printer."

"Laser engraving is a security feature you can see with the naked eye and it's impossible to create with any other type of desktop printer," Bowen says.

To listen, visit SecureIDNews.com/tag/Podcasts and select "Episode 35"

Episode 36: Building a bridge for digital identity

How do we ensure online transactions? How do we know that the person on the other end of a transaction is who they say they are? How do we ensure that transaction without a high cost? These are questions the Four Bridges Forum wants to answer. Regarding ID Editor Zack Martin spoke with executives from half the Four Bridges Forum, Jeff Nigriny, from Certipath, and Mollie Shields-Uehling, with Safe Bio-Pharma, about the initiative and what they're trying to accomplish.

Highlights: "As we move into the digital world there are tremendous efficiencies to be gained from going electronic," said Shields-Uehling.

"We need interoperable trusted identity management standards and a digital signature linked to that identity so people can do business across that bridge."

"The identity fraud and social engineering attacks that we're suffering today, especially in online environments, are largely rooted in us not having transactions based on face-to-face proofing," Nigriny said. "Once you have the strong binding of a person with the credential, we will see a number of our Internet social ills literally evaporate over night."

To listen, visit SecureIDNews.com/tag/Podcasts and select "Episode 36"

Morehead State goes contactless with iCLASS and Odyssey PCS

"Tap and go" is the new mantra for students, faculty and staff at Morehead State University in Kentucky. The campus has expanded its use of The CBORD Group's card solutions with an implementation of iCLASS contactless card readers from HID Global.

A long-time user of contact chip and magnetic stripe technology for EagleCard applications, Morehead State recently upgraded to iCLASS contactless readers for its existing Odyssey PCS campus card system from CBORD. More than 220 iCLASS readers are in place across campus to manage purchases and privileges for access control, dining services, snack/beverage vending, copying, printing and laundry payment.

In addition to increased convenience for students and staff, the contactless readers are also producing revenue for the school. Vending sales were previously managed with a contact smart chip, requiring students to maintain separate accounts for vending purchases. With iCLASS readers managing purchases across campus, the university now offers students a multi-use account known as BeakerBucks, making it easy to spend and manage EagleCard funds. EagleCard-based vending sales have increased nearly 10% since the change was made.

Interac partners with INSIDE to bring contactless debit to Canada

Interac Association, Canada's payment network, has launched a partnership with chipmaker INSIDE Contactless to develop chips containing specifications for Interac's contactless payment service. This will enable members to offer a card-based payment solution for small ticket purchases.

As Frost & Sullivan industry analyst Shyam Krishnan explained it: "The small-ticket purchase segment in Canada, which is still dominated by cash and coin, represents green field territory for card payments, and although this market has been targeted time and again, it has been difficult to penetrate due to the lack of the right technology solution delivered at the right cost."

ACS to provide contactless ticketing for buses in Peru

Affiliated Computer Services, a Dallas-based information technology company, has been chosen to provide the City of Lima, Peru with a contactless ticketing system for the country's first bus rapid transit line. Under the terms of the $200 million contract, ACS will operate the system for a 14-year period.

ACS will supply and operate a fully integrated fleet management and ticketing solution to cover the needs of the first bus system installed in one of Lima's busiest areas. The line is intended to carry over 700,000 passengers a day, and the city intends to build 10 other ticketing solutions, along similar lines, in the next few years.

The ticketing solution will be based on smart contactless cards that will be controlled at each station by gates and sold by automatic ticket vending machines and manned POS terminals. The 220 buses will be fully monitored and regulated, which is expected to significantly minimize wait times at each station.

Cubic purchases ERG assets in U.S.

Cubic Transportation Systems Inc., a subsidiary of San Diego-based Cubic Corp., is buying the Vix ERG's Concord, Calif. operations center and will assume responsibility for ERG transit operations in the U.S.

Cubic will use its new assets that include select software licenses to expand services to transit agencies in San Francisco, Seattle, Boston, Ventura and Las Vegas. The deal brings about $20 million in annual revenues.

The agreement initially covers servicing the TransLink contract in the San Francisco Bay Area; and eventually will include the other transit agencies that currently use Vix ERG systems.

The Concord operation is designed to support smart card distribution and call center operations for transit authorities. Approximately 125 ERG employees have joined Cubic from ERG's U.S. operations and engineering operations in Perth, Australia.

Cubic currently provides fare collection systems and services in London, Germany, Sweden, Italy, Australia, Atlanta, New York-New Jersey, Philadelphia and Los Angeles.

MAN Diesel launches multi-functional employee badge based on LEGIC technology

MAN Diesel, Augsburg, Germany, has combined two contactless identification technologies on a single smart card chip for its new employee badge. LEGIC's card-in-card solution is the technological backbone for the badges.

The new card includes access control, time & attendance and cashless payments for more than 3,000 employees at MAN Diesel's Germany plant. In addition, German employees will also have access to the company's Denmark factories in the future.

LEGIC card-in-card solution runs as secure applets on third-party smart cards which make it

possible to combine different contactless systems on a dual interface card while supporting contact-based applications such as logical access.

The LEGIC card can be used in nine shops, eight canteen tills, eight top-up stations, 44 vending machines and over 50 access control and time & attendance terminals supplied by various manufacturers.

Gemalto providing personalization service for Singapore NFC pilot

Gemalto announced that it is providing personalization services to Citibank and Visa in support of the Citi – M1 mobile – Visa payWave NFC pilot in Singapore.

More than 750 merchant locations across Singapore are participating in the three-month pilot launched in May 2009. Up to 300 selected Citi M1 Visa Platinum card members have been invited to join. They are able to purchase items at Visa payWave merchants simply by waving their NFC-enabled phones in front of a contactless reader at the point of sale.

Gemalto is providing the management and preparation of sensitive user information from Citibank and performing secure Visa personalization services on the phones enabling subscribers to gain access to the Visa payWave service on Singapore M1's mobile network.

The service is performed at Gemalto's certified personalization facility in Singapore.

NFC Forum launches N-Mark

The NFC Forum has unveiled its "target mark," what its chairman called a "milestone in the global commercialization of NFC technology." The new N-Mark, introduced during an NFC Forum Web cast, is designed to show consumers where they need to touch to activate the NFC interaction.

The NFC Forum N-Mark is available to anyone for download free of charge from the NFC Forum Website, via a click-through license. NFC Forum N-Mark Trademark Usage Guidelines are provided with the N-Mark, and users must follow the guidelines for implementation to ensure global consistency.

Innovision's Julia Charnock, Marketing Communications Working Group chair for the Forum, said these trademark specs also include the color, a shade of blue. The N-Mark can also appear in black and white, she said.

"The N-mark should be placed in an easily accessible area," Charnock emphasized during the Web cast. She also said the Forum "won't be promoting the N-Mark to consumers. It's a tool for end users so they'll be supporting it themselves."

Within a year, the Forum is slated to issue a certification program along with a certification mark that will have to be added to all devices that pass compliance testing, said Dino Bekis of Broadcom, NFC Forum Compliance Committee co-chair.

EPC, Global Platform coordinating mobile payments standards

The decision making body of the European payments industry, the European Payments Council (EPC), and GlobalPlatform, a specification body for smart card infrastructure, have agreed to coordinate initiatives within the mobile contactless environment. The two parties aim to promote interoperable and neutral technology that will support a mobile payments marketplace.

The formal relationship between the EPC and GlobalPlatform aims to ensure that the mobile contactless technical specifications and use cases of each organization are compatible and adhere to pre-defined common requirements for mobile payments. By synchronizing their activity the organizations will minimize the duplication of effort, have access to member-only work priorities, and capitalize on the impressive wealth of market and technical expertise available across both parties.

The first priority of the organizations is to verify compliance between GlobalPlatform's technology and the EPC use cases. Focus will also be placed on the capabilities of the GlobalPlatform Messaging Specification to standardize communication between the different players in the mobile proximity payments ecosystem such as banks, trusted service managers and mobile network operators.

The second objective is to analyze cooperation on compliance and certification of the secure element that hosts the mobile payment applications.

Oberthur unveils sticker technology

Oberthur Technologies has deployed its FlyBuy contactless stickers to three banks internationally, including one of the largest card issuers in the United States. The sticker is the latest product in Oberthur Technologies' development of contactless payment form factors.

Approved and developed in cooperation with MasterCard, Oberthur Technologies' FlyBuy Sticker is a contactless payment device that can be attached to any surface including a mobile phone, PDA, MP3 player or key ring, enabling the end user to choose their personalized payment device.

To pay, the user simply needs to place the device with the Sticker attached in front of the contactless reader. It can be used as a normal payment card at any point-of-sale terminal accepting contactless. Tested in pilots internationally, the FlyBuy Sticker is designed to work with existing business models, and can

be personalized on any standard contactless equipment.

Oberthur has five financial institutions buying the stickers, says Martin Ferenczi, managing director of the Americas Region for the Card Systems Division of Oberthur Technologies.

But banks may not be the only customers, Ferenczi says. Oberthur is targeting public transportation groups as customers as well.

U.S. getting squeezed by EMV

With Canada and Mexico both going to EMV and most of the rest of the world doing the same it may be a matter of time before U.S. card issuers are forced to go to chip and PIN.

Geography isn't the only issue, said Rene Bastien, product manager for payment products at SAFENET at the CTST Conference in New Orleans. It's becoming more common for U.S. travelers in Europe to have transaction denied because retailers aren't authorizing transactions with just the mag stripe. "EMV is happening everywhere."

Jack Jania, vice president and general manager of secure transactions at Gemalto, says some U.S. banks are considering issuing EMV cards to high-end customers who frequently travel overseas.

Dual-interface cards are also starting to appear on the scene, Jania says. These cards have one chip but can perform EMV transaction through a contact interface as well as contactless.

Canada may also bring to bear some pressure for EMV, says Deb Baxley, managing partner at Keypoint Solutions. If Canadian issuers start to see credit card fraud add up with mag stripe transactions merchants could start denying the transactions.

So when will the U.S. make the move? It's hard to say. "I hate to put a date on it," Jania says. But there has been progress. Two years ago U.S. issuers wouldn't even talk about EMV but they are now, Jania says.

Students don't worry about ID theft, survey finds

College students and their parents don't exactly see eye-to-eye when it comes to ID theft. A new survey shows less than a quarter of students interviewed were concerned about having their identities stolen, while the opposite is true for their parents. About 74% indicated they believe students are at moderate-to-high risk for identity theft.

The Campus Security Survey of 1,000 college students and an equal number of parents was conducted by uni-ball pens and the Identity Theft Resource Center.

Students' lack of concern, combined with the fact that 40% said they provide their social security numbers online, may also mean parents' warnings are falling on deaf ears: 89% of parents said they had discussed safety measures with their students before they left for school.

The survey also points out that just 44% of students are concerned about having their personal belongings stolen (laptop, mp3 player, purse, etc.), 40% regularly leave their apartment or dorm doors unlocked, and only 34% are afraid of walking home from campus at night.

However, half of the students surveyed said they shred important documents and bills, and only 9% said they share personal online passwords with friends.

ITRC recommends that students come to school with a shredder and a lock box big enough to hold their laptops. They should also be encouraged to reconcile their bank statements monthly to identify fraudulent activity (nearly one-third of students rarely, if ever, reconcile their credit card and checking account statements, according to the U.S. Department of Education), never share online passwords with anyone, and take precautions when posting personal information on social media Web sites.

LaserCard to supply national ID cards to Angola

LaserCard announced that the Angolan government has officially approved the design of its new national ID card, triggering production of the initial supply of secure optical memory cards for the country's national ID program.

Issuance of cards to Angola's adult citizens is scheduled to begin in Luanda, the nation's capital, by this fall. Delivery of the $8.8 million program will begin this quarter and is scheduled to be complete this fiscal year.

The cards will be issued as wallet-size ID credentials to citizens nationwide and will store data including personal and biometric identification. The cards are based on the same optical memory technology used in the U.S. Department of Homeland Security's "Green Card" program.

LaserCard is a subcontractor to the Angolan government's prime contractor, DGM-Sistemas of L.D.A. DGM-Sistemas and other team partners have been engaged in the implementation of the national IT infrastructure and criminal registry database to support the personal data capture, card issuance and downstream application processes.

L-1 signs contracts, extensions for driver license issuance

L-1 Identity Solutions was awarded contracts and contract extensions from Delaware, Louisiana, Tennessee, and Indiana to continue pro-

viding secure driver license solutions. The total value of these contracts is $27.6 million.

A seven-year contract with the Delaware Division of Motor Vehicles includes a new tamper evident card with various security features from L-1 embedded in the card to make counterfeiting more difficult. The new system will integrate L-1's document authentication solution into the state's process. Additionally, facial recognition technology from L-1 will enable a comparison of a customer's photo against the DMV's database of photos to detect fraud.

L-1 secured a contract extension with the Louisiana Office of Motor Vehicles to continue secure driver license production and vehicle registrations. L-1 has provided solutions to the Louisiana department for more than three decades. The Tennessee Department of Motor Vehicles also extended its driver license solution contract with L-1.

Indiana recently received federal funding for secure issuance of driver licenses. The state will continue to work with L-1 to apply these funds toward fully implementing the recommendations of the 9/11 Commission and the federal regulations regarding identification documents.

Gemalto launches portable card reader in Germany

Gemalto announced the commercial launch of Ezio Optical TAN, an optical authentication reader for online banking designed for the German market.

The size of a credit card, the Gemalto reader fits in a wallet along with the banking card. Ezio Optical TAN is compliant with the latest German handheld device standard and leverages the security of the Secure Chip Card Operating System banking cards.

With Ezio Optical TAN, online customers can conduct secure e-banking anywhere at any time. Users just present the device in front of their computer screen and optical sensors capture the data they would normally enter from the reader keypad to carry out and sign online transac-

tions. No software needs to be installed to use the device.

The Gemalto product is part of an extended family of authentication and digital signature solutions that includes readers, tokens, software and services. Gemalto has already delivered Ezio authentication solutions to leading banks in Asia, Europe and the Americas.

HID's naviGO receives top security rating

HID Global's naviGO software version 1.37 has received the highest possible rating, an A, from Veracode, a company that tests software for security vulnerabilities. This rating, says HID, means that naviGO has been evaluated against industry-standard benchmarks such as the common weakness enumeration, common vulnerability scoring system, and the National Institute of Standards and Technology to determine software weaknesses and vulnerability severity levels.

The Veracode rating also incorporates business risk so that critical applications like naviGO are evaluated in the context of the data they handle.

HID's naviGO is the key component of the company's logical security solution, which improves risk management across the enterprise by using an organization's existing physical access control cards to log into the IT infrastructure.

Mirroring the secure user experience popularized by the company's physical access control platforms, HID on the Desktop is a three-component solution (HID cards, readers and naviGO software) that delivers authentication enabled by the use of a single credential for both physical and logical access.

EU funds student ID project

The European Education Connectivity Solution (EECS) project commenced on June 1 and was officially launched at the Annual European Campus Card Conference held in Stansted, London. The overall cost of this project is $2.1 million, which came from the European Union and other contributors.

The idea behind the student ID is to set up a framework where students can study at different universities across the continent without having to physically carry academic records, says Eugene McKenna, chief executive of campus services, Waterford Institute of Technology in Ireland. The ID will act as a key for students to access these records.

For example, if a student were going to study aboard for a year he would go to the registrar's office and have his academic records uploaded to a secure server. The student would be authenticated with the ID and a fingerprint biometric. After arriving at the other university the student would again use the ID and biometric to be authenticated and this would enable his records to be downloaded to the other university.

In the trial phase, students from Waterford and the Technical University of Lodz in Poland, two members of the consortium, will become trial exchange students. The project will use NXP's Mifare technology to start, but will review other options as well.

UK IDs will not be mandatory

UK Home Office Secretary Alan Johnson announced that the identity scheme put in place would be voluntary for citizens. The only individuals forced to apply for the cards would be foreign nationals living in the UK. 50,000 of these cards have already been issued.

The IDs also will no longer be mandatory for airport workers. Under the new proposals, ID cards will be voluntary for workers at Manchester and London City airports. Workers will continue to be encouraged to get an ID card, which they can do for free, as it makes it easier for employers to carry out background checks and issue passes.

K-12 schools lack student badging

Just 16% of K-12 schools actually badge students and staff, according to a recently-released nationwide survey from the American Association of School Administrators. More significantly, there is a surprising difference in this rate among regions of the country.

While 16% of respondents said staff and students are badged, another 35% reported that staff only are badged. Some 20% say badges exist but aren't enforced and 28% don't use badges at all. Just 4% of the western states, such as California and Washington, reported badging students and staff. Compare that to a high of nearly 26% of respondents in the northeast, such as New York and Connecticut. Additionally, about 45% of responders from the western states say badges aren't used at all.

However, more than 85% of respondents require all visitors to sign in and receive a badge.

What's not so surprising is that nearly 80% of administrators responding to the survey describe their funding level as "stretched" or "inadequate." One of the study's findings points out that this lack of funding could be directly tied to the fact that not a single respondent reported all doors can be locked down electronically in the event of an emergency, which "represents a potentially problematic situation."

The survey was conducted last year by AASA, security provider Ingersoll Rand Security Technologies and security consultant RETA Security on the status of safety and security in America's K-12 public schools.

CoreStreet, Senture partner for TWIC

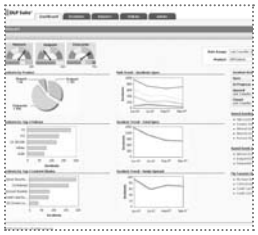
Senture Security Solutions LLC, a security solutions integrator, and CoreStreet, the provider of credential validation solutions, announcedthey will team up to deploy national security programs for both the maritime and transportation industries, as well as the defense, homeland security and emergency management markets.

With more than 10 years of smart card and biometrics experience, Senture offers its customers a unique balance of Transportation Worker Identification Credential regulatory and technical expertise. Maintaining product and technology neutrality, customers benefit from Senture's hardware and software components to complement its TWIC services.

The CoreStreet PIVMAN for TWIC Solution enables Transportation Security Administration-approved mobile devices to verify the identity and attributes of TWIC card carriers. The CoreStreet Enabled devices are synchronized with the authoritative source for this information, the TSA TWIC hotlist. By having this secured data resident on mobile devices, operators have the ability to determine if the TWIC credential is still valid.

The CoreStreet for TWIC Solution has upgrade options to validate and verify off card attributes for the Department of Defense's Common Access Card, the Personal Identity Verification cards used by civilian agencies and the Emergency Response Official Community's First Responder Authentication Credential used by federal and state emergency management officials. This allows mobile operators to make the same type of informed decisions when presented with any U.S. government credential.

RSA unveils products to protect personal information



RSA announced a set of solutions to help organizations address the challenging aspects of complying with the U.S. Data Breach Notification Laws for protecting personally identifiable information (PII) and mitigating the risk of security breaches. Specifically, RSA is announcing three packages of information security products – including two-factor authentication, security information and event management (SIEM) and data loss prevention (DLP) – designed for mid-sized companies.

Organizations entrusted with personally identifiable information from customers and employees are required to take appropriate actions to secure and protect this information. In addition, laws across the United States levy varying penalties – including public notification requirements – for organizations suffering a compromise.

RSA's personally identifiable information package is engineered to deliver technologies that support these efforts by enabling customers to:

- Identify PII across their environment, and understand where and how this data is being accessed and stored, and how and by whom it is being used
- Implement appropriate security controls based on policy and risk
- Monitor the environment and proactively identify potential security events in real-time

Blackboard adds iPhone app capabilities to product suite

A company created by two Stanford students to build iPhone applications that enable students to access a host of campus services has been purchased by Blackboard. Purchase price, sources say, was $4 million. In addition, Kayvon Beykpour, one of the co-founders of Terriblyclever Design, is joining Blackboard as a vice president and will lead the company's focus on mobile technologies for education.

San Francisco-based Terriblyclever was started by a group of students who worked with Stanford University to build iStanford, a set of iPhone applications to support campus life. Terriblyclever has also developed iPhone and mobile Web campus applications under the banner MobilEdu for Duke University, Medical College of Georgia, Texas A&M University and several other higher education and K-12 institutions.

"We started MobilEdu because we wanted to empower students and faculty by allowing them to engage with their university in a powerful and mobile way," said Beykpour. "Joining forces with Blackboard was the best way to work towards that vision."

MobilEdu allows education institutions to deliver a set of campus life services and content to mobile devices, branded for each institution. With an Apple iPhone, iPod Touch or other device with a mobile Web browser, MobilEdu users can navigate course catalogs and campus maps, e-mail professors and classmates and get real-time updates on their course schedules, campus events, news and sports teams.

ID SHORTS

SkyRFID offers automated library system

Canada-based SkyRFID, a provider of RFID-enabled automated data collection systems, has announced the release of an Automated Self Serve Library Management system. Patrons of a library deploying the system can access a full range of library services with a swipe of their RFID-enabled library cards.

Patrons can access their records and check out library items at self-serve stations. The SkyRFID system also simplifies the catalog search process, enabling patrons to reserve and request books from multiple branches of a library system with a minimum of effort.

With the addition of optional PC/SC CCID NFC Smart Card readers to the system, SkyRFID gives customers the option of accepting payment for overdue fines via smart cards or NFC cell phones. A range of administrative functions, including the transfer of catalog items from a barcode system to RFID, are also supported by the system.

