re:ID

Spring 2008

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

THE COMING STORM

SECURING IDENTITY in an online world

Outsourcing ID programs

Real ID becoming reality

London trials NFC

AVISIAN

INNOVATION REDEFINED

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

NEW FEATURES

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

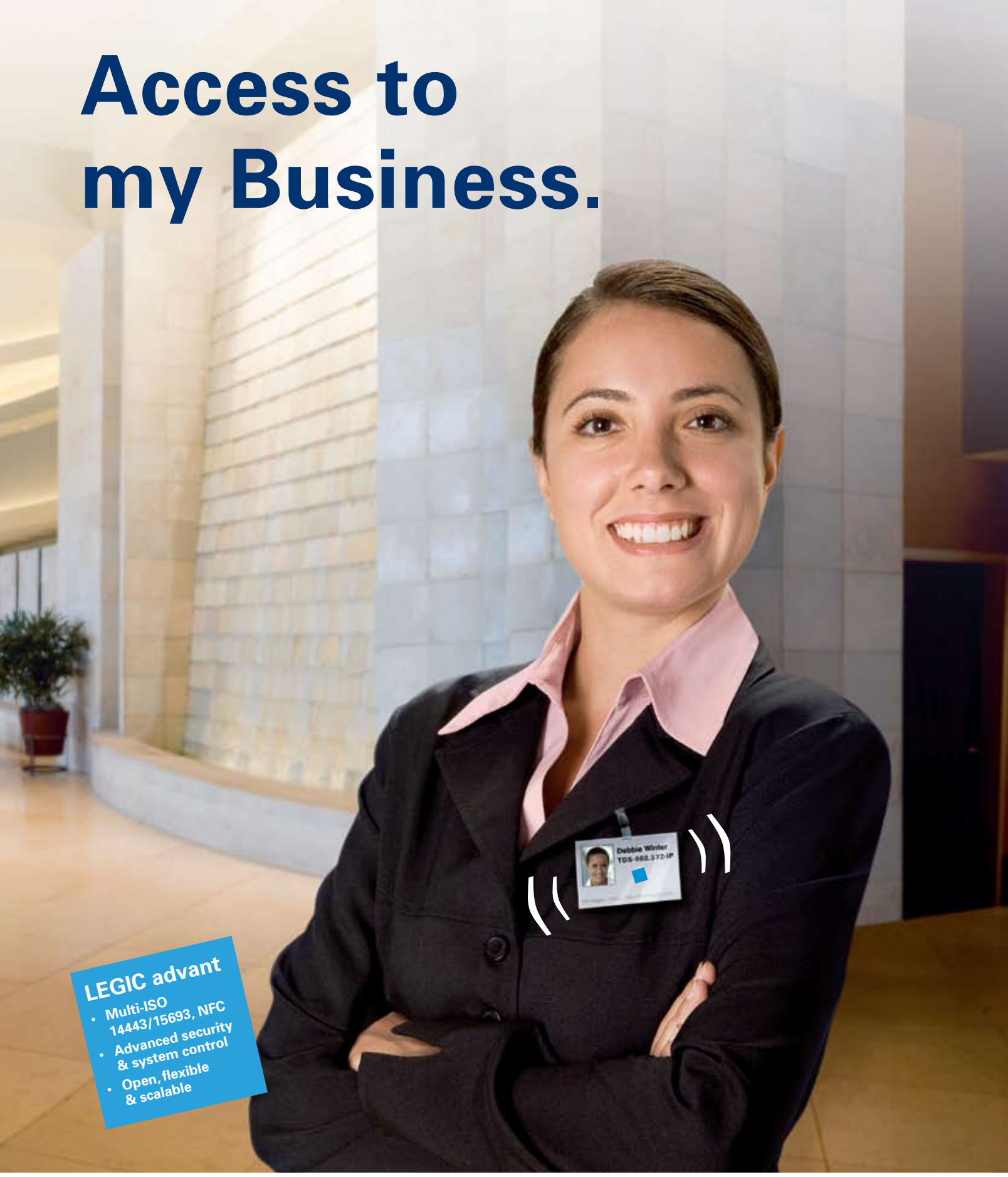
IMPROVE YOUR CARD PROGRAM

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

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

DatacardGroup
SECURE ID AND CARD PERSONALIZATION SOLUTIONS

Access to my Business.