SkyRFID also offers libraries an additional security function through the new system. The RFID-enabled patron IDs can be used as key cards to gain access to locked library facilities for special events, scheduled for hours when the building is closed to the general public.

PingPing, touchatag partner on application development

PingPing, a brand by Belgacom for mobile and micro payments, and touchatag, an Alcatel-Lucent venture, have teamed to define a business model that combines PingPing's payment system for mobile phones and touchatag's contactless and NFC services, such as interactive advertising, loyalty programs and coupon services.

This fall, Belgian consumers will be able to use one contactless card or sticker to initiate a variety of applications, as opposed to numerous cards currently required. With a single contactless card or sticker, a consumer will be able to add loyalty services, pay for new services and receive information. For example, someone walking past a movie poster can use his phone to learn more about the movie, see recent reviews, check on movie times and seating availability and even buy a ticket for a particular showing, simply by holding his cell phone near the poster and clicking a few buttons.

PingPing and touchatag will work together to create an accreditation program that will enable other technology suppliers, operators and application developers to develop new programs and uses for the technology.

Chicago's Shedd Aquarium uses RFID for new exhibit

The revamped Oceanarium exhibit at Chicago's Shedd Aquarium just completed a $50 million renovation that includes an interactive kiosk where children can maneuver a mechanical claw to pick up items such as shells and stones that are embedded with RFID tags.

A sensor in the claw reads the tag as the item is picked up and triggers an animated video to appear on the kiosk screen providing information about the particular item. The system was created by Chicago-based Mightybytes media design firm.

The Shedd is not the first aquarium to take advantage of RFID technology. In 2007 Singapore's Underwater World began embedding their fish with RFID tags in order to help visitors identify the different species. As the tagged fish swim by a sensor, information is relayed to a touch screen, providing visitors with the name, species and other facts.

BookFactory, FileTrail partner for RFID-enabled notebooks

FileTrail, a provider of browser-based records management software and RFID-enabled solutions, has announced a new partnership with BookFactory, a producer of custom laboratory and engineering notebooks for scientific applications. The result of the collaboration is an RFID-enabled scientific notebook.

The new notebooks will be embedded with RFID tags, enabling the monitoring of their location and movement via any desktop computer using FileTrail's browser-based tracking system. FileTrail's handheld RFMobile Portable RFID Detectors complete the tracking solution.

The system is intended to streamline the tracking process, keeping tabs on notebooks as they change hands between lab personnel and enabling users to quickly locate a particular notebook. This level of information management can be invaluable, especially in situations where scientific data and research must be documented and preserved to benchmark development or secure a patent.

The system also addresses another issue of intellectual property development by offering enhancement of security operations. Companies can restrict notebook access by using the FileTrail system to implement a check-in/check-out procedure, or to assign a notebook to a particular scientist. The RFID technology can also issue alarms when a tagged notebook crosses an exit or doorway, helping administrators prevent removal.

CTA considers dropping fare card, accepting contactless payment cards

The Chicago Transit Authority is exploring dropping its fare cards and instead going with contactless credit, debit and prepaid cards for payments on the system. The agency will issue a request for proposals in late August.

Switching systems would save the CTA money because it wouldn't have to issue fare media and manage the fare payment and collection system. The contactless fare payment system would reduce the need for customers to carry cash or have the right denomination or currency to ride the system.

In addition, the same card that would pay for fares to ride CTA also could be used for everyday transactions such as purchases at retail outlets, thereby reducing the number of cards an individual would need to carry.

The first phase of the procurement process will examine the CTA's options for developing the card, including considering possible procedures, management and cost of the program. After reviewing these proposals and developing a final plan, the second phase will give companies the opportunity to submit proposals for the actual implementation of the program, which will take place summer 2010.

Italy's Lega Pro football league to issue fans ID cards for upcoming season

Lega Pro and Telecom Italia have announced that at the start of this year's season new cotactless-enabled ID cards will be issued to league fans in order to better manage stadium access.

Each ID card comes embedded with an microchip that is used to record the fan's ticket purchases. Stadium employees using hand held terminals read each fan's card at the gate and verify that the cardholder has purchased a valid match day ticket, eliminating the need to present paper tickets for stadium access.

The card, which doubles as a rechargeable Visa card, also offers access to a variety of football club-supplied services, such as bonus tickets, fast-track turnstiles, and other fan benefits.

The ID cards, called "Tessere del Tifoso" (or "Fan Passes"), will be issued to fans of each of the leagues 90 affiliated Italian football clubs.

2009

September

ICAO Worldwide Symposium on MRTDs
September 21 – 23, 2009
ICAO Headquarters
Montréal, Quebec, Canada

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

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

October

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

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

Biometrics 2009
12th World Conference and Exhibition
October 20 – 22 2009
Westminster, London, UK

November

2009 NACAS Annual Conference
November 8 – 11, 2009
Hawaii Convention Center
Honolulu, HI

Cartes & IDentification
November 17 – 19, 2009
Paris-Nord Villepinte Exhibition Center
France

2010

April

NACCU 17th Annual Conference
April 18 – 21, 2010
Pointe Hilton Tapatio Cliffs Resort
Phoenix, AZ

May

Smart Card Alliance Annual Conference
May 17 – 20, 2010
Marriott Camelback Inn Resort & Spa
Scottsdale, AZ

Is strong online identity just around the corner?

Government, private sector and consumer groups all push for solutions

Zack Martin
Editor, AVISIAN Publications

The old saying goes: On the Internet nobody knows you're a dog.

But that may not be the case for much longer. Efforts from corporations, the U.S. government and others may provide a trusted and secure way to identify individuals on the Internet. Momentum seems to be building to stem the potential "identity crisis" in the U.S.

A White House review of U.S. cybersecurity, released in May, showed significant weaknesses in cybersecurity and making better use of identity management systems is one precaution that can be taken to improve the situation, according to the report.

"We cannot improve cybersecurity without improving authentication, and identity management is not just about authenticating people," the report states. "Authentication mechanisms also can help ensure that online transactions only involve trustworthy data, hardware, and software for networks and devices."

The report calls on the federal government to work with the private sector to create an online identity management system that uses privacy-enhancing technologies. As a starting point the report suggested using the National Science and Technology Council's Subcommittee on Biometrics and Identity Management report that was released in 2008. (See Obama's Plan, right.)

The report also states that the federal government should continue to fund the implementation of HSPD-12 and extend the availability of the credentials to operators of critical infrastructures and others. The release of the new PIV Interoperability specification will make it easier for non-federal entities to issue these cards. (See page 26.)

Sources say there may also be plans for the U.S. to consider issuing a high-assurance credential to citizens on a voluntary basis.

In addition, there are projects in the private sector. Technology providers and associations have joined together to form the Kantara Initiative. The idea behind the program is to unite the various existing identity management schemes so the end user doesn't have to sign up multiple times.

Improved credentials on the horizon

In the next five years 150 to 200 million high-assurance credentials will be issued to U.S. citizens, said Peter Alterman, former deputy associate administrator for technology strategy at the office of government-wide policy at the General Services Administration who is now with the U.S. Department of Health and Human services. Alterman made the comments at the CTST conference in New Orleans in May.

Alterman doesn't know who will be issuing these credentials. But it's most likely federal standards, such as FIPS 201, will be used by citizens as well as federal employees.

While he wouldn't say which agency would issue the credentials or how they would be used, but he did say there are activities in store for the next year around health care, the IRS and Social Security Administration.

"We're going to see more of an emphasis on communities of people demanding better means of identity as they move into the digital world," says Neville Pattinson, vice president of government affairs and standards at Gemalto.

Health care is a market where the identification industry needs to focus. "There's a great deal of concern about health care," Pattinson says.

OBAMA'S PLAN *for securing the Internet*

President Barack Obama's review of U.S. cybersecurity shows that there are a number of security challenges facing the country and its digital infrastructure.

News reports this spring showed that the nation's electric grid was vulnerable to hackers and had been infiltrated, and attacks on various government sites in July further highlight the issues raised in the report.

"It is the fundamental responsibility of our government to address strategic vulnerabilities in cyberspace and ensure that the United States and the world realize the full potential of the information technology revolution," the report states.

To tackle these issues Obama plans to appoint a cybersecurity official to ensure the country takes the necessary steps to secure networks. This individual will work with the private sector to come up with solutions. "The government, working with State and local partners, should identify procurement strategies that will incentivize the market to make more secure products and services available to the public," the report states.

Recognizing that the Internet is a crucial component of everyday life for most U.S. citizens, the federal government needs to take steps to educate the public on online safety. "The United States should initiate a K-12 cybersecurity education program for digital safety, ethics, and security; expand university curricula; and set the conditions to create a competent workforce for the digital age," the report states.

Securing identity was singled out in the report. "Identity management also has the potential to enhance privacy through additional protection against the inappropriate release of personal identifiable information," the report states.

Initiatives the government should take include:

- The federal government should work with the private sector, civil liberty organizations and privacy advocates to create an identity management system.
- For high-value activities, such as the Smart Grid, the country should deploy an opt-in system of interoperable identity management systems to build trust for online transactions and to enhance privacy.
- The National Science and Technology Council's Subcommittee on Biometrics and Identity Management in 2008 published a report that provides a vision for future federal identity management and a series of research and development recommendations. The government should use the report as a starting point for identity management strategies.
- The government should ensure that resources are made available so HSPD-12 is full implemented.

"The Federal government also should consider extending the availability of federal identity management systems to operators of critical infrastructure and to private-sector emergency response and repair service providers for use during national emergencies," the report states.

The biometrics industry is lobbying for its technology to be used solely, but the use of a smart card would enable other functionality, including protecting against identity theft, authentication for bank accounts and health records and other possibilities.

"Money is heading in that direction and this may be the coattails we live off of to create an identity infrastructure."

Doug Simmons, vice president of consulting at the Burton Group Consulting Services, says the U.S. government's Personal Identity Verification specification has paved the way for non-government entities to deploy smart cards. "Enough people are getting fed up with the identity theft and saying enough is enough," he says. "We're smart people and we need to put the policies in place to take care of it."

One of the major issues with the high-assurance credentials is who will issue them. The federal government may not be able to do it because it reeks of a national ID program, which many consider a poison pill in the U.S.

But Simmons suspects that states are in a perfect situation to issue the credentials, but Pattinson has concern. Who is liable if someone gets a fake credential and does something malicious? This liability may keep private companies from issuing them as well.

New Social Security card in the works?

But there are signs that the federal government is preparing to issue citizens some type of credential. The U.S. Senate Judiciary Committee is exploring the use of biometrics and smart cards for a new Social Security card. This could lead to as many as 300 million electronic credentials being issued in the next six to eight years.

Two different ideas are being floated when it comes to the Social Security number, sources say. One involves enrolling individuals, capturing the fingerprint biometric and then linking it to the Social Security number. The biometric data would be stored and checked against a database for official functions, such as verification of employment eligibility.

The other idea involves the issuance of a smart card with match-on-card biometric functionality. Cardholders could use this card for official functions and potentially as an authentication token for other transactions both in physical and virtual environments.

The primary purpose for using the new technologies would be to show employment eligibility for residents and non-resident aliens. Before being hired an individual would have to have the biometric checked to make sure he is eligible to work in the U.S.

The new card would not be mandatory. "It's an upgraded Social Security card with the added benefit of authenticating the cardholder and protecting against identity theft," says one source, stressing "it's not a national ID."

The biometrics industry is lobbying for its technology to be used solely, but the use of a smart card would enable other functionality, including protecting against identity theft, authentication for bank accounts and health records and other possibilities.

Studies suggest that U.S. citizens are overwhelmingly opposed to a national ID card. But at the same time when asked if they want protection from identity theft the answer is a resounding yes. "We don't have any way of putting our identity out there in a trusted manner," says a source. "I see the political indicators aligning and the Obama administration seeing the challenges."

The Senate Judiciary Committee, particularly Sen. Chuck Schumer (D-N.Y.), chairman of Senate Judiciary Committee's Subcommittee on Immigration, Border Security and Citizenship, has been the driving force behind the efforts. Schumer's office did not return calls.

But a hearing in July has Schumer backing a biometric-only approach that would be used for verifying employment eligibility.

E-Verify is the system in place now and it verifies the Social Security number, date of birth and other demographic data. Schumer says the system is prone to errors and doesn't work and wants to add additional identification, such as biometrics, to prevent fraud and increase secu-

rity. He called for a "non-forgeable identification system to completely and accurately identify workers."

The system would be mandatory and apply to citizens and non-citizens who would use the system to verify employment eligibility. The system would have no other purpose, Schumer says.

Testifying at the hearing was Rep. Luis V. Gutierrez (D-Ill.), who has proposed using biometrics for employment verification before. "In my last comprehensive immigration reform bill, we included a requirement to better secure the Social Security card by making it a tamper-proof, biometric card," he says. "Schumer's proposal, to actually make the entire system biometric-based takes the system one step further."

Gutierrez says using this type of system will provide workers with greater power and access to employment records, prevent pre-screening and misuses by employers and reduce fraud because an individual would have to swipe a card and authenticate a biometric in order to be verified.

The challenges for such a system did not go unnoticed. "A system that depends on a biometric card rather than a database query would require every American and legal foreign worker to obtain a card," Gutierrez says. "This would place the bulk of the changes necessary at the front end of rolling out such a system, and Congress would need to commit sufficient resources."

It would also require employers to have equipment to verify the card and biometric. "I think Congress and the American people will want to have a clear understanding of how such technology works, how their privacy will be protected, the process and cost of rolling out access to employers," Gutierrez says.

One source says a mandatory, biometric-only approach won't work. In order to get buy in from the public there has to be an upside for them, such as protection against identity theft. "It must be voluntary and be able to be used for other applications," the source says.

Privacy groups will almost certainly come out against the credential and there will be some intense lobbying on both sides of the issue.

Still while the political will seems to exist now and legislation could be proposed this year there are still challenges. Exactly how the card will be used has to be determined. Political insiders say immigration reform may be the best political way to get a bill passed.

While there are still obstacles to hurdle, it appears as though there may be serious movement to offering citizens a way to secure their identity

Standing guard. Entrust ePassport security solutions are the most scalable, interoperable and proven in the world.

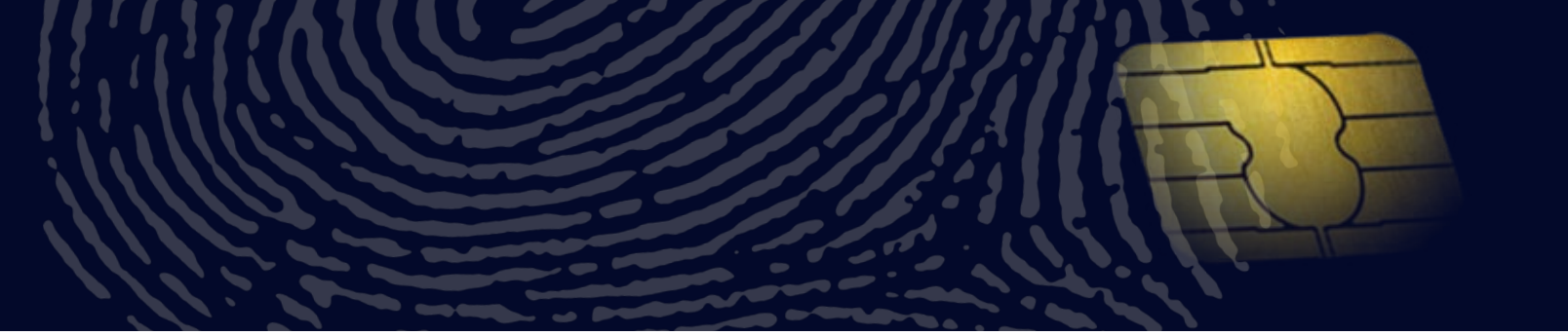
As the global PKI leader, Entrust provides trusted security solutions for first-generation (BAC) & second-generation (EAC) ePassport environments. In fact, Entrust is the No. 1 provider of ePassport security solutions and is leading the migration to the EAC standard.

No matter if you're just beginning development or evolving your ePassport strategy, Entrust is the choice for ePassport security.

Visit entrust.com/epassport

Entrust® Securing Digital Identities & Information

Entrust and Entrust product names are trademarks or registered trademarks of Entrust, Inc. or its affiliates. All other company and product names are the property of their respective owners. © Copyright 2009 Entrust. All rights reserved.



online. "This is going to be the beginning of a trusted credential in the U.S.," a source says.

Private sector also seeking solution

Brett McDowell, executive director of the Liberty Alliance, says the market needs to come up with a solution so individuals will be able to get a credential if they want one.

The Liberty Alliance is one member of the Kantara Initiative, an organization working on technical interoperability for all the different electronic identity schemes, says McDowell. The group is working on solving the policy question around ID interoperability as well as the technical issues.

There are a number of different technical solutions for online identity. Open ID, PKI, SAML and Information Cards all serve to identify individuals online and they all do it in a different way. The goal of Kantara is for these different systems to become interoperable, McDowell says.

"We're focused on interoperability at the protocol level. None of the solutions in the marketplace can solve the full Internet ID continuum," he says. "The stakeholder on any one solution is focused on solving that problem on his own and we now realize we have to work together to solve the problem."

Part of the process will be setting up four levels of assurance for different online transactions, McDowell says. Every network transaction will then be placed in one of the four levels of assurance and a user will have to authenticate to that level before the transaction is completed. For example, logging on to a social networking site may the lowest level while transferring money from a bank account will require a higher level of assurance.

"In the end the goal is for a person to assert their identity across the continuum," he says. "From your banks to your social network and working with the government and your employer."

Kantara aims to enable the individual to have different personas with separate attributes, McDowell says. An individual could have one persona on a social networking site and a different one when logging into the bank account even though they are using the same identity management system to log in to both.

But how does that identity get vetted for the first time? How is it trusted?

McDowell says financial services companies will likely have a role in this. "You look at the banks and they authenticate everyone," he says. "They have an infrastructure and are regulated. Google and Yahoo have the users and they are authenticating people but they have no knowledge of who they are."

No matter who issues the credentials it seems as though there may soon be some type of high-assurance credential available to the public. Between the federal government's efforts and those from the private sector it will be interesting to see who comes up with a solution accepted by the public first to solve the identity crisis in the U.S.

The Experts Weigh In

WHAT DOES THE GOVERNMENT SAY?

It's the fundamental responsibility of our government to address strategic vulnerabilities in cyberspace and ensure that the United States and the world realize the full potential of the information technology revolution.
Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communication Infrastructure

USE WHAT WE HAVE ALREADY CREATED

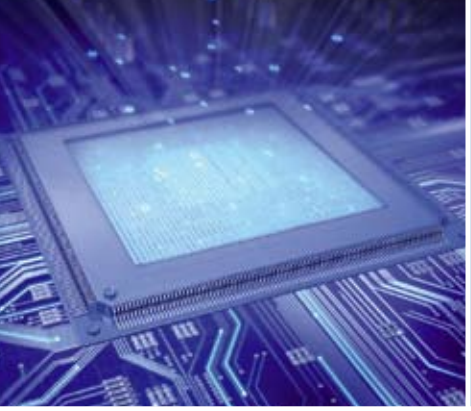
The U.S. government's Personal Identity Verification specification has paved the way for non-government entities to deploy smart cards. Enough people are getting fed up with the identity theft and saying enough is enough. We're smart people and we need to put the policies in place to take care of it.
Doug Simmons | VP Consulting | Burton Group

FREE MARKET WILL DETERMINE SOLUTION

We're going to see more of an emphasis on communities of people demanding better means of identity as they move into the digital world.
Neville Pattinson | VP Govt Affairs & Standards | Gemalto

ONE ID, MANY POSSIBILITIES

In the end the goal is for a person to assert their identity across the continuum. From your banks to your social network and working with the government and your employer.
Brett McDowell | Executive Director | Liberty Alliance



Verify Your Semiconductor is Secure and Licensed.

Ask your chip supplier the following three questions:

1) Is your semiconductor protected against DPA attacks?

2) Does the chip supplier have a patent license from Cryptography Research for DPA countermeasures?

3) Has the security chip been tested by a qualified testing lab and approved for the "DPA lock" certification logo?

DPA™

Be sure your product is properly protected, licensed, and tested.

Over 4 billion security chips are made each year with DPA countermeasures licensed from Cryptography Research, Inc.

Cryptography Research is committed to helping enhance semiconductor security.
For more information, visit www.cryptography.com/dpa

Differential Power Analysis (DPA) is a powerful non-invasive attack that enables attackers to extract keys from semiconductors. Cryptography Research owns the fundamental DPA countermeasure patents. It is a violation of patent law to make, use, sell, offer to sell, or import products that use these techniques without a license. U.S. patents include #6,278,783, #6,298,442, #6,304,658, #6,327,661, #6,381,699, #6,510,518, #6,539,092, #6,654,884, and other U.S. and international patents.

Cryptography Research, Inc. • 575 Market Street, 11th Floor • San Francisco, CA 94105 • www.cryptography.com

CRYPTOGRAPHY RESEARCH

Building bridges to identity

The Four Bridges Forum aims to bring trusted identity online

Trusting transactions online can be difficult. How does a user know who he's dealing with on the other end of a computer?

To ease this concern the federal government created the Federal PKI Architecture, or the Federal Bridge. It enables government agencies to issue digital certificates that can be used to authenticate individuals for trusted transactions online.

Now organizations outside of the federal government are cross-certifying with the federal bridge for trusted transactions. Along with the federal bridge, there is CertiPath, which serves the defense and aerospace industries, Safe Bio-Pharma, for biopharmaceutical and healthcare industries and HEBCA, which serves the higher education sector in the United States.

Together, these organizations have formed the Four Bridges Forum to help facilitate trusted electronic business transactions their respective constituencies.

"As we move into the digital world there are tremendous efficiencies to be gained from going electronic," says Mollie Shields-Uehling, president and CEO of the Safe Bio-Pharma Association. Fundamental to secure electronic transactions, she stresses, are digital identifications that enable us to recognize each other without creating "a tower of babble."

This is what drove Safe Bio-Pharma, an association formed by U.S.-based pharmaceutical manufacturers, to investigate digital signature and PKI technology, says Shields-Uehling. "We need interoperable trusted identity management standards and a digital signature linked to that identity so people can do business across that bridge," she says.

While pharmaceutical companies can't yet make regulatory submissions online, there are a number of ways PKI can help in the health care industry, says Shields-Uehling. Safe Bio-Pharma is working with the U.S. Centers for Disease Control and physicians in Minnesota on a cross jurisdictional public health surveillance project.

In the past it could take up to a week before physicians were able to recognize a public health threat and allocate medicine and resources to combat the problem, says Shields-Uehling. But physicians in Minnesota will be using digital certificates to enter and access information in order to potentially spot outbreaks earlier.

"Physicians could gain access using an HSPD-12 credential, login and get access to patient files," says Shields-Uehling.

"Once you have, the strong binding of a person with the credential, we will see a number of our Internet social ills literally evaporate over night."

Another use case is for clinical investigators working on multiple research projects, she says. Entering an investigator's office someone may see three laptops and two USB fobs and each will have a different sticky note on it with a different user name and password for the different trials. Having one trusted credential to file reports will make it easier for the investigators.

Defense and aerospace contractors have been using PKI for a longer time than the health care industry and there are established use cases with contractors using digital certificates to send information to the U.S. Department of Defense, says Jeff Nigriny, president and CEO at CertiPath.

The company has a new product that enables the PKI certificate on a FIPS 201 card to be authenticated for physical access control, Nigriny says. The physical access control system uses the federal bridge to authenticate the certificate.

Someone from the General Services Administration, DOD, or Boeing, as long as they have a valid digital certificate on the card can use it to access the Herndon, Va.-based CertiPath headquarters. "It leverages the same bridge mechanism and decides who can come to our offices," Nigriny says.

One knock against PKI has been its high cost, but the organizations with the Four Bridges Forum are reducing costs through a shared-services model, says Shields-Uehling. Safe BioPharma's members pay for the digital signature technology through the fees paid to the association.

Nigriny says once you scale up with the number of standardized credentials cost is driven down. "One credential with multiple providers is how you drive down the cost," he says.

Could the work of the forum eventually trickle down to everyday citizens?

Nigriny says PKI is on the path most technologies follow before being adopted by the public, with the government investing and using the technology, followed by business and then to citizens.

And the sooner the technology gets into the hands of individuals the better off everyone may be. "The identity fraud and social engineering attacks that we're suffering today, especially in online environments, are largely rooted in us not having transactions based on face-to-face proofing," Nigriny says. "Once you have, the strong binding of a person with the credential, we will see a number of our Internet social ills literally evaporate over night."

PIV I enables states, others to issue high-tech credentials

There's been a lot of discussion about using the Personal Identity Verification credential outside of the federal government. First responders are the biggest group to discuss issuance of an interoperable credential, but other jurisdictions also want to issue the ID to employees.

The problem was that the PIV/FIPS 201 specification was for federal employees and contractors and didn't translate seamlessly to other areas. One of the primary differences is the required identity vetting processes, but there were some technical challenges too. This changed in May when a new Personal Identity Verification Interoperability For Non-Federal Issuers standard was released.

The new specification enables states and others to issue interoperable PIV credentials and clears up any concern that states could start issuing credentials to one standard and then have it changed. "States and others felt that without clear guidance they were at risk because if the specification changed they would have to redo things," says John Bys, executive vice president at CoreStreet. "This wipes that fear away."

CoreStreet is working with a number of states and first responders on PIV I projects, Bys says. Colorado, Hawaii and Illinois are starting to issue credentials along with Washington DC.

Colorado invokes a two-tiered credential system

Colorado will use the PIV I spec but will also have another tier of credentials for first responders, says Micheline Casey, director of identity management at Colorado's Office of Information Technology. The state

'Spring Ahead' demonstrates many technologies

FEMA's 'Spring Ahead' demonstration showcased many different technologies and use cases. The purpose of the demonstration was to showcase FIPS 201 interoperability, with credentials issued from multiple private sector, federal, state and local jurisdictions utilizing the same technology as recommended in the draft National Incident Management System Credentialing Guideline.

The demonstration included the electronic validation of federal agency-issued FIPS 201 compliant and state/local government issued FIPS 201 interoperable credentials for risk mitigation and human resource situational awareness across more than 30 organizations in 20 locations throughout the United States.

The Illinois Terrorism Task Force was a key participant in the trial. A representative sample of Illinois-based emergency response officials from the emergency management, fire rescue, law enforcement, and critical infrastructure sectors reported to a simulated emergency operations center and presented smart credentials for electronic authentication and entry to the scene. The task force's credentials used public key infrastructure from Entrust Inc.

Business consulting firm, CGN & Associates, provided program management for the State of Illinois FIPS 201 Interoperable Secure Credentialing Project. CoreStreet's PIVMAN Solution was used to control access to the sites by authenticating and validating the identities and privileges Spring Ahead participants.

Photo: FEMA / Win Henderson

Spring Ahead consisted of:

- Eight scenarios that demonstrated the relocation of government personnel via air, water, and land assets
- The issuance of "just-in-time" credentials for emergency response officials who deploy to the scene of an incident without their credentials
- Smart phone application proof-of-concept: routine and emergency access to seaports using the Transportation Worker Identification Credential
- Federal and mutual aid out-of-area ingress for disaster response
- FIPS 201 migration technology
- Citizen evacuation, post-disaster re-entry, and sheltering-in-place.

Colorado first responders will issue two separate credentials, one will use the PIV I spec and have a contact and contactless smart card chip while the other will use a two-dimensional bar code.

wanted to be interoperable with the federal government and U.S. Department of Defense because it has the second largest concentration of federal government employees and military installations in the country.

But Colorado's governance poses an interesting challenge. The state is a commonwealth and it cannot force local jurisdictions to use a specific technology, says Casey, stressing that the local government must choose to adopt it. When the state first decided it wanted to go with a FIPS 201 credential the Information Technology Office spent nine months working with different groups across the state reviewing policy and standards before coming to an agreement.

"Those local agencies are the ultimate determining factor in how it will be used," Casey says. "A lot of this is monetary-based. When they are able to replace existing physical access control systems with FIPS 201 products they may. We are a very rural state and have a lot of volunteer forces that don't have a lot of money to do this sort of thing."

Because some of these smaller agencies don't have the funds, the state is recommending that first responders issue one of two credentials, Casey says. One will use the PIV I spec that will have a contact and contactless smart card chip. The other will use a two-dimensional bar code, Casey says.

Both credentials will include the bar code but the smart card will be issued to the first responders who cross jurisdictions while the other ID will be distributed to those who do not, Casey says. The non-PIV cards will be able to be validated using the bar code, which will act as a pointer to information stored in a database.

The North Central Region around Denver will be the first of Colorado's nine regional homeland security areas to issue credentials, Casey says. While the credential will be a statewide ID, it will also serve as an employee ID badge for access where agencies have a physical access control system in place.

Areas are also looking at uses beyond the typical first responder applications, Casey says. There's a city that hosts a major music festival in July and first responders from other jurisdictions help staff the event. The city hosting the event reimburses the other areas for staff time and hours will be logged using the first responder credential.

DC to badge city workers as well as first responders

Washington D.C. wants to issue first responder credentials too, but the district may take it a step further and issue IDs to city workers as well, says Chris Wiley, Washington D.C.'s chief technology officer. They are calling the proposed credential the DC One Card.

The district is taking a similar approach to Colorado, issuing different tier credentials to different employees, Wiley says. The primary difference is that all the DC One cards will be smart cards and the cards will be issued to city employees as well as first responders.

The district is planning to issue the cards to 5,000 first responders and then possibly add 10,000 to 20,000 city employees over the next couple of years, Wiley says.

One tier will follow the PIV I specification with third-party verification of identity, Wiley says. "PIV I will be important for us," he says. "We don't have to reinvent the wheel, look to those types of standards and it saves us a lot of energy." The other will be a card that's issued by the city agency and goes to city employees who need smart cards to bridge the physical and logical worlds.

Wiley has been working with the first responder program in Washington to set up the back end system and but he is thinking ahead to how city employees will use it.

The first application Washington will enable with the smart cards is single sign-on, Wiley says. The card will be a second factor of authentication that enables access to the different applications an employee uses. File encryption and email digital signatures will be the next applications the district considers after single-sign on.

Anticipating the use of smart cards Wiley has already been purchasing laptops that have built in smart card readers. On the physical access control side, he has been working with the district's property managers to install dual proximity and contactless smart card physical access control readers as older readers are phased out.

Federally interoperable credentialing in Illinois

Technology as a cultural lever

Dennis L. Gavin MBA, PMP
CGN and Associates

Illinois is unique among states because it has deployed an enterprise-level PKI that is cross-certified with the Federal Bridge. While this is a major accomplishment, it is only one component in the state's quest to develop a federally interoperable credential. Technology is a lever and a force multiplier in any process, but must take a subordinate position to process and policy. Prior to the existence of the PIV Interoperable standard or FIPS 201, Illinois had a coordinated and engaged emergency response community that recognized the critical importance of interdisciplinary and cross-jurisdictional cooperation. Interoperable technology thus found a welcome home in the Land of Lincoln.

Empowering the emergency response community

Beginning with its pilot rollout in September of 2008, Illinois has more than 1,200 emergency responders in various stages of the credentialing process. These responders are drawn from a highly diverse cross-section of disciplines – from Emergency Management and Counterterrorism Professionals to HAZMAT and Technical Rescue Teams. This initial population of candidates represents not only members of state agencies, but also the strong tradition of not-for-profit associations formed for the purpose of cross-jurisdictional mutual aid within the state.

From its inception, the DC One Card also was expected to serve as the employees' transit card for the Washington's Metro public transportation system. "One of the clearest benefits to this is having a Metro card built in," Wiley says.

Unfortunately, this has held up the project because the Metro uses a proprietary contactless technology from fare collection system operator Cubic. It's been difficult to get the Cubic chip put into a card with the other smart card technology.

Eventually the plan is to have one city employee badge instead of the dozen or more currently issued. Eventually it could be pushed out to citizens as well, who could use it for identification to different city services, such as the library and the Metro.

The DC One card is still in the capital phase, Wiley says. "We're trying to make operating costs lower. If you look at all the different carding operations in place and how this will consolidate those," he says, "it will save us some money."

The core process vision of the credentialing program is one of decentralized authority. Rather than centralize the process at a specific agency or location, the credentialing system delegates the authority and responsibility for candidate selection, validation and activation down to constituent organizations and teams. This is accomplished using a Web-based portal where credentialing candidates and their supervisors create and validate responder profiles.

Highlights of the credentialing process

The background check

Users enter the credentialing system through a fingerprint-based background check. The candidate reports to a site capable of collecting both fingerprints and a digital photo, which passes through a criminal background process before transmission to the Web-based credentialing portal. In addition to the obvious benefit of screening the criminal background of credentialing applicants, this process provides a crucial validation point. Submission of fingerprints in this manner provides reasonable assurance that the individual presented as an emergency responder is the individual whom he or she purports to be – a crucial factor in an identity validation application.

The team concept

The backbone of the Illinois Credentialing Process lies with the team. The team serves as the "administrative home" of the credential profile and may or may not correspond to the team or organizational affiliation of the individual. The team, which may be as large or small as needed, consists of individuals with a common emergency response affiliation. When a candidate joins a team, the Team Leader is responsible for review of the profile and affirmation of the candidate's skills and abilities as enumerated. When the Team Lead digitally signs the profile, he/she is giving credence to the qualifications and identity of the applicant. This has three advantages.

1. A Team Leader accepting an applicant into his/her team provides administrative control over the profile.
2. By requiring a Team Lead to digitally sign an applicant's profile certifying the validity of the information, there is a strong incentive for Team Leaders to ensure that the applicant's data is accurate.
3. A Team Leader validating the candidate's qualifications with a digital signature provides a much more cost-effective and streamlined method of validating qualifications than building interfaces to external qualifications databases, assuming that such a database exists for a given qualification.

A responder may, of course, belong to more than one team. For example, an individual may be a member of a local fire department, while also serving on a HAZMAT response team and an Urban Search and Rescue team. In these cases, the candidate would enter the system under his primary team. The other two Team Leaders would then add the credentialed individual to their teams once the primary Team Leader approved the profile.

Designated card distributors

After a card has been approved for production and created, the finished product will be sent to a Designated Card Distributor for final delivery to the recipient. This individual, who is selected by the Team Leader, will arrange to meet the credentialing candidate to activate the card, write the certificates to the chip, and implant both the PIN and biometric signature. This separation of duties provides an additional auditing step. No single person has authority from beginning to end over the process, requiring a second individual to verify the identity of the user.

In conclusion

Illinois has achieved federal interoperability through diligent and focused efforts and effective program design. Many states are looking at the Illinois model with an eye toward achieving interoperability for their own state.

Mr. Glavin is a senior project manager with CGN and Associates and served as project lead for the Illinois First Responder Credentialing initiative.

Securing Macs with smart cards¶ in a Windows environment

As government agencies and corporations embrace Macs, software lets CAC, FIPS 201 and .NET cards secure login via Active Directory.
¶

Making Mac computers work in a Windows world has never been easy. But as more private-sector companies and U.S. government agencies add Macs into their environment, there's a growing need for tools that enable them to operate easily and securely in a PC world. The challenges are particularly difficult in Windows-centric environments with heightened security requirements, such as the need to enforce two-factor authentication via smart cards in order to log in to a personal computer.
¶

Making Mac computers work in a Windows world has never been easy. The challenges are particularly difficult in Windows-centric environments with heightened security requirements, such as the need to enforce two-factor authentication via smart cards in order to log in to a personal computer.

Sunnyvale, Calif.-based Centrify Corp. offers a solution that enables IT administrators to leverage the same management tools and security policies for Macs that they have for Windows users, says David McNeely, director of product management at Centrify.
¶

Centrify is seeing an increasing number of corporations and government agencies using Mac computers, McNeely says. A company's vice president comes in with a MacBook and wants her IT staff to support it. But instead of having different staff handle PCs and Macs, especially in tough economic times, there is a need to have one system administrator for both operating systems.
¶

Using Centrify's DirectControl for Mac OS X, organizations can add Mac computers to their existing Microsoft Windows Active Directory infrastructure. This enables them to centrally manage the authentication, authorization and configuration of Mac OS X systems as well as to lock down the user's desktop environment. DirectControl has been available for more than three years, McNeely says. It has been installed at Fortune 1000 companies and is used by federal customers.
¶

Apple does offer a plug-in so Macs can run in Windows Active Directory, but in order to manage the security settings, preferences and application controls, PC administrators need to use a separate set of Apple tools, McNeely says. "DirectControl enables the PC administrators to use the same Active Directory administrative tools on the Macs that they do on Windows," he says.
¶

While Centrify has the capability to manage both PCs and Macs in a typical security environment where only a user name and password is used for authentication, it also enables smart cards, such as those required by HSPD-12, to be used on Macs too, McNeely says.
¶

In a PC environment, the smart card is inserted into a reader, the PIN is entered and the domain controller validates the PKI certificate and enables the user to log in and seamlessly access other Active Directory-integrated systems, McNeely says. DirectControl allows the same functionality with a Mac.
¶

"The user experience is the same," he says. "The PC administrator only needs to install DirectControl on the Mac and turn on a Group Policy to enable smart card login to Active Directory to work." The Group Policy sets up smart card login as well as the Mac keychain trust for the Certificate Authorities stored in Active Directory, McNeely says, enabling both online and offline login to Active Directory with a smart card.

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**.

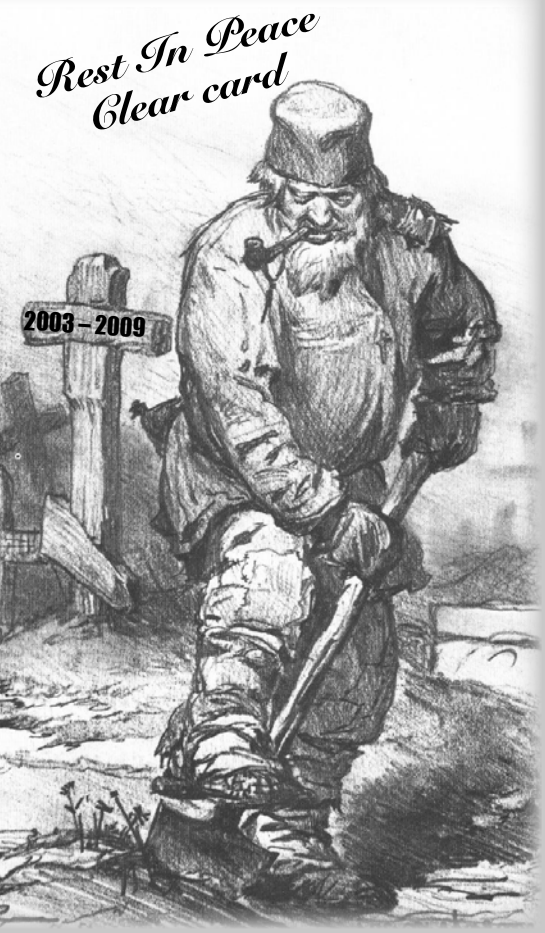
8th Annual Smart Cards in Government Conference 2009

Smart Card Alliance

October 28-30, 2009
Washington Convention Center
Washington, DC

THE YEAR'S LARGEST GOVERNMENT SMART CARD FORUM

FOR EVENT INFORMATION AND TO DOWNLOAD AN EXHIBITOR AND SPONSOR PROSPECTUS VISIT WWW.SMARTCARDALLIANCE.ORG



Does CLEAR's demise signal the end of Registered Traveler?

In a post-9/11 world getting through airport lines was a hassle. Removing shoes, laptops, coats all took time and often lead to lengthy lines.

One solution was to set up a service where individuals would pay a fee, provide information, undergo a background check and receive expedited processing through those security lines. The idea was popular, especially in Congress which held hearings on the programs that came to be known as registered traveler.

After undergoing background checks, travelers were issued smart cards that contained fingerprint and iris biometrics. These cards were used to verify identity before being allowed past security.

The leading company to emerge for registered traveler programs was Verified Identity Pass, or Clear. The company had security lanes at some 20 airports and around 250,000 customers.

But in late June Verified Identity Pass, or Clear, died, leaving behind … well nothing really. And it wasn't issuing refunds.

Cause of death, sources say, was greed. When Clear pitched its program the company guarantee that the airport would receive a flat fee every year as well as a percentage of the membership fees from travelers enrolled. This made it difficult for others to compete in the space because they wouldn't offer the minimum annual guarantee.

Airports should have looked at the program as something to benefit travelers and not as a revenue item, says one source. "The operators and airports saw this as a revenue stream where they should have seen it as something else," says a source.

But some say the program may rise from the ashes. "It's going to depend airport by airport," says Carter Morris, senior vice president of transportation security policy at the American Association of Airport Executives. "Clear was the biggest provider but registered traveler isn't dead."

While Clear ran the majority of the airport gates two other providers also offered registered traveler services. Vigilant Solutions was reportedly still operating in Jacksonville, Fla. and Louisville, Ky. FLO Corp. also had cards issued but the status of the company was not known at press time.

Each of the airports that had registered traveler lanes in place will have to determine its next step, Morris says. "It's going to be interesting to see how the program evolves from here."

Officials at Orlando International Airport, the first to deploy Clear, already made a decision what to do with the lanes in place there, says a spokesperson at the airport. Less than a week after shutting down, the Transportation Security Administration had expanded its Black Diamond lanes in the space once occupied by the Clear program. The kiosks and systems that were once in place have been dismantled, the spokesperson says.

The Black Diamond program has different lanes depending on a travelers proficiency getting through security, for example, Black Diamond is for the experience traveler while the family lane is for less experienced travelers with small children.

Bryan Ichikawa, vice president of the Identity Solutions Group at Unisys, doesn't see anyone

Signs were placed at Clear lanes like the one pictured below at Hartsfield-Jackson Atlanta International Airport announcing the company's demise.

Photo: Viktor Vasnetsov

The Registered Traveler program was in operation in the following airports until June 22:

- Albany International Airport (ALB)
- Cincinnati Northern Kentucky International Airport (CVG)
- Denver International Airport (DEN)
- Gulfport-Biloxi International Airport (GPT)
- Hartsfield-Jackson Atlanta International Airport (ATL)
- Indianapolis International Airport (IND)
- Jacksonville International Airport (JAX)
- LaGuardia International Airport (LGA)
- Little Rock National Airport (LIT)
- Logan International Airport (BOS)
- John F. Kennedy Airport (JFK)
- Newark Liberty International Airport
- Norman Y. Mineta San Jose International Airport (SJC)
- Oakland International Airport (OAK)
- Orlando International Airport (MCO)
- Reno/Tahoe International Airport (RNO)
- Ronald Reagan Washington National Airport (DCA)
- San Francisco International Airport (SFO)
- Salt Lake City International Airport (SLC)
- Washington Dulles International Airport (IAD)
- Westchester County Airport (HPN)

stepping in to take over the abandoned lanes. The cost to run the program is just too great. "They issue a high-assurance credential and just to maintain the security wrapper and the annual audit that's necessary is a huge expense," he says. Maintaining the backend system and staffing costs also contributed to Clear's demise, he adds. Unisys was the contractor for some of the first registered traveler pilots the TSA conducted in 2004.

And with some airlines offering expedited travel lanes at airports and the TSA's Black Diamond program there is less of a need for this type of program, Ichikawa says. "The TSA has done a good job managing its lanes," he says.

Also, the security element of registered traveler isn't there anymore, Ichikawa says. A year ago the TSA stopped requiring background checks for participants of the registered traveler program. "It's a great program," he says. "But it's a cut to the front of the line program."

The long term future of the program is unknown. The TSA did not return calls requesting comment.

The following airports have expressed interest and/or have requested TSA approval for the RT program:

- Baltimore-Washington International Thurgood Marshall Airport (BWI)
- Birmingham International Airport (BHM)
- Chicago Midway International Airport (MDW)
- Huntsville International Airport (HSV)
- Los Angeles International Airport (LAX)
- O'Hare International Airport (ORD)
- Pittsburgh International Airport (PIT)
- Springfield-Branson National Airport (SGF)
- Ted Stevens Anchorage International Airport (ANC)

Toronto Pearson International Airport (YYZ) was currently implementing an RT program.

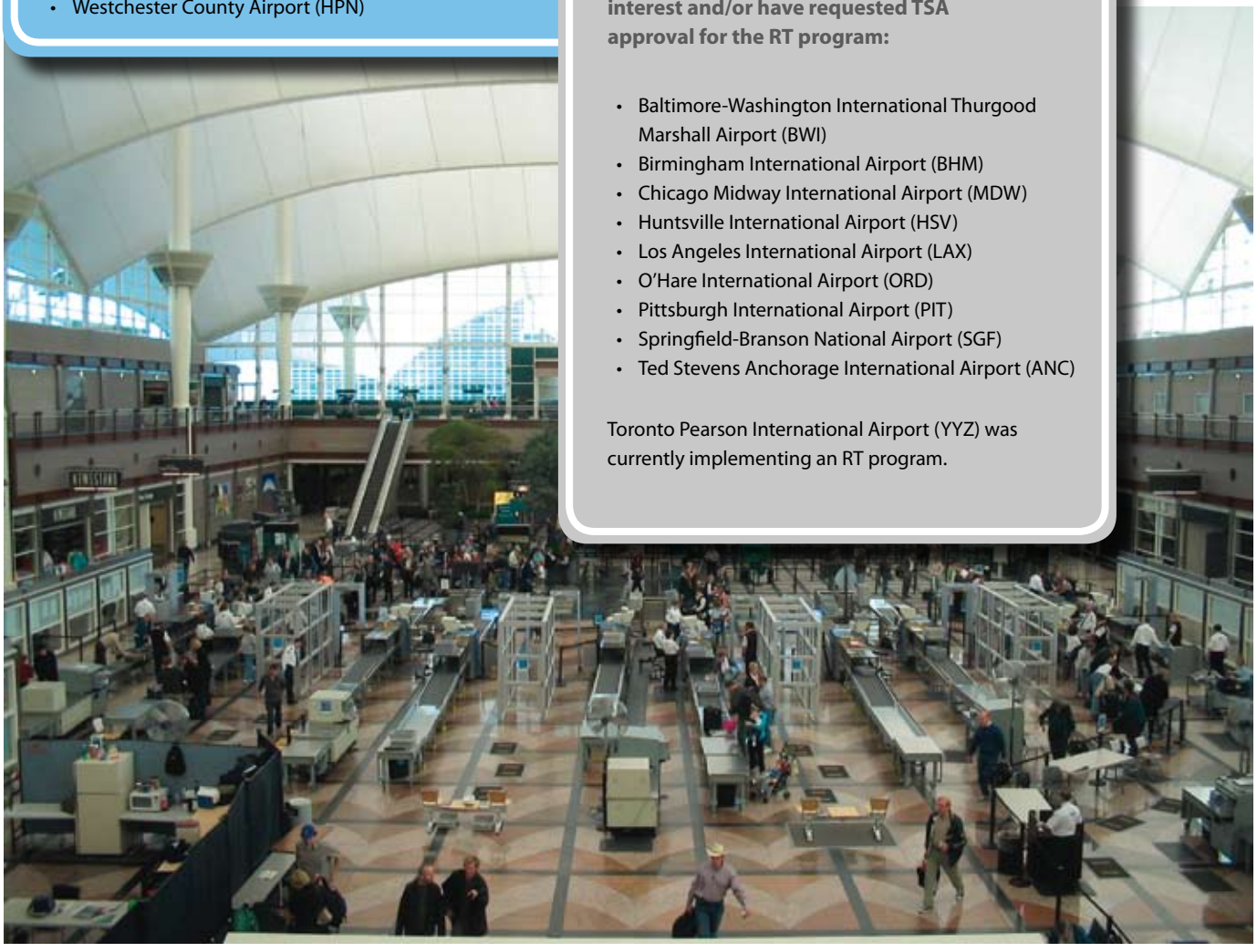


Photo: David Benbennick

New driver license legislation proposed

Debate on whether it increases or decreases security runs rampant

Some believe that new proposed driver license legislation would help states better secure IDs while also protecting citizen privacy. Others say it "guts" an existing law and takes states back to pre-9/11 identity vetting for IDs.

A hearing held in the U.S. Senate Committee on Homeland Security and Governmental Affairs on the proposed bill called the Providing Additional Security in States' Identification (PASS) Act of 2009. Testimony revealed very different takes on the bill that would basically roll back, REAL ID. It's not clear how the proposed change would impact states already complying with REAL ID and rolling out new documents. Even with this new bill looming, some states are still moving ahead to comply with REAL ID.

"The major problem with REAL ID is that it is producing very little progress in terms of securing driver's licenses, and it is not getting us to where we need to be," said Janet Napolitano, secretary of the U.S. Department of Homeland Security. "Simply put, REAL ID is unrealistic."

Citing the almost $4 billion estimated price tags for states to switch to REAL ID and unfeasible deadlines, Napolitano offers up PASS as an alternative. Napolitano, when she was governor of Arizona, had signed a law against REAL ID.

"PASS ID is a critical piece of national security legislation that will fix the REAL ID Act of 2005 and institute strong security standards for government-issued identification," she said.

SECRETARY NAPOLITANO on the hill testifying in front of the Senate Committee on Homeland Security and Governmental Affairs on PASS ID.

> **PASS ID** will enact the same strong security standards set out by **REAL ID** as quickly as **REAL ID** but, critically, this bill provides a workable way to get there.
>
> **JANET NAPOLITANO**, U.S. Department of Homeland Security

"PASS ID will fulfill a key recommendation of the 9/11 Commission, that the federal government set standards for identification such as driver's licenses and non-driver identification cards – and this bill will do so in a way that states will implement, rather than disregard. PASS ID will enact the same strong security standards set out by REAL ID as quickly as REAL ID but, critically, this bill provides a workable way to get there."

Napolitano said that PASS ID keeps document verification and authenticating of source documents, advocates the physical security of ID production, requires that photos of applicants be taken and still has the requirement to show compliant IDs. "All in all, PASS ID would match the security provided in REAL ID, while providing the states with more flexibility to innovate and meet the standards," she said.

How does it differ from REAL ID?

The major difference is that PASS ID gives states different options to meet the criteria. "While REAL ID mandates electronic verification for all source document information, PASS ID would maintain a focus on ensuring the authenticity of identity source documents that applicants present, allowing states to adopt cost-effective ways to achieve or exceed that threshold," Napolitano said.

Since states would be able to choose how to verify identity there would be some cost savings, Napolitano said. The bill would also codify state grants for driver licenses and speed up implementation.

"States would have one year after the issuance of final DHS regulations to begin issuing compliant documents, and would have five years from that date to enroll driver's license holders as they see fit," she said. "The REAL ID deadline

Fifth ICAO Symposium on

ICAO MRTDs, Biometrics and Security Standards

21–23 September 2009
ICAO HQ, Montreal, Canada

ICAO will hold its Fifth Symposium and Exhibition on ICAO MRTDs, Biometrics and Security Standards from 21–23 September 2009. An Exhibition will complement the Symposium and highlight important products and services related to MRTDs, biometric identification and border inspection systems.

The Symposium will focus on ICAO's pivotal role in coordinating the development and implementation of the MRTD Programme as a means of strengthening integral travel document issuance and border security programmes. It will also highlight the United Nations' Global Counter-terrorism Strategy and the importance of ensuring the integrity of the systems through which travel documents are issued. This includes the inspection, verification and examination of ID breeder documents, and serves to demonstrate how effective travel document security can significantly augment activities targeting the detection and prevention of criminal and terrorist mobility.

Your participation is encouraged. Presentations and handouts will be available only in English. Simultaneous interpretation will be available in English, French, Spanish and Russian, as required. For further information on the programme, exhibition, and arrangements for the Symposium, please be sure to visit:

www.icao.int/MRTDsymposium/2009

Efforts are being made to encourage currently non-compliant States to issue ICAO-Standard Machine Readable Travel Documents (MRTDs) by the April 2010 deadline. If your State is not yet issuing these documents please contact the ICAO MRTD Programme for further information.

How do EDLs fit in with new bill?

Unlike REAL ID, The PASS ID bill would recognize the enhanced driver licenses as being compliant with any federal law regarding driver licenses and state-issued IDs, says Vermont Gov. Jim Douglas, who testified at the U.S. Senate Committee on Homeland Security and Governmental Affairs.

STATES ISSUING EDLS

Michigan
New York
Vermont
Washington

Quebec
British Columbia
Manitoba
Ontario

Vermont started issuing EDLs earlier this year and believes they should be compliant with any future requirements. "The importance of Vermont's EDL being recognized as compliant with federal driver's license standards cannot be understated as Vermont's economic, environmental and cultural relationship with Quebec is of paramount importance," Douglas said. "The EDL cost Vermont about $1 million to implement, but more importantly the ease of border travel it creates is key to our economy and our relationship with Canada, Vermont's largest trading partner."

Not including the EDL would create a tough choice for Vermont's citizens. "If the Vermont EDL were not recognized as REAL ID compliant, citizens would be faced with a difficult choice – either carry an EDL for land border crossings to Quebec or carry a REAL ID compliant card for flying and/or accessing federal buildings," Douglas said. "If Vermont's EDL is not compliant, it would become essentially useless as most customers would be better off obtaining a regular license and also maintaining a passport or passport card for border travel."

But Ari Schwartz, vice president of the Center for Democracy and Technology, testified that Homeland Security should rethink the technology used in EDLs and also find a better way to secure any type of machine-readable code on the IDs. "When used for human identification, long range or vicinity-read RFID poses serious threats to personal privacy and security: it reduces user notice and control over when information is collected from the card and enables location tracking of the cardholder because the unique identifier stored on the chip can be easily skimmed (if unencrypted)," he said. "These serious risks make such long range RFID technology inappropriate for human identification and far outweigh the justifications asserted for its use in the EDL and passport card initiatives."

EDLs and the Passport Card use radio frequency identification technology that can be read from 15 to 20 feet and is designed to expedite travel over land border crossings. The chip doesn't contain information other than a unique number that acts as a pointer to a record on a secure database containing the cardholder's photo and other biographic information.

Schwartz would like the PASS ID act to reject the use of RFID and have any machine-readable technology on the card be encrypted to protect the privacy of the cardholder. Also, he believes the data stored on the card should be limited to what's necessary for law enforcement of other officials.

"While PASS ID is a major improvement over current law, the bill should be strengthened to further protect privacy and civil liberties while still achieving security objectives," Schwartz said. "PASS ID provides the opportunity to establish privacy guidance and protections for features of the state driver's license system that will exist regardless of REAL ID."

for completing issuance of compliant driver's licenses is December 2017. If Congress enacts the PASS ID Act as it is currently written by October 2009, states could complete enrollment by July 2016, a full one year and five months ahead of the REAL ID timetable."

PASS ID potentially rolls back one key requirement of REAL ID, checking other states to see if an individual has multiple licenses. Napolitano and others say this was cause for privacy concerns. "PASS ID would not require states to provide direct access to each other's driver's license databases; in fact, the bill contains protections against creating any national identity database containing all driver's license information and requires states to adopt adequate procedures to prevent unauthorized access to

Deciphering IDs in the U.S.

Passports: Typically used to prove citizenship and for overseas travel, but can also be used for general identification such as boarding domestic flights. Since 2007 the U.S. State Department has been issuing electronic passport that have a contactless smart card chip that stores the information on the data page of the passport book.

Passport Cards: Created because of the Western Hemisphere Travel Initiative, the standard ID-sized card enable citizens to cross both land and sea borders without a passport book. WHTI called for greater security at the Mexican and Canadian land borders. The Passport Card is a cheaper alternative than a passport book for those who cross the land borders often. The document contains a long-range RFID chip that is used as a pointer to information about the cardholder that is stored in a secure database.

Enhanced Driver Licenses: Issued by a small number of states, these documents are dual purpose IDs that serve as both a Passport Card a driver license. Applicants must go through a more rigorous background check to receive an EDL than a standard driver licenses. The EDL card uses the same RFID technology that is used in the Passport Card.

Photo: Vermont DMV

or sharing of personally identifiable information," she said.

Opponents see PASS ID as a weak substitute for REAL ID

But what Napolitano sees as privacy protection others see as a security issue. The proposed legislation would basically take driver licenses to where they were before 9/11, says Janice Kephart, a member of the 9/11 Commission and director of national security policy at the Center for Immigration Studies. "It guts the key element of the 9/11 Commission in regards to driver licenses, which is ID verification," she says. "PASS ID pulls the plug on people proving who they are."

Cutting out identity verification isn't the only aspect of PASS ID. Kephart says the bill was put together by the National Governors Association and Napolitano.

The bill creates a new grant process for states to get funding for driver licenses, Kephart says. The new grant process doesn't require states to account for the funds doled out. Also, if states decided to hook into federal databases to check Social Security numbers or passport information the states wouldn't have to pay for the access. "The way it's written it's a windfall for the states," she adds.

The bill would also freeze minimum driver license security and ID standards for states to where they are now, Kephart says. "It's about creating an appearance of security without any real security."

But the biggest issue is still the lack of identity verification, Kephart says. The bill would not require states to store a photo, check birth records, Social Security numbers or passport numbers. "There's no cross checks to make sure people don't have multiple licenses in different states," she says. "The bill pulls back on all significant areas of identity verification."

Kephart contends that the bill would also remove the REAL ID stipulation that individuals could not board airplanes without compliant identification. "You still have to take your shoes off at the airport but the bill says no person shall be denied solely by not showing an ID or driver license," she says.

There are some questions as to whether the bill will get anywhere in Congress. It has been shopped around since Barack Obama was elected, but it took some time before it was submitted in the Senate, suggesting there may be questions as to whether it can pass. "As much as the Senate has not liked REAL ID I don't think any senator wants to be pinned with rolling back a 9/11 Commission recommendation," Kephart says.

> It **guts** the key element of the **9/11 Commission** in regards to driver licenses, which is ID verification. **PASS ID** pulls the plug on people proving who they are.
>
> **JANICE KEPHART**, Center for Immigration Studies

The bill has received White House attention from Rahm Emmanuel, Obama's chief of staff, but the administration has its concerns. "The bill doesn't have the support the administration wants," Kephart says. "It took so long for submission because they were trying to get members signed on."

For this and other reasons it's more likely that REAL ID will get amended, Kephart suggests. The extent of any amendments, however, aren't clear.

Photo: Michigan Department of State

Some states on the way to REAL ID compliance

Despite potential changes to legislation impacting state driver licenses and IDs, Nevada is moving forward to comply with REAL ID. The Silver State, however, is giving its residents a choice of whether or not they want a document that complies with the law.

If the individual doesn't want the new document he can receive one that does not meet the terms of the law, says Tom Jacobs, a spokesman with the Nevada Department of Motor Vehicles. Nevada will start issuing the documents in the fall and will be materially compliant by the first of the year.

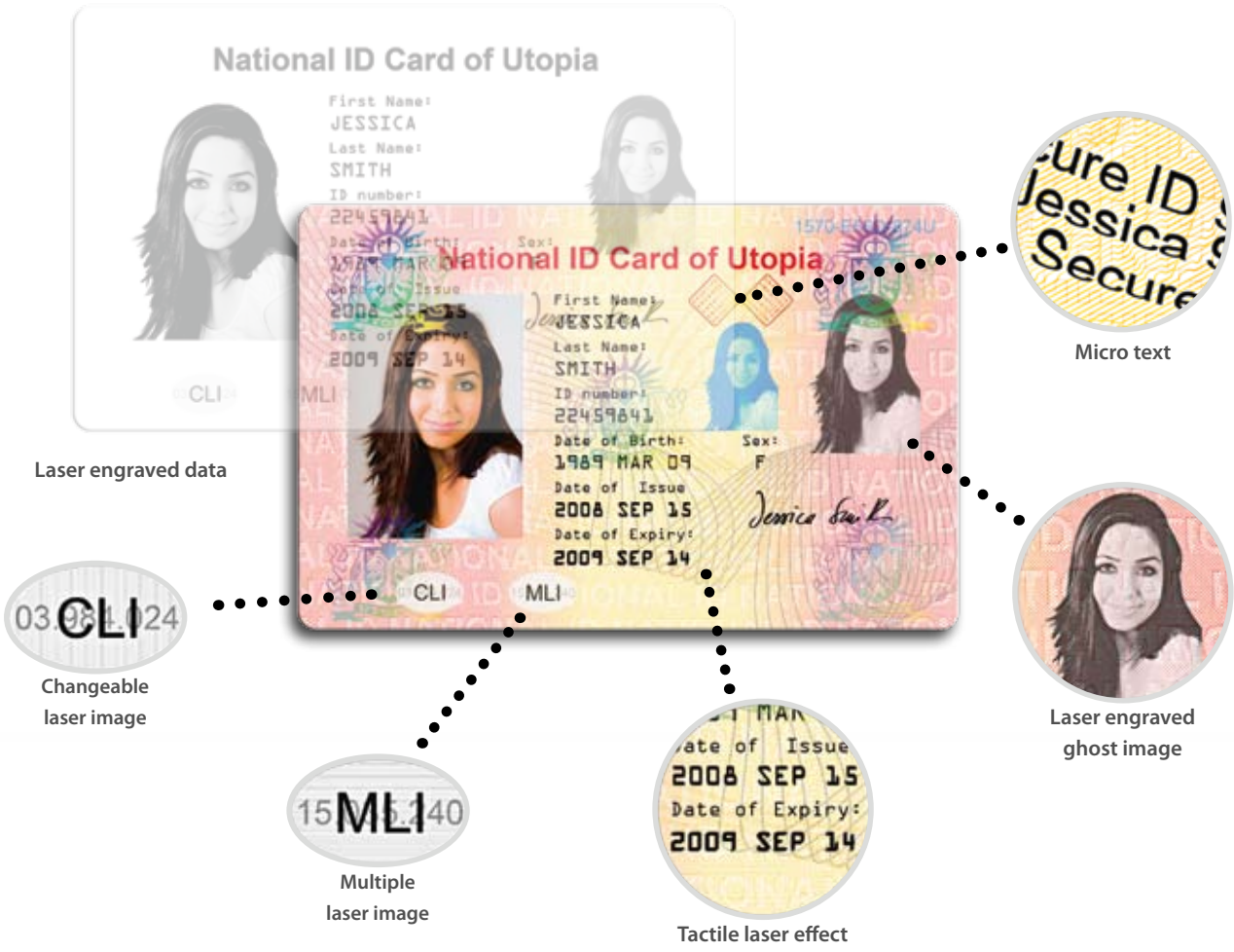
The primary difference between the REAL ID documents and the others are the documents used to prove an individual's identity. Under REAL ID residents can only use seven different documents but Nevada will allow 14 to be used to get a basic license.

The other license won't be REAL ID-compliant and can't be used to enter federal buildings or airports, Jacobs says. The conforming driver licenses and state IDs will have security features that identify it as being such.

There will be no difference in cost between the REAL ID documents and the others, Jacobs says. The state will conduct a marketing campaign to let residents know the difference between the documents and educate them on what they may not be able to do with the non-compliant licenses.

The campaign will also educate residents on REAL ID, Jacobs says. "There's a lot of misinformation out there. It's not as insidious as everyone thinks."

There is no national database of driver licenses, as many say, Jacobs stresses. If a resident wants a REAL ID-compliant document the breeder documents will be authenticated, scanned and stored. States will be able to share access to databases to make sure duplicate licenses aren't being issued but the information is only stored with the state that issues the document.



Laser engraving for secure ID documents catches on

Passports, driver licenses and national IDs already rely on the security feature but other issuers consider use as document fraud rises

A Finnish company called Setec Oy brought laser engraving to the ID document world in the late 1980s when they began issuing engraved driver licenses in Finland. In 2005, Gemplus now part of Gemalto, purchased Setec citing the company's "expertise in the security printing and polycarbonate business," a clear reference to the laser engraving capability. The laser engraving process, however, is not patented and a number of companies provide the technology to the ID marketplace.

Often the emphasis is on the security used to protect the data stored in a card, but what's equally as important are the security features techniques used to protect the data printed on the card itself.

Laser engraving is nothing new, but the price is dropping and more customers are looking at the security feature, says Jonathan Bowen, sales manager at Digital Identification Solutions. The Greer, S.C.-based company released the EDIsecure LCP 9000 Laser Color Personalization System last year, one of the first desktop laser engraving systems that sells for less than $100,000.

Digital Identification Solutions is targeting the printer to the driver license and government markets in the Americas, Bowen says. "Those who have huge issues with forged and faked cards are our primary customers," he says. The company is expecting to ship its first units this fall.

Photos: Digital Identification Solutions

Overseas more governments are using laser engraving or looking at the technology as well, says Chris Dyball, chief operating officer at Lasercard Corp. The Mountain View, Calif.-based company provides national ID systems to a number of countries. Costa Rica's national ID and the U.S. and Canada's Permanent Resident Cards each use laser engraving, he says.

As governments are looking for better ways to secure documents many are finding a solution in laser engraving. "The predominant way of creating images on a card was dye transfer but many are transitioning to laser engraving," Dyball says.

Money matters

But with dye sublimation printers a fraction of the cost of laser engraving why make the switch? "Laser engraving makes it difficult to remove or alter the card information," Bowen says. "The normal person who wants to fake the card won't bother with it, he'll move on to another target. It's also expensive enough to keep the criminal element away and technical enough to where if he got it he wouldn't know what to do with it."

Laser engraving actually burns the information into the card, Bowen says. "It burns through the top level and reacts with the inner card body," he says. "It's impossible to scratch the information off or remove it with chemicals."

Information can sometimes be removed or changed from cards printed on dye sublimation machines, Dyball says. "The image is essentially at the surface," he says. "You can then put a overlay over the dye transfer image but even when you do that you can peel off the patch and take solvent or a mild abrasive and remove it and the fraud would be difficult to detect."

Dye images can also suffer over time, Dyball says. Temperature and humidity can affect the images over time causing them to fade.

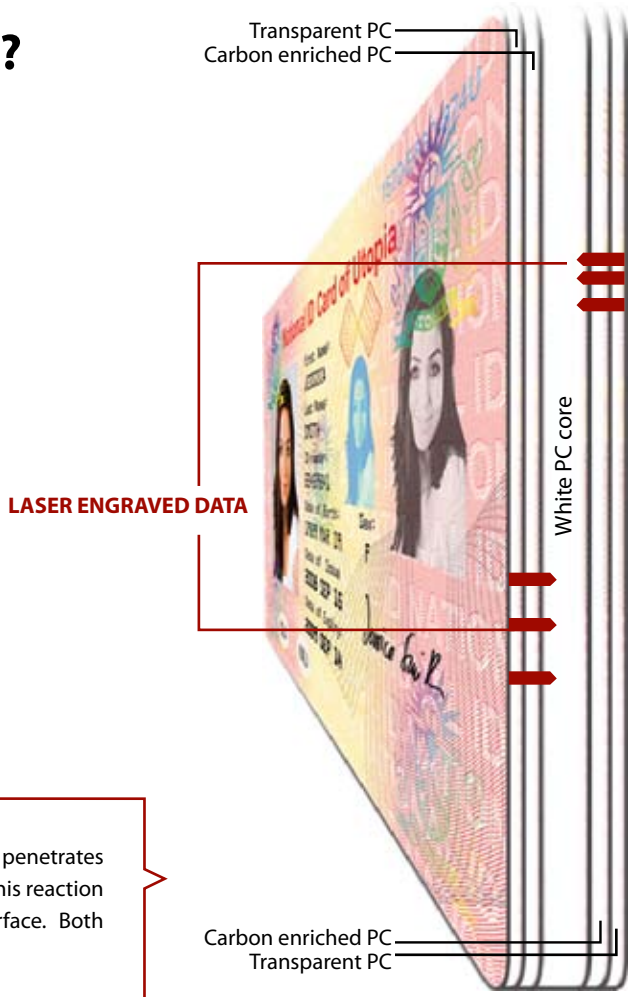
Laser engraving also creates a tactile security feature on the card, Bowen says. When the information is burned into the card body it creates raised ridges that can be felt, similar to an embossed credit card. "When a state trooper pulls someone over and only has a few minutes to validate an ID the tactile feature is great," he says. "It's virtually impossible to forge on a desktop printer."

How does laser engraving work?

Laser engraving is a technology that burns data into an ID card or data page in a passport. It enables standard text and images to be added as well as special security features such as microtext, tactile data, perforated images , and variable images that change with different viewing angles.

Laser engraving can be conducted on various materials, but it works best with documents made of polycarbonate. When a laser beam is applied to the polycarbonate substrate, the heat causes a chemical reaction that essentially burns, or carbonizes, a minute area changing it from white to black. Repeated and controlled application of the laser creates the text and images within the card.

This carbonization process occurs at the material's core and extends up to the surface of the document. Thus laser engraved data cannot be scratched or peeled off of the document because it truly becomes a component of the card's construction. The ability to modify a valid laser engraved document for fraudulent use is virtually impossible.



When a laser is applied to a specially-designed polycarbonate card, it penetrates the transparent outer layer and reacts with a carbon-enriched layer. This reaction creates a dark colored material that moves through the card to its surface. Both the front and the back of the card can be engraved separately.

Laser engraving also has the ability to print changeable laser images and multiple laser images on cards, Bowen says. This enables an issuer to print a last name and date of birth in the same area but depending on what angle you hold the card what is seen changes. For example, at one angle an individual will see the name but at another he will see the date of birth.

To enable this feature an issuer has to make some changes to its card stock manufacturing process and place a small lens on the card body. The laser will then burn the information in at different angles to enable the feature. "It's a security feature you can see with the naked eye and it's impossible to create with any other type of desktop printer," Bowen says.

Laser printers have another advantage, no consumables, such as printer ribbons, Dyball says. People with widely distributed issuance sites are looking at laser engraving because of the savings on consumables," he says. "You have an upfront investment but savings over time."

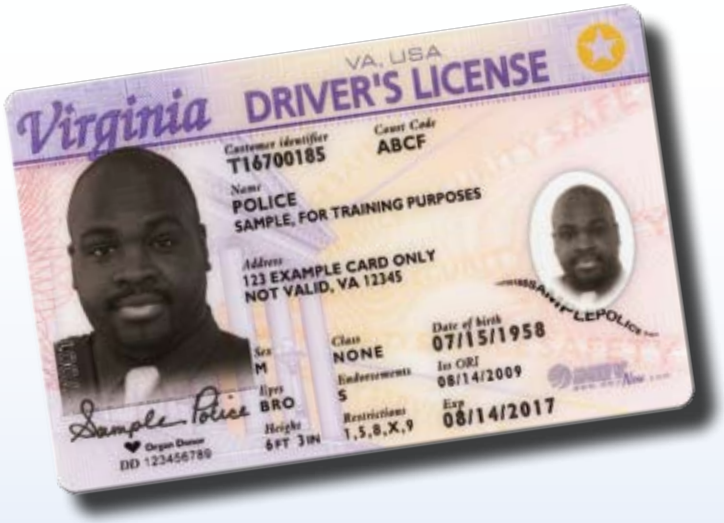
Drawbacks of laser engraving

The high cost is one drawback to laser engraving, another is the inability to print color images, Dyball says. "Laser engraving over the past few years have gotten better at gray scale images," he says, noting that current engravers can modulate the pulse of the laser and get much better gray scale images.

Some still want color, though, and use both dye sublimation and laser engraving. "We have a customer in Italy who buys the card bodies and color prints the photos and laser engraves the text," Dyball says.

As counterfeiters get more sophisticated and governments want to increase security, laser engraving is one solution they may look at. ID

The EDIsecure LCP 9000 Laser Color Personalization System from Digital Identification Solutions is one of the first desktop laser engraving systems.



Virginia begins issuance of new laser engraved driver licenses

This summer, the State of Virginia's Department of Motor Vehicles began issuance of a new, more secure driver license.

The ID has two laser engraved photos, one of which appears in a clear window that is visible from the front and back of the card. It also uses security lettering and ultraviolet features to verify authenticity.

The state has also moved to a centralized issuance model. Rather than producing licenses in the local offices, all credentials are produced in a secure, central production facility. Located in Danville, Va., the site is comparable to a credit card production center with high levels of security and restricted access.

Virginians still go to a local service center to apply for licenses and ID cards, have their photographs taken, and get a temporary 30-day permit to be used until actual card arrives via mail. ID

Major identity programs issuing laser engraved polycarbonate documents:

Driver License			
Virginia	Sweden	Hungary	Estonia
Alberta	Ireland	Switzerland	Slovakia
Ontario	Spain	Portugal	Luxembourg
British Columbia	Holland	Czech Republic	Greece
NWT	Germany	Norway	Romania
Nunavut	Italy	Belgium	Turkey
France	Poland	Lithuania	Bulgaria
UK	Latvia	Malta	
Passport			
Finland	Switzerland	Czech Republic	Singapore
Ireland	New Zealand	Lithuania	
Holland	Latvia	Slovakia	
National ID			
Finland	Hong Kong	Namibia	Switzerland
Holland			

Source: Ian Williams, Identity Systems Group Inc.

Photo: Virginia DMV

2005 2006 2007 2008

OWN THE ENTIRE COLLECTION

1000+ pages of ID technology insight just $200

- 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.

To order, visit *http://store.AVISIAN.com*.

AVISIAN

Searching for 'green' card stock

Sustainable options are still a ways off

Ed McKinley
Contributing Editor, AVISIAN Publications

Polyvinyl chloride – or PVC for short – dominates the nation's plastic-card market despite efforts to find more ecologically friendly materials. Cards made of 100% PVC account for perhaps 90% of all the plastic cards made in North America, according to card-industry executives. Most of the other 10% are composite cards with polyester cores sandwiched between layers of PVC.

"PVC has been honed in our trade for over 30 years for print-grade stock – everything is built around PVC," says Bill Crawford, vice president of sales and marketing for Franklin, Ohio-based Waytek Corp., a materials and coatings supplier to card manufacturers, and a board member of the Princeton Junction, N.J.-based International Card Manufacturers Association.

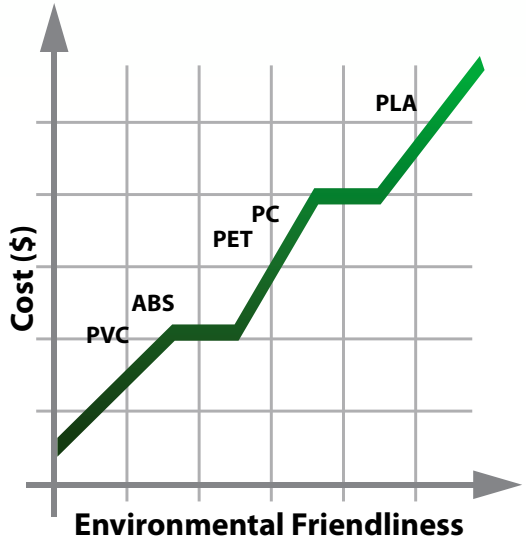
Low price makes PVC the material of choice for most cards. It sells for a dollar a pound, yielding cards that cost about four cents each, much less than cards made from other materials, says Shane Cunningham, marketing communications manager for Digital Identification Solutions LLC, which provides printers and software for creating secure credentials.

The advantages of PVC don't end with price. Manufacturers find it relatively easy to print on PVC and to glue magnetic stripes, Crawford says. Card makers can laminate, hot stamp and die cut PVC, it accepts dye from a variety of printers, Cunningham says. And it is the only card material that "self extinguishes," meaning that if it catches fire it puts out the flame, he adds.

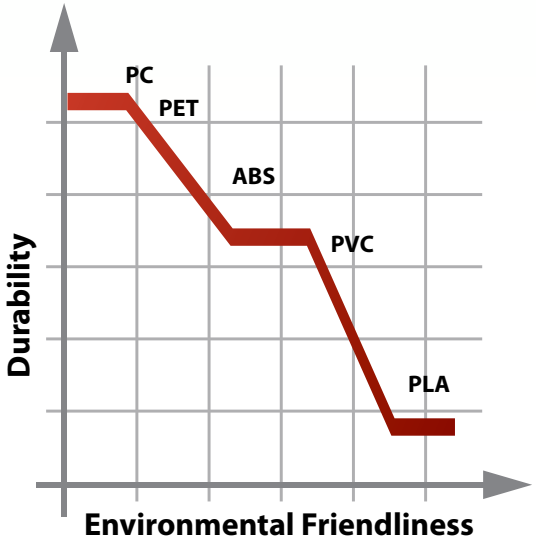
But 100% PVC cards don't last as long as cards made with some other materials, says David Ogonowski, an estimator who handles product development for Denver-based CPI Card Group. That's why manufacturers make composite cards with polyester cores and PVC on the outside, he says.

Depending upon how the public uses cards, 100% PVC versions last two to four years, and composite polyester and PVC cards last four to six years, says Mark Degan, corporate marketing manager for Cornelius, N.C.-based ColorID LLC. In tests on specially designed machines, pure PVC cards break after an average of 30,000 to 40,000 flexes, while polyester survives more than 55,000 flexes, Crawford says.

The price of a card tends to increase as the environmental friendliness of its construction increases.



The durability of a card tends to decrease as the environmental friendliness of its construction increases.



Composite PVC and polyester cards also withstand heat and cold better than 100% PVC cards, says Crawford. Putting photos and birthdates on driver licenses and ID cards with desktop printers can require heat, so those users often choose composite cards, he continues. Credit cards don't require personalization via desktop printers, so 100% PVC works well for them, he notes.

PVC is good for cards, but some say bad for the environment

Still, not everybody loves PVC. While winning the trust of the card industry, PVC has earned the ire of environmentalists. "PVC is the single most environmentally damaging of all plastics," says the Web site of Washington-based environmental group Greenpeace. The organization advocates phasing out PVC because producing it creates the deadly poison dioxin as a byproduct. Burning PVC also can release dioxin into the air, Greenpeace says.

Environmentalists also point out that PVC is not biodegradable. In other words, it will not break down in landfills, making it an objectionable material, they say. Some groups have branded PVC acceptable for long-term use in products that include plumbing pipes and house siding, but contend the material should not find its way into cards used for just a few years.

Environmental concern over PVC is spreading to the general public, says Daniel Gilliland, business development director for Lowell, Mass.-based Mirel, a supplier of bioplastics. The industry is thinking hard about "green" materials "due to card issuers seeing pressure from consumers," he says.

"Retailers, such as Target and Wal-Mart, and card issuers, such as Visa, MasterCard, Discover and American Express, are pushing for green solutions to market to their customers," agrees Brad Paulson, founder of Thor Engineering, a Northfield, Minn.-based consulting company, and ICMA Standards Representative.

The plastics industry has responded by creating biodegradable PVC cards. An additive to the cards attracts hungry microbes that break down cards in nine months to five years, industry observers say. It shares most of PVC's good qualities in the manufacturing process, according to tests by card manufacturers. But it has been available in cards for less than two years, Crawford says, describing the material as in its infancy.

"We're at the mercy of consumers," Crawford says of biodegradable PVC. "At the end of the lifecycle, are you going to recognize a card in your wallet is bio PVC and you're going to do something different with it than you did with your cards that aren't bio PVC?" Crawford asks.

Biodegradable PVC costs slightly more than regular PVC and some fear that as it degrades

it releases harmful toxins into the soil. Regardless, for some card users, making PVC biodegradable will not be enough because manufacturing it still requires petroleum and thus fails to qualify as sustainable.

Replacing petroleum with renewable sources for card materials

The search for renewable materials has led to cards made from polylactide acid – or PLA – mostly from corn in the United States and from sugar cane elsewhere. "We've tried it with potatoes, we've tried it with wheat, and corn does pretty good," says Crawford. "In a few years we might be using something else." Crawford's company, Waytek, does not offer PLA but does make adhesives to bond the PLA to PVC.

PLA advocates, including Brian Glasbrenner, business director, films and cards, for NatureWorks LLC, a Minnetonka, Minn.-based provider of PLA, say the material has the potential to seriously reduce environmental problems.

"The environmental attributes can be really significant when considering something as large as the transaction card industry – which produces something like 19 billion cards each year, says Glasbrenner. "If just 40 million of these PVC cards were converted to PLA," he says, "it would give you the fossil energy savings equivalent to almost 39,000 gallons of gasoline, and the greenhouse gas savings equivalent to driving a car 1,200,000 miles."

Sustainability can provide a convincing argument for PLA among many consumers, but the cards themselves disappoint many in the card business. Cunningham cites problems with discoloration – either a slight gray or yellow tinge – that can reduce the clarity of the images printed on the cards.

Before processing, corn-based cards are susceptible to heat.

"You put corn sheets in a truck and send them three states away, they arrive and it's a solid block of plastic," says one source who requests anonymity. "Then you read on the tech data sheet that you're supposed to keep it refrigerated."

PLA cards need a PVC surface to work in dye-sublimation printers, adds Cunningham. Gluing a magnetic stripe to PLA can present challenges, Crawford adds. Inconsistency plagues PLA cards, according to another industry executive.

Cost is also an issue as PLA cards cost about 14 cents each, compared with four cents for a PVC card, Cunningham says, noting the difference can add up for issuers ordering hundreds of thousands of cards. "We're still a very cost conscious society, especially now during a recession," he says. "Everybody is going green if doesn't cost more."

Though sustainable, PLA cards fall short in another way, according to Crawford. "PLA cards are seldom recycled," he says. "They hate PLA in the recycle stream," he says.

Card recycling has yet to take off

Recycling can provide a selling point for cards, but reclaimed plastic often comes in less-than-pure shades of white that can drive away card-industry decision makers.

"The biggest concern among card manufacturers is being able to offer a consistent color," says T.R. Mitchell, vice president of New Wave Plastics, a Medina, Ohio-based recycler.

To overcome the problem of impure whites tinged with yellow or gray, New Wave is working with Bolatron Performance Products, a Newcomerstown, Ohio-based sheet manufacturer that supplies the card manufacturers with print stock.

"Through this partnership, we have developed a program where we offer 80,000 pounds of consistent loads so we don't have the problems of discoloration with recycled cards," says Mitchell.

Yet skepticism of recycling remains. "It definitely makes the whites look ugly," says Bill Crawford, vice president of sales and marketing for Franklin, Ohio-based Waytek Corp., a materials and coatings supplier to card manufacturers, and a board member of the Princeton Junction, N.J.-based International Card Manufacturers Association.

"Everybody likes to print on gorgeous virgin white stock and when you start to use recycled PVC in your stock it will look gray and streaky," Crawford maintains. "Are you OK with your logo on streaky gray stock?"

Off-white card stock also can change the shades of the colors printed upon it, thus changing the look of company logos, says Shane Cunningham, marketing communications manager for Digital Identification Solutions LLC, which provides printers and software for creating secure credentials.

> **Recycled PVC is "more of a PR thing than anything else."**

Other than color, recycled polyvinyl chloride – or PVC for short – performs almost exactly the same as virgin PVC in card manufacturing and processing, industry executives agree.

Recycled PVC has yet to establish a significant share of the market but could increase in popularity as consumers become more environmentally conscious. "We have been training society to recycle for many years," notes Mitchell.

Crawford acknowledges that recycling could provide a selling point in some markets, such as gift cards, and suggests that marketers could capitalize on the discoloration as a mark of recycling authenticity. "There are some specialty applications where green is important and looks are not," he says.

PVC is hard to beat

However, contrary to what some recyclers believe, PVC can be recycled. Recycled PVC works just about as well as virgin PVC in the manufacturing process, but cards made of recycled PVC often appear gray and cost slightly more than virgin PVC cards, Crawford says. Making a card of recycled PVC requires less energy than using virgin PVC, but the recycled-PVC cards cost more, Crawford says.

Besides turning to recycling, the search for greener cards has precipitated inquiries into other types of plastic.

Still, not one of the alternative plastics stands above the others or above PVC in all three criteria of sustainability, processability and functionality, says Tom Mucenski, business manager, card films for Gordonsville Va.-based Klöckner Pentaplast, a supplier of plastic films. His company has tested a number of plastics for those three characteristics.

Another study of eight common plastics, conducted by Waytek, indicates PVC requires the least energy to produce and that making PVC results in the second-lowest greenhouse gas emissions, Crawford says. The tests did not point to any one superior type of plastic, a result echoed in later studies by Thor Engineering.

"It will be quite some time before alternative green plastics meet the physical requirements and pricing provided by PVC, which makes it difficult to provide reliable and cost-effective 'green' cards," says Thor's Paulson.

ABS, PET and others challenge PVC

One plastic, called acrylonitrile butadiene styrene, or ABS, may someday undercut PVC on price in North America, says Cunningham. ABS costs less than PVC in Europe, but U.S. manufacturers don't make ABS because of their focus on PVC, he says.

Adding the transportation costs from Europe or Asia makes ABS more expensive here than PVC, he continues. Although ABS is more durable than PVC, it can't withstand direct-to-card printers and instead requires retransfer printing, says Cunningham.

Meanwhile, some card industry executives are turning their attention to polyethylene terephthalate, or PET, as a card material because it is recyclable. PET costs more than PVC, but it is more durable and can withstand direct-to-card printers, Cunningham says.

In such cases, a company marketing department could justify the expense of recycled PVC, which costs more than virgin PVC, Crawford says. Even when demand exists for cards made of recycled plastic, recycling the cards themselves might not make sense, according to Crawford. Driving two blocks to recycle a card would cause greater environmental harm than throwing away the card, he says.

Still, some are finding ways to make recycling the cards pay off. "We have set up a few programs with different manufacturers, where they will send cards to us and we will reprocess them and send them back," Mitchell says. "However, the cards cannot be intermingled; they must be 100% PVC to do this."

Crawford suggests the alternative of making cards from PVC used to make plumbing pipes or house siding. The use of PVC in building materials far outstrips the amount of PVC used in cards, he says.

In fact, he questions the need to recycle cards because of their relatively small amount of PVC. "The card industry use of PVC is insignificant compared to the packaging industry, the construction plastic – those markets are huge compared to the small amount of plastic you're carrying in your wallet," says Crawford.

Cunningham says his company has not received any requests for recycled PVC. He calls cards of recycled PVC "more of a PR thing than anything else."

cause Americans recycle so many milk containers made with PET or with amorphous polyethylene terephthalate, called APET, and oriented polyethylene terephthalate, called OPET. All offer more strength than PVC but present personalization challenges and cost more than PVC, Crawford says.

Polyethylene terepthalate glycol, or PETG, has gained popularity as a card material in Europe and Asia, Crawford says, and yields cards that look as good as PVC. Environmentalists consider PETG green because incineration presents no problems, he notes, and its lamination temperature is lower than that of PVC.

Europeans and Asians also have taken to polycarbonate, or PC, which incinerates to water and also offers durability, resists heat and accepts laser imaging, Crawford says. High cost presents a drawback, he notes.

The olefin family of plastics, including polypropylene, or PP, and polyethylene, or PE, has many variations and could become an alternative, Crawford says. Among types of resins captured in the recycling system, high-density polyethylene, or HDPE, places second in volume, and PP is third, he says. Olefins are light in weight, which reduces transportation costs, he adds, while noting the difficulty of printing on olefins.

Polyhydroxyalkanoate, or PHA, is a naturally occurring plastic made in bacteria cells, Crawford says. Natural enzymes can digest the material and thus return it to nature, he says.

While most of the industry explores the world of plastics for card materials, some manufacturers have turned to wood, sometimes with the grain intact, says Cunningham. "That might be a more biodegradable card," he says of wood, "but I don't know if you're saving the planet if you're killing the trees to make cards."

"Fundamentally, cards can be made from anything," notes Thor Engineering's Paulson. "Green materials need to provide the reliable functionality at competitive prices that is provided by the plastics currently in use."

Jim Colleran, project manager, global support, for Irvine, Calif.-based HID Global, summarizes his company's experience with green cards this way: "We're seeing a lot of questions but very little real demand. That part of the market is really young."

Plastics
commonly used in ID cards

PVC – Polyvinyl chloride
Most common material used in North America for ID cards. OTHER APPLICATIONS: pipes for construction industry, cling films, juice bottles and food packaging, etc. Plastic Identification Code 3.

PET (also called Polyester) – Polyethylene terephthalate
Used in combination with other materials such as PVC to add strength to plastic cards. There are various forms of the plastic resin or polyester as it is called in the textile industry. OTHER APPLICATIONS: beverage bottles, flexible food packaging, thermal insulation, textiles and boat sails. Plastic Identification Code 1.

Composite (also called Poly-Composite)
Plastic cards labeled composite most often consist of PET at the core with PVC outer layers. PET increases the card's durability while PVC keeps it low cost and easy to print on via standard dye sublimation card printers.

ABS – Acrylonitrile butadiene styrene
Most common material used in Europe for ID cards. OTHER APPLICATIONS: pipes for construction industry, automotive parts, golf club heads and toy Lego bricks. Plastic Identification Code 7 (shared with PC and others).

PC – Polycarbonate
Commonly used in ID cards that are personalized via laser engraving techniques. There are numerous types of PCs that are used frequently for injection molding processes. OTHER APPLICATIONS: single use and reusable drinking bottles, CD/DVDs, tubing and Apple computers. Plastic Identification Code 7 (shared with ABS and others).

PLA – Polylactide acid
Biodegradeable polyester made from renewable sources such as corn and sugar cane. Marketed for plastic card use under the name corn cards but only nominal use to date. OTHER APPLICATIONS: medical sutures, stents, plastic cups and food packaging.

Become more informed, more competitive, and more profitable.

IN A NEW YORK MINUTE.

Security with an emphasis on now. That's what these times demand, and that's what ISC East delivers. Conveniently local and globally relevant, ISC East is where top security professionals gather for the latest in product innovation, premier education, and bottom-line business building relationships. More than 300 exhibitors, enhanced demo theater and New Product Showcase all make this the place to see the widest variety of state-of-the-art products in the industry.

Secure your place. Register for free at:

WWW.ISCEAST.COM/RID

Where the best in the business come to better your business.

- Access Control
- Alarms & Monitoring
- Biometrics
- Fire Control
- Public Security & Safety
- Remote Monitoring
- Systems Integration
- Video Surveillance
- Wireless Applications
- and more...

CODE: AD12

International Security Conference East® is a registered trademark of Reed Elsevier Properties Inc., used under license.
©2009 Reed Elsevier Inc.

SPONSORED BY: SIA Security Industry Association

PRODUCED BY: Reed Exhibitions

ENDORSED BY: CASIA

CORPORATE PARTNERS: AXIS Communications, DSC, HID, Honeywell, Infinova, NAVCO, PELCO by Schneider Electric, GVI Security

Riding Seattle's rails, ferries, buses, ORCA style

Andy Williams
Associate Editor, AVISIAN Publications

Stands to reason that a transit card with large ambitions should be named after a whale, doubly so when that card serves Seattle a city where whale-watching is big business. When it involves replacing multiple types of fare media while linking seven disparate transit systems, you know the ORCA card is aptly named.

ORCA, stands for One Regional Card for All. It was rolled out in April and covers Washington's five county Puget Sound area, and serves a population of about 1.5 million.

"It replaces about 300 different kinds of fare media and links seven transit systems, including commuter rail, buses and ferry," says Candace Carlson, regional contract administrator for Central Puget Sound in Seattle. "Five of the seven had paper regional passes which were in many different denominations," says Carlson. "When we are fully deployed, the options will be ORCA or cash, period."

The seven agencies service about a half million riders a day on more than 2,000 buses, a dozen ferry terminals, a dozen commuter rail stations and, starting in July, light rail. There is also the van pool program which some agencies use for disabled individuals, says Carlson.

A consortium, made up of the CEO from each of the seven transit agencies, started the ORCA card program six-years ago. "Trying to link the seven agencies was encouraged by the state of Washington nearly 15-years ago," says Carlson. "The state was urging the agencies to make it easy for commuters, which led to technology studies and eventually to selection of the smart card."

Leapfrogging to contactless

In the beginning the card technology choices were limited. There was the ubiquitous mag stripe card or the new kid on the block, contactless. Given there was no infrastructure that needed upgrading, it made sense to start with the latest technology, she says.

"Contactless suits the complexity of the fares we have and it works well in an operating environment because there are very few moving parts," says Carlson. "It also adapts well, such as with a bus's heavy vibrations or when you have to wash down the buses with hoses," she says. In other words, the readers can withstand the day-to-day operations of a major transit system.

On April 29, 2003 an agreement to implement a smart card system was signed by the seven agencies in the Central Puget Sound Regional Fare Coordination Project: Sound Transit, King County Metro, Community Transit, Everett Transit, Pierce Transit, Kitsap Transit and Washington State Ferries. The $43 million contract was awarded to ERG Transit Systems and it was originally anticipated to be operational by 2006. The first ORCA card, however, wasn't officially rolled out until three-years later.

Once the ORCA contract was awarded to ERG they company started planning and designing the system, says John Winyard, Seattle project director, ERG Transit Systems, a subsidiary of Vix ERG, which was acquired by Cubic in July. ERG started testing ORCA in 2006 but additional features caused some delays. "We felt like we had a functioning system, then we began adding new features for the second part of the design phase. We completed the final phase late last year and went live in April."

Powering ORCA is the MIFARE DESFire chip from NXP Semiconductors, the high-end of the MIFARE chip family. ERG provides and manufactures the nearly 3,000 readers for the system, adds Winyard.

ORCA also has portable fare transaction processors that are used at ferry terminals or rails for verification. On the rail the system features standalone processors that look like parking meters. The customer taps his card before boarding then taps the card when he exits so the system knows how much to charge.

Photos: ORCA

Deciding who gets how much

Using one card to service multiple transit operators can be a challenge, but ERG's clearinghouse is designed to make it easier to ensure each of the transit agencies gets paid, Carlson says.

Larry Weissbach, ERG's general manager for the Americas, compares this clearing house software to that used by NASDAQ or the New York Stock Exchange. It enables the system to keep track of how much each agency is owed.

"We keep a record of the value on the card for e-cash and passes and at the end of the day all transactions are processed. We use a number of business rules to apportion funds to each agency," says Winyard.

Another complexity comes up with serving the business community. The Puget Sound transit agencies had always catered to local businesses and the University of Washington. This created different rules than those required by individual cardholders.

Since the university and some companies in the area subsidize travel cost for employees there was additional complexity to the project, Carlson says.

It will probably take about a year to complete the business side of the ORCA rollout. Services for individuals should take about six months. "Business accounts are timing their conversions for when their contracts are up," says Carlson.

The business account program as established by ERG, includes a Web portal that enables employers to manage accounts. "With ORCA, businesses will now have controls they never had," says Winyard. For example, if someone leaves a company, his ORCA card can be quickly locked out.

Three apps on the chip

The ORCA card can conduct three different types of transactions: a regional pass product that enables travel on transit services in the region for a specified period of time; an agency-specific pass, like a bus or ferry pass; and stored value, or an e-purse.

For example, if you're riding the bus, tap your ORCA card on the card reader on the bus as you board. If your card is loaded with an e-purse, the cost of the trip will be deducted from the transportation value in your e-purse. If you have a regional pass or agency pass loaded specific to the agency operating the bus, the reader will recognize your valid pass as fare payment.

The card has to be set up this way to make sure the different agencies are paid properly. There are also consideration from some of the businesses. Some of the business account subsidies only cover certain modes of transportation. But an employee could establish his own e-purse if he wanted to use the card for other purposes, says Carlson.

The card can be reloaded by phone, mail, on the Web or the rider can visit ORCA's customer service office. Some retailers also off autoload vending machines.

Smooth operation

When ORCA was still in startup mode, says Carlson, "there were some technical issues, which we expected, particularly with the way data is communicated to buses through wireless systems. But customers have been very understanding."

Winyard says there have been no glitches yet, "no real problems. Things have gone very smoothly and the ridership is building."

With the publicity ORCA has received, Carlson says she has already been approached by other transit agencies outside the Puget Sound area that want to join when, and if, the system is expanded.

"The way our contract is written, any agency in Oregon or Idaho can join our system," says Carlson.

Physical location doesn't impact the system, Carlson adds, noting that the central system clearinghouse is located in Concord, Calif.

"The system was designed to be scalable and was largely paid for via federal grants, so this is an effective way to amortize that investment by extending the resource to other properties," she says.

"It also helps the original core partners by spreading the costs over a larger group," she notes. "To date, only geographically adjacent properties have expressed interest in joining, but it's an interesting option for other agencies to consider."

Winyard says "two or three other agencies are monitoring ORCA very carefully," and it would not be a problem from ERG's position, to expand. "The more the merrier," he concludes.

FIPS 201 and India National ID, interoperability anyone?

Unique Identification Authority of India names 'Secretary of Identity'

Salvatore D'Agostino
CEO, IDmachines

A race is on, not unlike the race to the moon and we will see if the United States can catch up with the rest of the planet when it comes to identity credentials. We continue to tout the progress that has resulted from HSPD-12, its expansion to the private sector as evidenced by the activities of the 4 Bridges Forum and the continued expansion and evolution of FIPS 201. However, in terms of strong digital IDs, the EU is at 100 million as opposed to 10 million in the U.S. and India just upped the ante.

India has announced plans to roll out a national identity credential for 1.1 billion citizens and to get it going by 2010. The India Congress Party actions bode well for the Indian and hopefully global identity industry.

It's not surprising that one of the world's most dynamic economies and the world's largest democracy has decided to make identity infrastructure a priority. While not *surprising* it is *impressive* that the Indian government leveraged the mandate of the recent election (are you listening President Obama …).

India will create a cabinet level position for the Unique Identification Authority of India and has already named their Secretary of Identity touting entrepreneur, Nandan M. Nilekani, a founder and former chief executive of Infosys Technologies. Nilekani will leave his post as a co-chairman of the board to take on the ID card project.

Here in the U.S. we rightfully want to address finance reform, economic stimulus, expanded health care, climate change and other initiatives. It's great that the Obama administration has decided to show leadership on these important topics. But creating a national identity infrastructure should be the first step in addressing most of these issues (even emission trading is facilitated by a multi-purpose credential).

It seems that the rationale for the investment is well understood in India and articles in the media all make points of the benefits of investing in identity.

These sources cite, among other things, that the program will create 100,000 new jobs, streamline government to citizen disbursement, reduce fraud in benefits to the citizens (e.g. think savings in Medicaid, Supplemental Nutrition Assistance Program, Unemployment Benefits, etc.), and enable secure citizen to government transactions among other things.

All represent goals in play in this session of the U.S. Congress. In the U.S. we have yet to realize that identity runs across these programs. Neither Congress nor the Obama administration fully realize the leverage an identity investment gives to all of these legislative, policy and economic goals.

There are bits and pieces of identity in different bills and no coherent overarching approach. No offense to the ornithologists or vegetarians but we are missing the opportunity to kill more than one bird with one stone.

One interesting article even proposed skipping a generation of identity credentials and basing the national ID on a SIM card. This is a fascinating idea particularly given the capabilities of today's mobile devices.

This is clearly the future and while it's not a likely outcome in the India case (don't think that mobile devices have sufficiently penetrated to the 1.1 billion individuals who will be covered) but the fact that it's being discussed shows how an investment in identity has the potential to leapfrog the technology base of countries. Maybe it will be an option and if so it will create a whole new concept of mobility.

You have to give props to the Indian government for their initiative and good luck to Nilekani.

Finally, is anyone making the argument that India should be looking at FIPS 201 as a basis for their credential specification. More than most global ID specifications it meets the needs for multi-use by combining contact and contactless interfaces, logical and physical access control, strong authentication, digital signatures and encryption, and continues to evolve (e.g. match on card, contactless mutual registration, secure channel, elliptical curve).

Is it possible that we could be entering the world of "Identity Diplomacy" where the U.S. Ambassador in New Delhi has interoperable identity credentials as part of his brief? This would certainly be a boon to economic cooperation and another way to leverage the global investment by industry in FIPS 201.

Photo: Sandeep Dhirad

Featured FIPS 201 Products

Patriot Smart Card Holder
EK Ekcessories, Inc.

The FIPS 201 approved Patriot Smart Card Holder by EK Ekcessories is reliable, easy to use and significantly reduces loss of important credentials. ID cards slide in and securely lock into place, the Patriot holds up to 2 cards and features an open face that allows the card to be visually inspected without being removed, the Patriot easily attaches vertically or horizontally to soft end lanyards, Split rings, or retractable reels for easy accessibility while providing you with maximum security. The Patriot and all EK products are proudly Made in the USA.

TrustBearer Desktop & TrustBearer Access
TrustBearer Labs

TrustBearer Desktop is a smart card middleware product that supports both PIV and CAC smart cards on Windows, Mac and Linux operating systems. It provides the interface between the smart card and the applications that utilize the digital certificates on the card. Supported uses include network authentication, SSL client web authentication, digital signing of documents and emails, encryption, and VPN authentication. TrustBearer Access enables web applications to authenticate smart cards, USB tokens, and software certificates in addition to usernames and passwords. It supports SAML, OpenID and the TrustBearer SDK.

Newly approved FIPS 201 products

CHUID Card Reader (Contactless)

E-Plex 5800
Kaba Ilco Corp.

Electromagnetically Opaque Sleeve

SkimSafe - RFID Opaque Sleeve
Laminex, Inc.

Non-metallic Dual RF Blocking Badge Holder
National Laminating, Inc.

Fingerprint Capture Station

PIVSuite SDK with Cogent CS500e
Aware, Inc.

Cogent LiveScan Fingerprint Capture Station with CS500e Scanner
Cogent Systems, Inc.

OCSP Responder

AUTHENTX OCSP SERVER
XTEC INCORPORATED

PIV Card

Gemalto TOP DL with ActivIdentity Digital Identity Applet Suite
Gemalto, Inc.

TecSec Eagle Card
TecSec, Incorporated

Single Fingerprint Capture Device

E6500, M4400, M6400 w/ UPEK TSC1 Single Fingerprint Capture Device
Dell, Inc.

FC320U
STARTEK Engineering, Inc.

P6000
Zvetco Biometrics, LLC

Transparent Card Reader

Dell External USB Keyboard with Smart Card Reader
Dell, Inc.

E4200, E4300, E6400, E6400 ATG, E6500, M2400, M4400, M6400 w/ Broadcom USH Smart Card Solution
Dell, Inc.

Omnikey 4321 ExpressCard SmartCard Reader
Omnikey Americas

VISIT FIPS201.COM TO RESEARCH AND COMPARE APPROVED PRODUCTS

Mobile handsets and NFC tags help keep Pakistani children healthy

Near field communication may be hyped because of its payment abilities, but a health care project in Pakistan is helping save children's lives and showing the flexibility the technology can enable.

Called an Interactive Alerts system, it was designed by NextLab at MIT, Cambridge, Mass. and Interactive Research & Development of Pakistan (IRD), a Karachi-based non-profit company that offers low-cost health care technologies for developing countries. Indus Hospital, a 150-bed care center in Pakistan, is also involved in the project and Nokia has provided NFC handsets to support the initiative.

"The purpose of the project is to conduct surveillance for early childhood pneumonia in preparation for a vaccine trial," says Dr. Aamir Khan of IRD. Using the NFC phone as a reader makes it easier for IRD staff to compile information on the children, he says.

While the project started in 2007, it didn't begin enrolling children until November 2008. Khan says there are about 3,000 children enrolled in the program, but the aim is to get another 1,500 involved.

Using NFC phones to access immunization records and essential health alerts

At the time of their six-week vaccination visit, children are given an RFID tag embedded in a bracelet. This tag provides a unique ID to the child, and parents are advised and encouraged to take sick children to participating general practitioner clinics or general hospitals in the program.

The Nokia 6131 NFC phone scans the child's tag. Pertinent immunization, clinical and laboratory data is collected and posted to the server in real-time and can be viewed over a secure Web site.

The objective for collecting this data is to provide policy makers in Pakistan and in the region the information required for introducing new vaccines against pneumonia, a leading cause of childhood death in countries with high under age five mortality rates, according to IRD. The same system can also be used to track other diseases, such as meningitis, sepsis, severe dehydration, tuberculosis and malaria, says Khan.

This approach helps overcome the challenges of disease tracking and patient referral in settings where medical records and referral systems do not exist, says Dr. Khan. The RFID bracelet provides the information that health workers need to verify identity, view basic medical records and respond to emergencies quickly.

New Nokia phone could (finally) herald commercial NFC deployments

Even though full commercial deployment of NFC is a ways off–by some estimates several years away–one handset manufacturer well positioned to take advantage of the new technology when it does go mainstream is Finnish handset manufacturer Nokia.

Its newest NFC phone, the Nokia 6216 Classic is its first commercial NFC device incorporating the European Telecommunications Standards Institute (ETSI) single wire protocol standard (SWP), says Damien Balsan, Nokia's head of NFC Business Development.

At first the phone will be deployed primarily in Europe and Asia since that is where most of the NFC projects are taking place, says Balsan. "However, we also hope that some carriers in the Americas will use the phone for their NFC roll outs or pre-commercial deployments."

Probably the most important addition to this new phone is that it is Nokia's first SIM-based NFC device. "It allows operators to securely store contactless NFC payment and ticketing applications on the SIM card. The advantage is that you can easily take your applications with you when you swap phones," says Balsan.

Earlier Nokia NFC phones, such as the Nokia 6212 classic, did not support SIM-based NFC transactions. Instead the transaction information was stored on the memory of the device, Balsan says.

The Nokia 6216 classic is Nokia's third NFC device, says Balsan. "Bringing a SIM-based NFC phone to market was a strong requirement from the carriers and the GSMA and remained an obstacle to major roll outs."

The Global System for Mobile communications Association (GSMA) has been encouraging NFC launches and that they follow ETSI recommendations, including the single wire protocol standard for interface between the SIM card and the embedded NFC chipset.

"In addition to the benefits of SIM-based NFC transactions to the operators, the Nokia 6216 classic benefits the consumers as they could utilize these new services easily and conveniently if the infrastructure is set up," says Balsan. "They could use the device as their travel card, contactless credit or loyalty card. A lot of the infrastructure for this already exists in countries where contactless credit or debit cards have been deployed."

But Balsan believes other functionalities will also be deployed. "The ability to use the phone as an NFC tag reader with smart posters will trigger many new applications for segments of users that don't browse the internet yet. NFC also provides easy access to digital content and services. Having all this on the phone, which has a 3G Internet connection, allows users to access services thru just one tap."

Developers and integrators from all over the world, he adds, are starting to build up a contactless ecosystem for different applications. "The phones and SDK are accessible thru Forum Nokia at http://www.forum.nokia.com/ and tags are available from different manufacturers recommended by the NFC Forum."

Overall, the new device brings NFC one step closer to widespread rollouts. "There is a lot of work needed to be ready for a fully implemented NFC Ecosystem in 2010 and we hope to see more devices from other handset makers. We believe that the 6216 will help carriers prepare for a wider roll out," says Balsan.

Photo: Nokia

The NFC Forum unveiled its "target mark" to show consumers where to touch to activate an NFC interaction. Within a year, the Forum is slated to issue a certification program for device compliance testing.

One of the challenges was "figuring out the social acceptability of bracelets and cards," says Dr. Khan. "We went for the bracelet form factor in very young infants, although all patients have the option of taking a card only."

When the patient is examined at a participating clinic the practitioner can generate an "interactive alert," a text message, to the doctor or health worker, who can respond as needed, including visiting the patient at the clinic, adds Khan.

The genesis of this project came from an initial 2008 MIT class on information and communication technologies, recalls Luis F. G. Sarmenta, research scientist at MIT Media Lab. That class has since evolved to become part of MIT's Next Billion Network initiative, called "NextLab," which focuses on new cell phone technology. The initiative is aptly names as one billion new people are expected to become regular cell phone users over the next couple years.

"During this class, our students communicated with IRD, and produced a basic working prototype of the idea," says Sarmenta. "We then handed the source code to IRD, and they continued to develop it themselves, adding many more features and integrating it into their other mobile systems."

What IRD coders did was design a data capture and reporting system called "Interactive Alerts," says Khan. The system enables a health worker or doctor easy access to a patient's records. After scanning the bracelet, the doctor can log in to a Web site to review the patient's data and see if they are scheduled for any treatment. For example, has the patient missed a vaccination.

Why NFC instead of other types of identification, such as bar codes?

NFC technology was new to the IRD team. Khan had never heard of it before it was suggested by Sarmenta's team. "We had considered other RFID readers, but none on cell phones," says Khan.

"NFC requires a simple tap. Phones that take pictures of bar codes need to be handled in just the right way to get a readable picture," says Khan. "There is often no time in the general practitioner clinics for this, and they would almost never make a second attempt if the first one did not work. Some see more than 100 patients in three hours."

Khan says the program has been very successful, but IRD is trying to figure out a way to further entice physicians to use it.

"We are trying to figure out what incentives to provide the general practitioners to get them to use the system," says Khan. "What does this bring him? More patients, more referrals? The system definitely works, but to scale up to the next level, we need to package the incentive of participation for the physician without transferring the costs on to the patient," he adds.

Buyers, Researchers, and Technology Leaders—Here It Is!

The Big Event in Biometrics

Supported by the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA), the Biometrics Consortium Conference is focused on Biometric Technologies for Defense, Homeland Security, Identity Management, Border Crossing and Electronic Commerce.

The Conference will be two and a half days of presentations, seminars and panel discussions with the participation of internationally recognized experts in biometric technologies, system and application developers, IT business strategists, and government and commercial officers.

The Biometric Consortium Conference and Biometric Technology Expo are pleased to welcome the co-located IEEE International Conference on Biometrics, Identity and Security (BIdS) to Tampa this year!

Keynote Speakers:

John M. (Mike) McConnell, Senior Vice President, Booz Allen Hamilton, Former Director of National Intelligence

Louis E. Grever, Executive Assistant Director, Science & Technology Branch, Federal Bureau of Investigation

Join nearly 2,000 participants, including:

- 100 speakers
- 60 Federal, State and local agencies
- 25 Universities
- Biometric Industry, System Integrators and Users

www.biometricconference.com

Biometric Consortium Conference and Technology Expo

Loyalty goes high-tech with advanced ID technologies

Rewards keep customers coming back and smart cards, cell phones make it personal

Loyalty programs are all about keeping customers. In a down economy, holding on to the business you have is more important than ever. While some businesses create their own loyalty programs, solutions providers can help do the heavy lifting and ease the burden that these programs can place on retailers or card issuers.

A new player in the loyalty market is working to tie retail loyalty to the consumer's mobile phone. "It's all about tethering the consumer to a brand via a mobile device," says Jay Highley, president and COO of loyalty provider Tetherball LLC.

Tetherball offers customers mobile coupons, mobile rewards (frequency or purchase-based), mobile sweepstakes, and mobile notifications.

Tetherball's approach is to target audiences by identifying what a business' customers want and then delivering a mobile campaign that involves interaction on the part of the customer. This is what Highley calls "permission-based mobile coupons" and can include rewards, sweepstakes and notifications.

Highley defines mobile loyalty as creating a trusted relationship with members. "These members have already held up their hands and said they want to hear from you, but do it in a way that's relevant to me and creates value," Highley says.

Tetherball is working with Dairy Queen (DQ) and Indiana-based Hotbox Pizza. "We're also doing work with McDonald's and a number of other national brands," he says.

What makes Dairy Queen stand out is that it's the first use of a contactless smart loyalty tag, a sticker that can be affixed to a cell phone to identify the user through Tetherball's platform, says Highley.

"The program is easy to deploy, easy for a user to sign up. A customer comes into a store, sees the POS displays for a free blizzard (milkshake). To join the DQ mobile rewards program, he texts a key word which says go to DQ," says Highley.

The customer comes to the Tetherball platform and follows the opt-in process. A text is sent to the DQ counter and the customer is presented with his own Tetherball tag, which he can attach to the phone.

"Once they get that tag, they then tether it. They text a unique ID number on that tag to tetherball tying it to the cell phone number. To redeem offers (that they receive on their cell phone via SMS message), they just wave the tag in front of a reader," says Highley.

Blizzard anyone?

Dairy Queen is using the loyalty program in a variety of ways. The chain is sending offers to customers to increase business during slow times. They also use it to reward frequency. For example, a location could offer a Blizzard special that's only good between the hours of 3 pm and 6 pm, explains Highley.

"One Dairy Queen (location) ran an ad for a free tax relief ice cream cone on April 15, tax day in the U.S. It had 112 members visit the store that day and more than 50% of those visitors purchased other products. That's the power of mobile," says Highley.

Tetherball clients are able to send offers to their customers or members via standard text messaging. These coupon-type offers are then redeemed electronically using contactless point-of-sale terminals or stand-alone kiosks provided by Tetherball.

Mobiquitous, a real time Web-based reporting system, delivers the coupon redemption rates and overall program performance. It provides clients with real-time visibility so that they can adjust quickly and leverage the real time nature of mobile marketing. "When you login you can see your stores and see what offers are working, your redemption rates. It opens up a whole new dimension of analytics and usage and it gives the retailer a chance to customize what his member receives," says Highley.

Tracking is accurate and real time. "That's the significant difference between other forms of couponing which can take you weeks to gather that information."

Tetherball also ensures that only the intended user redeems a coupon. "The coupon can't be forwarded, it can't be copied, you can't use fake codes and it can't be sold online. It even prevents theft at POS, such as an employee giving away free product to a family member," says Highley.

One tag can also serve an infinite number of loyalty programs, says Highley. For example, even if a tag is obtained at Dairy Queen it can be used at other retailers that are associated with Tetherball as long as it's registered.

"We've only seen six percent of members electing to opt out … to put it another way, 94% have stayed in the program. That's going back two years when it was first created," says Highley. "Those are game-changing types of numbers that demonstrate the value of what we're delivering for our clients."

Welcome's solution builds loyalty to one payment card over the others

Welcome Real-time started 12-years ago in Aix en Provence, France. According to Aneace Haddad, Welcome's founder and chairman, the company was launched to help retailers get marketing value out of

their point of sale systems and payments infrastructure. In the late 1990s, Welcome applied its expertise in smart card technology to help banks get a better return on investment from the mandated migration from magnetic stripe cards to chip cards. Since then, Welcome has focused almost entirely on banks.

Called Welcome XLS, the software offers instant rewards when a cardholder conducts a transaction, explains Sebastien Slim, vice president, product marketing. Loyalty through payment cards can be achieved through a variety of cardholder rewards, including gift cards, discounts, e-coupons, cash back and points.

Generic campaigns are driven by the transaction amount and provide bonuses when the customer reaches a predetermined threshold. Other campaigns provide rewards based upon a cardholder's purchasing behavior, his last visit, number of visits, amount spent and quantity of items bought per visit. There are also event-driven campaigns that are dependent on times and events, for example, first card use, birthday and even a happy hour, says Slim.

Coupons or e-coupons can be issued through a point-of-sales terminal, ATM, mobile device, Web site as well as via more traditional marketing channels, such as being mailed with a statement.

In the beginning, Welcome's solution was geared around contact chip cards and offline transactions. Today, the company supports any card technology. "Most of our customers using chip cards are now using our online solution whereby the customer data are stored on our server and not on the chip. The main reason for this is that we can support 'Card Present' transactions as well as 'Card Not Present' transactions in the online configuration. Also banks do not have to reissue cards," says Slim.

Many licensees, many uses

Right now, Welcome has about 30 licensees worldwide, including Visanet Brasil, Maritz, which handles Welcome in the U.S. and Canada, Barclays in the UK, Alphabank in Greece, PBZ bank in Croatia, BPI Bank in the Philippines, Venture Infotek, a transaction processing company in India, and the National Commercial Bank of Saudi Arabia.

There are a variety of reasons that banks offer Welcome's loyalty programs, but most do it to differentiate from the competition, Slim says. "Visa in Brazil went with our solution to compete against MasterCard. It was a way to enhance existing payment systems," he says.

Interswitch in Nigeria, another Welcome client, uses the solution to promote payment cards. "It's not Visa versus MasterCard here," says Slim. "Cash is king and they're trying to incentivize the use of electronic payments as opposed to cash."

Photo: Jim Corsaii

Dairy Queen is using the loyalty program in a variety of ways. The chain is sending offers to customers to increase business during slow times. They also use it to reward frequency.

The changing market for converged security products

Scott Howell
Director of world wide marketing, Hirsch Electronics

A number of critical market trends are aligning in an unprecedented manner leading to a market disruption that could dramatically change the logical and physical security arenas.

These game-changing trends include many factors.

Growing need for security

Market demand continues to grow for more effective solutions to secure buildings, information and people to address increasing identity theft, financial data fraud, litigation, attacks by disgruntled workers, network attacks, regulatory compliance pressures, geopolitical threats and more. Organizations are increasingly seeking to establish a significant level of trust for identities/people, information and devices.

Technology maturity

The technology is also advancing and maturing. After decades of sputtering adoption they are seeing dramatic market growth. The market is now embracing these enabling technologies:

Smart cards:
Smart cards and other tokens such as USB flash memory drives containing smart chips are becoming the de facto standard for portability of secure digital certificates.

Public key infrastructure (PKI):
Huge certificate authorities (CAs) have been stood up to utilize digital identities. And massive interconnect trust networks have been established for shared trust using PKI. Digital certificates are almost universally recognized as the best method to ensure effective identity verification and security.

Biometrics:
Advancements in processing power and algorithms have enabled most biometric technologies to realize 99% or greater accuracy. Biometric is now recognized as the best way to ensure the card holder is the card owner.

Physical security products:
Physical security products are increasingly IP-enabled, facilitating new, advanced applications utilizing interoperability with other network devices, applications and databases.

Contactless technology:
Data transmission via radio waves has proven itself secure and highly convenient for a wide range of applications such as access, identity and monetary transactions (e-payments). Even emerging technologies such as near field communication (NFC) are seeing rapid transition from the successful pilot to wide-scale commercialization.

Proven implementations

There is a proliferation of countries utilizing digital certificates in a variety of applications, from national IDs to e-health. These successful implementations have helped establish infrastructure, use cases, best practices and have driven down costs.

Mandates

Governments and industry groups are stepping in and mandating that sophisticated systems for identity and security management be applied for a wide range of applications

including electronic passports, citizen identification cards, banking, voting and welfare services.

Vulnerabilities of digital assets

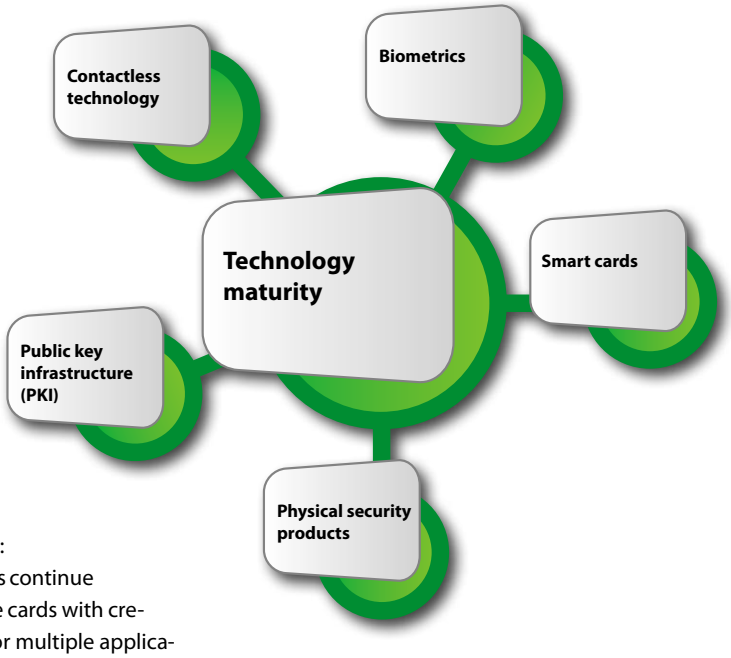
Advanvced ID technologies are also being used to protect digital assets. Computer log-on is most commonly secured by a single authentication factor – the password. Cybersecurity experts repeatedly point to the extreme risk inherent in password-only access and proof stories are starting to gain traction. Just as PC manufacturers are starting to offer hard drive encryption as standard, similarly smart card log-on, encrypted e-mail and digitally-signed documents will soon become the norm.

Convergence

Several technologies and organizational factors are converging:

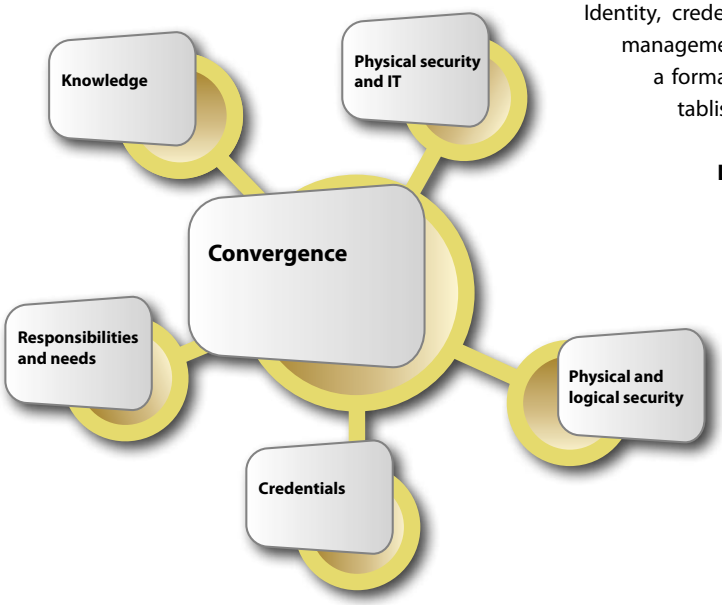
Convergence of physical security and IT:
Physical security products have moved from dedicated networks to IT's networks and from myriad protocols to one protocol – IP. This not only eliminates a physical network of wires and lowers costs, but also provides a common infrastructure and communication protocol to facility interoperability.

Convergence of physical and logical security:
Organizations increasingly demand a single card to access both building and computers. This functionality enables companies to utilize a person's physical access as a policy for network access, defeating external hackers in the process.



Convergence of credentials:
Organizations and countries continue to implement multipurpose cards with credentials that can be used for multiple applications, such as, facility access, computer log-on, payment, identification (voting, welfare services, etc.) and health records.

Convergence of responsibilities and needs:
Organizations are changing the way they evaluate, buy and utilize identity and security solutions. Due to technology convergence and the critical nature of these deployments, the IT department, physical security team, facility management, and executives must all work together to evaluate and install a security solution. Security objectives must now align with and support the overall organizational objectives.



Convergence of knowledge:
Identity, credentialing and access management is evolving into a formal discipline with established best practices.

Lower costs, improved services

Organizations are realizing lower costs and better services through digital identity systems.

The health care industry is one sector that is aggressively applying security and identity technologies to safeguard patient health records, improve patient care, and streamline claims management.

Success and return on investment (ROI)

There is an increasing recognition that effective security can lead to organizational success. The effects of a single breach – costs of remediation, loss of customers, litigation, penalties and reputational costs – can put a company out of business. Therefore, organizations are increasingly seeking to establish a significant level of trust for identities/people, information and devices. Through trust and security, companies can achieve sustained, profitable growth and continuity by utilizing effective security and identity management systems to mitigate risks, reduce potential liabilities, vet identities, enforce policies, prevent negative incidents, avoid and defend against lawsuits, reduce insurance premiums and claims, comply with regulations, pass audits, and ensure privacy of personal information.

As these trends indicate, the security and identity market is truly in the midst of dramatic change.

Biometrics on campus

While usage remains light, hand scanners are making their presence felt on some college campuses

Biometrics aren't exactly taking the college world by storm but it is gaining traction in some areas. While the technology can be expensive, some schools are finding uses that both aid in identification and, in light of the current budget crunches, recoup what otherwise might be lost income.

Most campus card providers offer biometrics as an option to their college clients. And most of these providers use what can only be described as the big biometric provider on campus, Ingersoll Rand.

"We're on most campuses because we have a broad product line that includes door locking systems as well as biometric readers," says Bob Bazemore, director, education solutions, Ingersoll Rand.

Bazemore estimates IR is on some 100 campuses, mostly in the U.S. Surprisingly, the biometric of choice isn't a fingerprint reader but one that reads the hand geometry.

Read Winkelman, vice president of sales for colleges and universities at The CBORD Group, says biometrics is viable in certain situations. "We haven't seen the demand for biometrics as the primary credential, but have seen it as a form of secondary authentication, usually in higher security areas, such as computer labs." He says about ten CBORD schools have biometrics installed, nothing "a number are research institutions with very expensive equipment."

Some CBORD schools do use a fingerprint reader, but it's for employees and is used with CBORD's point-of-sales system. "As with most POS terminals, registered operators log in to begin their shift. Often this is done with an employee card that is swiped. We have customers who use a fingerprint reader for this purpose instead. They register their fingerprint in the database and use it to log in. We have five or so customers using this application," says Winkelman.

Heartland Campus Card Solutions can also offer fingerprint scanners if their clients want it, but none have asked for it yet, says Fred Emery, Heartland's vice president and general manager. Some say there are privacy issues with fingerprints. "They've gone with the hand. It seems less obtrusive," says Emery.

The University of Georgia has been using hand scanners since they were first created. The Athens, Ga.-based school has had lots of time to experiment with scanners and has had such scanners, and its different versions, in place for more than 35 years. The scanners are primarily used in food services, campus recreation and dorm access, says William McGee, manager of UGACARD Services at the university.

Obviously the university has upgraded its scanners since that first 1972 installation. "The first hand scanner was about the size of a 20-inch TV,"

The HandKey 2 biometric scanner from Ingersoll Rand helps with access and privilege control at the University of Georgia.

says McGee. "It's a beast." The company that first installed that scanner later became part of Ingersoll Rand. The university is now using IR's HandKey 2 scanner.

The university requires either an ID card or the ID number to be physically entered in addition to the hand scan. The ID number is nine digits long. "It's not a hard number to memorize. Most have it memorized in the first week," says McGee of the school's 37,000 students.

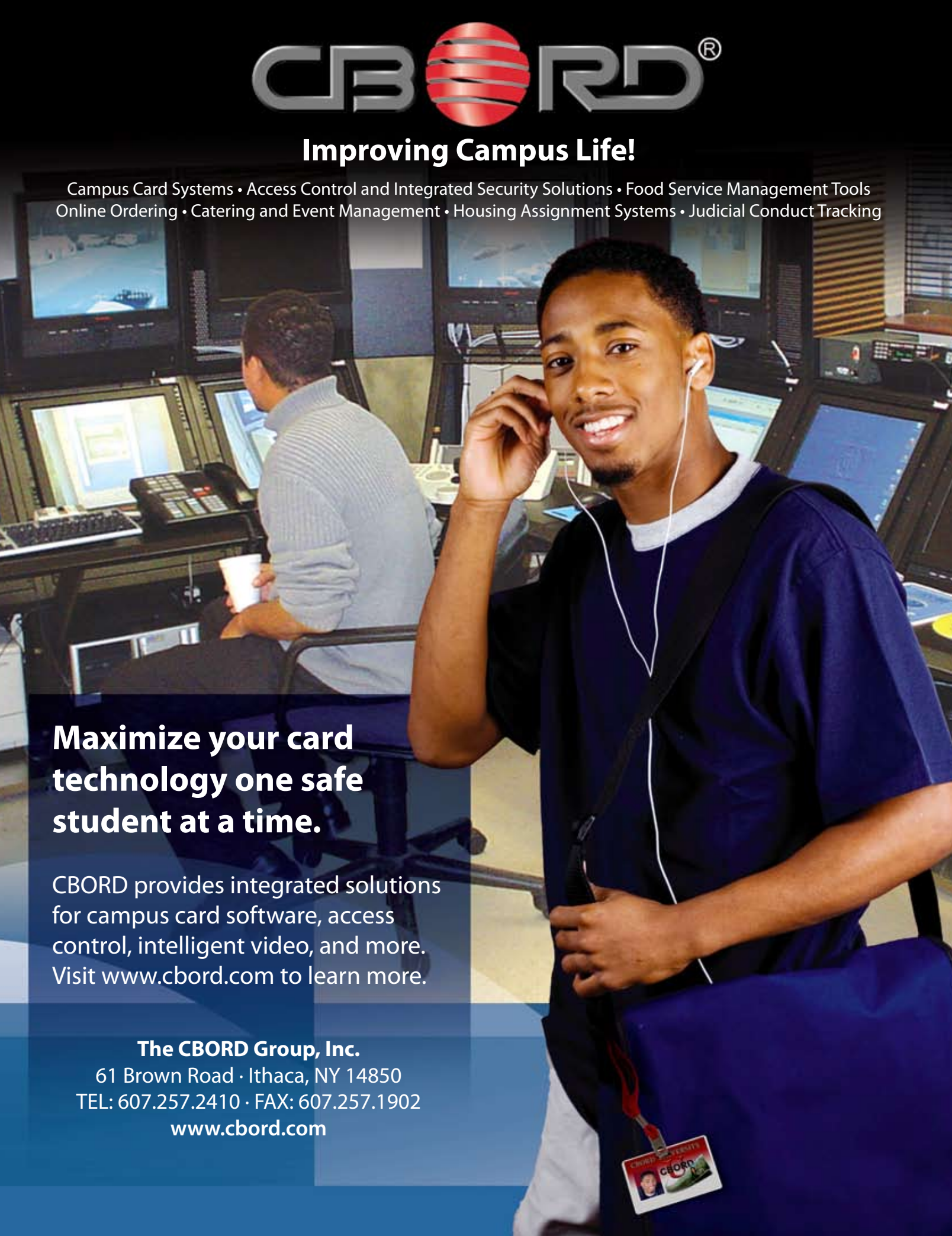
"Biometrics takes security to a new level," says McGee. You're dealing with something you have (the ID card or something you know (PIN) in addition to something you are. "Even if you knew my ID number, your chances of getting in with your hand is impossible and reader locks down after the third attempt," he says.

As far as read times, 30 years ago it was probably in the three or four second range, but now it's much less, says McGee. In addition the scanners have gone from a one-to-many comparison to one-to-one.

Dining services was the group that first brought it to campus. "They were looking for a better way to identify patrons than the meal token, something that could provide quick and easy access. We have an all-you-can-eat program, so whether you come once a day or 20 times a day, you can get service. With a hand scanner you don't have to have staff to physically check the card," says McGee.

He says the university upgraded to HandKey 2 because it provided "better read quality and an outline of the hand so students know where to place their hand. It also includes an antibacterial platen to cut back on germs," adds McGee.

Photos: Univ. of Georgia


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

Biometric authentication ensures that only eligible students are allowed to eat in dining locations across the University of Georgia campus.

Even twins can't fool a scanner

The university is also experimenting with different uses for the scanner. "We had a request from a faculty member who wanted to verify if the right students were taking a test." When students come in, they perform a hand scan and swipe their card and the reader turns red or green so the professor can see at a glance if the student deserves to be there.

"This will prevent other students from taking the test. You can adjust the tolerance to where it's very strict. We have twins who do not show up the same. We had a set that tried to share a meal plan, and that's how we caught them," says McGee.

A convenience for students

Colleges need a good cost saving reason to think about using the technology, says Emery. Budget shortages could be holding the hand scanning technology back because they are more expensive than a mag-stripe reader or PIN pad.

Two Heartland clients are Emory University, Atlanta, and Hofstra University, Long Island, N.Y. – have biometrics systems in place, says Emery. "They use hand geometry scanners from Ingersoll Rand integrated into our solution so they communicate to our access control software."

For Emory University, hand scanners are about student convenience. The school uses them at one of its recreation facilities so students don't have to carry a card to get in, says Emery.

At Hofstra, they were to increase security in some of the residence halls and entry ways. "They wanted to harden access to the dorms and to make sure a student couldn't hand the card out the dorm window to another student for access," Emery says.

For ease of use hand geometry is great, however, it's not for all buildings. "If you go into a computer lab or library, a lot of campuses would feel it's overkill. You can do more with a regular card, or card plus a PIN," says Emery.

"A lot of people like (hand scanners) and would like to do it, it's just a matter of practicality and cost. It's very fast but not as fast as an RFID or mag- stripe read," adds Emery.

Why hand scanners?

The speed of hand scanners make them a good fit for college campuses. "A fingerprint doesn't work as well in a high volume capacities like you find at universities," says Ingersoll Rand's Bazemore. "You need to get a lot of people through very quickly."

IR's top scanner is the Schlage HandKey 2 used by both CBORD and Heartland schools. The only difference from Handkey 1 is the casing. The first version had a white metal housing while No. 2 has a polymer case which means it comes with a lower price tag. Even though it is more esthetically pleasing, it's not as durable, says Bazemore. "It will last as long except in an abusive environment" which a university can tend to be. "The white metal casing, they don't kick it but once," laughs Bazemore.

The popular idea now is to use the card and then place a hand on the scanner. The scanner compares the students hand against a stored template, or mathematical representations, and performs a one-to-one match. The template can be stored locally on the device or on a network. Bazemore says the price of the scanner, which is basically a reader, is around $2,000, he says.

Many hand measurements, small file

When a student first enrolls a hand, the device takes a 3D photo that captures it from several angles, says Bazemore. "It takes about 90 different measurements and converts that to a 9-byte file. Later, when you put your hand on the scanner it only does a one-to-one match." In other words, it checks the current scan against the store 9-byte file associated with the cardholder.

Bazemore says he's seen no decline in schools wanting biometrics because of the recession. In fact, it may be driving schools to put in such programs. "They may be looking for tighter controls over their meal programs to make sue everyone is paying," says Bazemore. "They're trying to keep someone from giving his card to a buddy and two people coming through and shorting auxiliary services out of a fee. This stops all that."

For a technology that's 30-plus years old, which is a lifetime in this computer-driven age, it's hard to imagine that biometrics on college campuses is still at the infant stage, meaning a smattering of schools here and there are actually using it.

CBORD's Winkelman believes it's not the cost so much as universities wondering if they really need two forms of identification. "It's kind of the same story we've had with smart cards. There are some neat applications and some things they can do, but mag- stripe is so ubiquitous and easy to implement. When you talk about hand recognition, how many vendors are out there? A lot more are providing mag-stripe cards."

Have you gained access to Biometrics Certification?

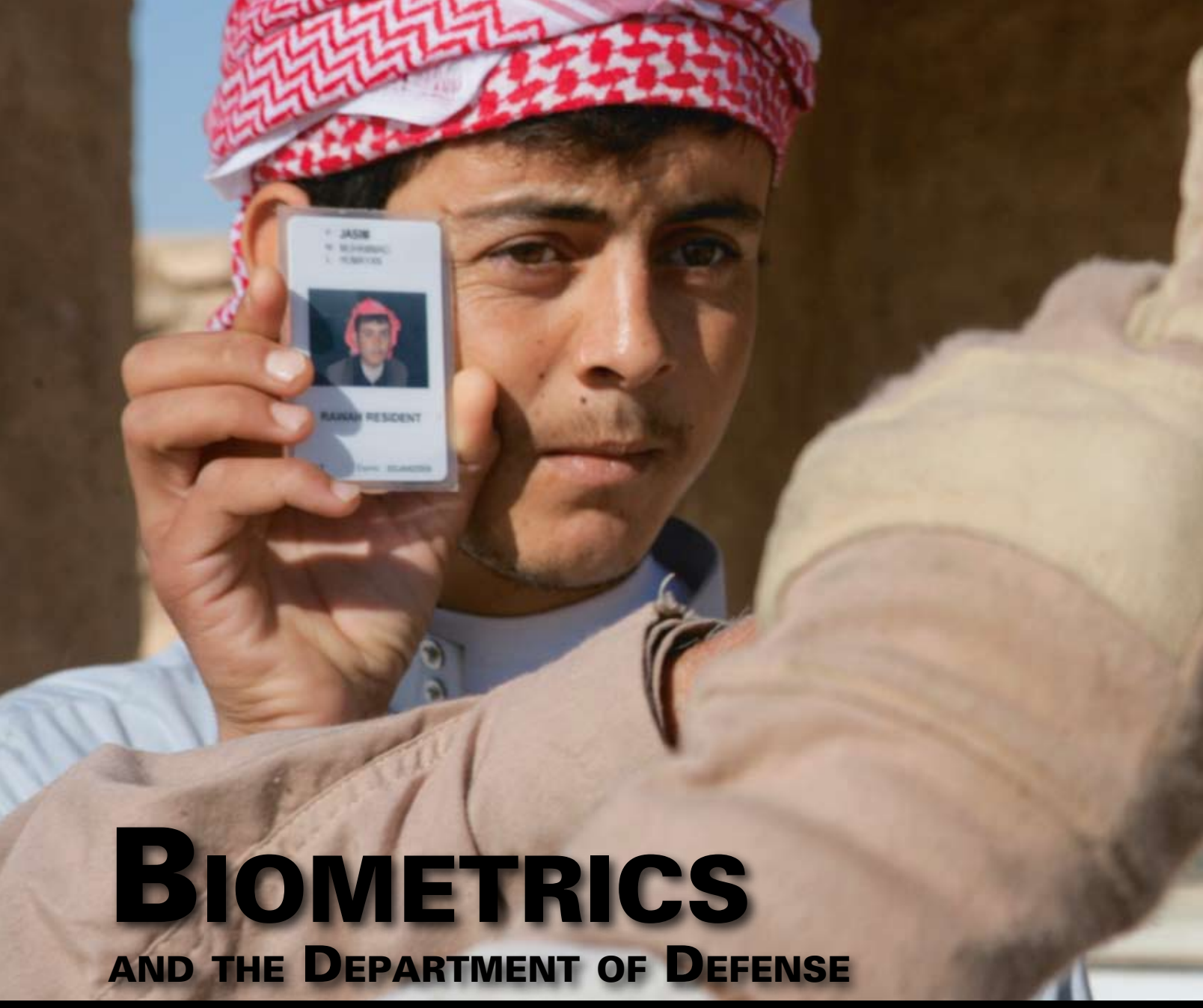
Access is now being granted to qualified Biometrics Professionals.

IEEE, along with some of the world's leading biometrics experts, has developed a new certification and training program for biometrics professionals and their organizations. The IEEE Certified Biometrics Professional™ (CBP) program focuses on the relevant knowledge and skills needed to apply biometrics to real-world challenges and applications.

- Certification: Earning the IEEE CBP designation allows biometrics professionals to demonstrate proficiency and establish credibility.
- Training: The IEEE CBP Learning System combines print materials and interactive online software – ideal for job training, professional development, or preparing for the CBP exam.

To gain access to more details, visit www.IEEEBiometricsCertification.org.

IEEE



BIOMETRICS
AND THE DEPARTMENT OF DEFENSE

The U.S. Department of Defense has been a leader when it comes to smart cards with its Common Access Card, but the agency is also forward thinking when it comes to biometrics.

The Defense Department is using biometrics in a variety of ways, including overseas for access to bases, at crime scenes to collect forensic information and at some facilities in the U.S. for access control, says Lisa Swan, deputy director for the Defense Department's Biometric Task Force. The agency is even using multi-modal biometrics, a combination of face, fingerprint and others, to identify individuals in different circumstances.

The Biometric Task Force is a division of the U.S. Army but it works across the Defense Department to enable biometrics. Key to the agency's efforts is its next generation Automated Biometric Identification System (ABIS), which was launched Jan. 30 with the help of prime contractor Northup Grumman.

The ABIS is used in a variety of ways, including storing forensic evidence collected from crime scenes, Swan says. "We take latent fingerprints from improvised explosive devices, sniper rifles and store them in ABIS," she says. The database contains around 3 million records, including fingerprints, palm prints, photos and iris scans, Swan says. Previously the database stored just fingerprints.

ABIS incorporates multi-modal biometrics, Swan says, using more than one biometric technology to ensure a match. For example, ABIS could have a fingerprint and face record stored that might be partial records but not of the best quality. Yet, if this data is taken in context with other information it may be enough for a positive identification.

"You get a score on a fingerprint that's not high and a face that's not high, but fused together it will provide a potential match," Swan says. The FBI's next generation IAFIS will have similar functionality.

This feature and information can be useful when hiring individuals for jobs on U.S. bases abroad. Before being allowed on base soldiers collect the individual's fingerprints, iris and photos to run against ABIS, Swan says. "That print may be tied back to a latent print and that's something you want to know before hir-

Photo: U.S. Dept. of Defense

Soldiers in the field use handheld devices to collect and check the biometric information. There are around 6,000 devices deployed between Iraq and Afghanistan.

ing someone," she says. Fingerprints are also run against FBI files as well.

If a foreign national passes the background check he is then issued a smart card that contains his biometric information, Swan says. The card and biometric are verified each time he arrives on base. Soldiers in the field use handheld devices to collect and check the biometric information. There are around 6,000 devices deployed between Iraq and Afghanistan, Swan says.

Biometrics were also used to help residents of a village near Fallujah in Iraq, Swan says. The village was having problems with insurgents and asked the Army for help in identifying residents. "We identified everyone in the city, and issued them a credential with a biometric," she says. "People use that to gain access to their own space. You don't have to have one to get into the village but it's easier."

Not just used in theater

The Biometric Task Force is bringing the technology to the "friendly side" as well, says Swan. Biometrics are used at different points throughout the Defense Department for physical and logical access.

The task force has an iris solution deployed at its West Virginia location for physical access, Swan says. There are also small implementations of fingerprint and hand geometry for physical access at bases throughout the Defense Department.

Using biometrics with the Common Access Card is in future plans, but there's no timeline for deployment even though there are some applications, Swan says.

"Biometrics and the Common Access Card will be used in concert," she adds. "For more secure applications you will see biometrics fairly soon, it's just a matter of what's practical and what you're trying to safe-guard."

And the Common Access Card will eventually be used with biometrics to access different computer records, Swan says. "The biometric could be used for access to health records," she concludes. "We'll see more and more of this. Our soldiers are mobile and this is something that could tie them to their record."

Facial recognition in Apple's iPhoto

Zack Martin
Editor, AVISIAN Publications

Apple Inc. is taking facial recognition biometrics to the masses by including the technology in the latest version of iPhoto, the computer company's photo management software. iPhoto is one of a suite of products in iLife, which includes movie, audio and Web design tools.

Apple sent me a copy of the software to and I gave it a spin to see how it worked.

It took about 15 minutes to install the software on my two-year-old MacBook. During this time it was also searching my photo library of more than 1,900 images to find faces, a process that took about 45 minutes.

After restarting, iPhoto offered to take me through a guided tour of the new features, including how to use the facial recognition. It's pretty easy to use, you pull up a picture and hit the "name" button on the bottom of the screen. A box will surround the faces in the picture and enable you to click and key in a name.

After doing this for a few people it will start to recognize the faces of the people pictured in your photo library. From then on when you click on the photo a dialogue box will appear asking if the picture is someone you previously tagged. You can click on a check mark if the facial recognition has correctly identified the person or an "x" if it isn't them.

Now you can search your library by individual. So if you're looking for pictures of a specific person you can search by his or her name instead of trying to remember an event or specific date when you took the photo.

The ability of the software to recognize individuals at first wasn't great, but wasn't awful. For the most part it did a fine job and after tagging someone it would recognize that person in future photos. But then it would make a suggestion that would be a head scratcher, mixing up people with different hair color, ethnicity and face shape. What did make sense is it mixed up people with similar body types and facial hair.

Even with the minor confusion the facial recognition feature in iPhoto is a plus. Instead of having to page through photo after photo looking for a specific individual you can click on a person's face and have every image of that person available. It's not a killer application but it's a nice feature and a great introduction to biometrics for a new segment of the population.

Photos: Courtesy of Apple

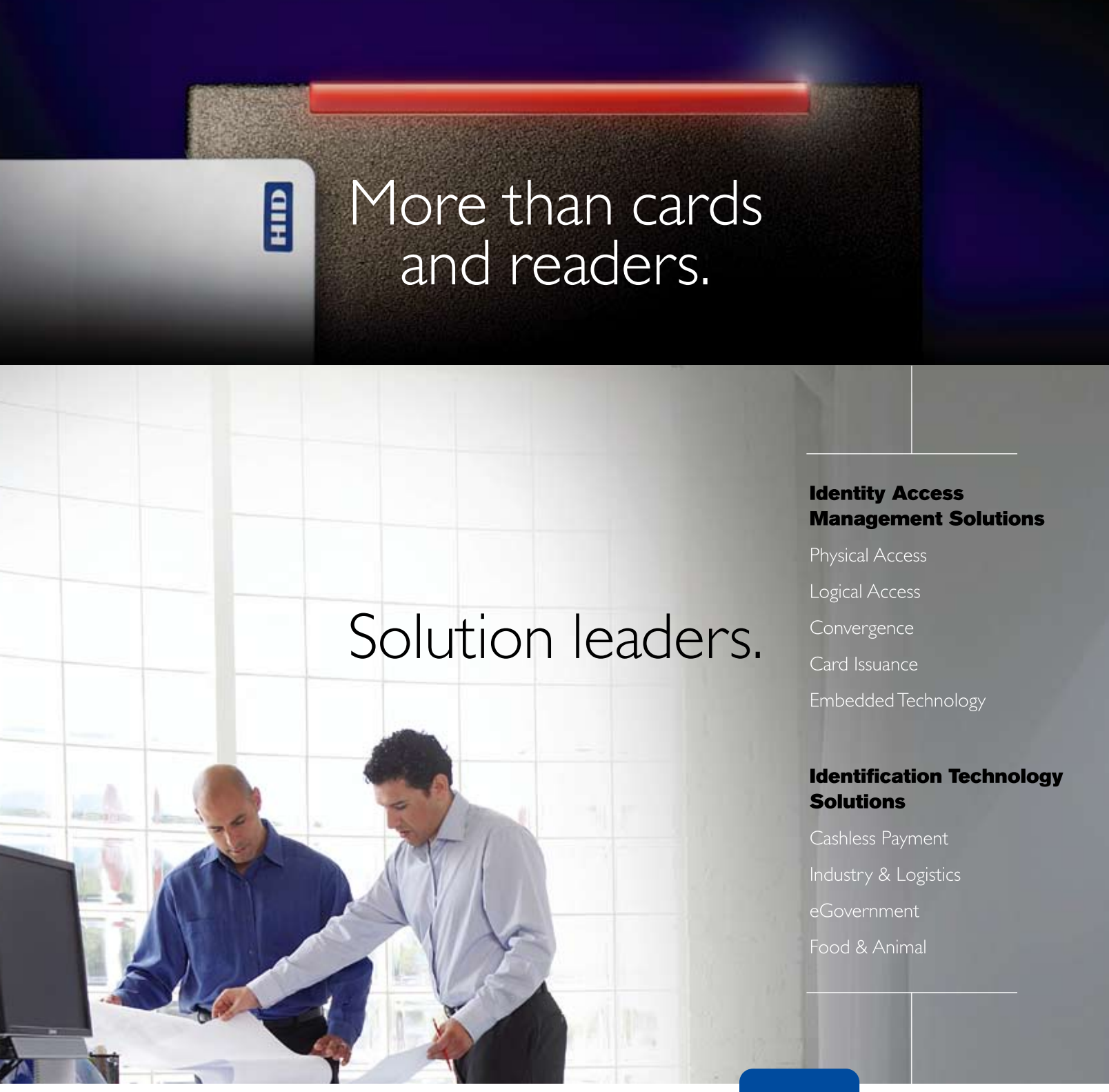
The *Original* Multi-Technology Readers

The Most Versatile, Secure Readers in the Industry

XceedID®
Xceeding The Ordinary

To learn more please visit: www.xceedid.com

Copyright © 2007, XceedID Corporation. All rights reserved. XceedID, XACTT, and ISO-X are registered trademarks of XceedID Corporation.



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

Food & Animal

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.

HID

ACCESS choices.

hidglobal.com