LEGIC advant

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

Any application I can think of, any security level I demand.
All in one card – Proven and superior, the best value for my money.

Contactless smart card technology: www.legic.com

LEGIC®
innovation in ID technology

Spring 2008

Contents

INDEX OF ADVERTISERS

Online Identity

Meet the new elephant in the corner

Let me begin by saying I'm a huge geek.

For the past eight years I have participated in an online message board devoted to the Chicago White Sox. There have been highs, the 2005 World Series win, and lows, last year and I have a feeling many more years to come.

When I started on the site I didn't know anyone. But over the course of the years I have met probably 75% of the people who post on the board, either by going to games or other outings. And yes, I know this may be a bit strange but White Sox fans have an inferiority complex in Chicago and we band together for support.

When I read the message board I always trust the information and opinions from the people I have met a bit better than those I haven't. It's just the way it is. How do I know that the person ranting against trading Joe Crede isn't anything more than a 12-year-old sitting in his parents' basement?

The issue of online identities with social networking sites is the focus of the cover story for this issue and made me think of my own experiences online. Before writing this story my familiarity with these sites began and ended with LinkedIn, which I call MySpace for professionals. I am just a little too old to have a MySpace account and much too old for Facebook.

But I know people who are involved in these sites and was interested in seeing how the identification process works. And then I found out there isn't one. There's nothing to stop anyone from creating a fake profile on MySpace, Facebook, LinkedIn or most other social networking sites.

In the story Ant Allan, from Gartner, says that sometimes people want to be anonymous, and I agree with him. If an individual wants to go online and have an anonymous profile that's his or her choice. But because of that choice they should also be classified as anonymous.

Roger Sullivan, with the Liberty Alliance, paints an interesting picture of what may be to come in online identity proofing and classifying individuals based on the level of identity authentication.

The scarier situation is with minors. Currently, there is no technology that can easily authenticate the identity of someone under the age of 18. And even if there were, many would argue that the privacy implications outweigh the benefits.

It's going to be interesting watching what happens with online identities over the next few years. With predators using social networking sites to find underage victims it may only be a matter or time before federal legislation is proposed. Perhaps before then sites may realize the magnitude of the problem and start to look into solutions that would enable them to fix the problems without any laws.

Zack Martin
Editor, AVISIAN Publications

After a bit more than two and a half years away from the biometrics and identification business, all I can say is it's good to be back.

I spent more than three years covering the industries for *IDNewswire* and *Card Technology* magazine and it was hard to leave. When Chris Corum and I spoke about me joining AVISIAN, I was excited to come back and cover what I consider one of the most interesting technology beats out there. And it's been great reconnecting with some of my old contacts and finding out the status of different projects.

Over the next few months I look forward to digging into new stories and touching base with even more contacts. If anybody has any questions on what we're up to or would like to pitch me a story please feel free to email me at zack@AVISIAN.com.

My avatar is not who he claims to be

First impressions of identity in Second Life

Chris Corum
Executive Editor, AVISIAN Publications

A few weeks ago the AVISIAN staff took a field trip. We had lunch brought in to the office, gathered around one of the bigger monitors, and went to Second Life. We spent a couple hours "in-world" talking to residents, shopping or more accurately browsing, and teleporting from place to place in a hapless, newbie manner.

"Huh?"

Second Life is a 3D virtual world that boasts two million residents and has swallowed up the free time of some avid users to the extent that this second world is arguably their first.

It has its own in-world currency with an exchange rate that enables transfers in and out to first world currencies. Major corporations have set up shop, universities offer courses, and governments are establishing embassies.

And during lunch that afternoon, our staff – appearing as a jeans and t-shirt clad avatar named Frank – stumbled around anonymously exploring virtual buildings and hanging out with European strippers.

There was a point to this madness. We were beginning our exploration of identity on the new Internet. Web 2.0 – as it is called – is the next generation beyond the brochure-ware and one-sided conversations of the web as we have known it. Web 2.0 is a social space where users spend time with friends and create entirely new relationships. Whereas Web 1.0 was about information gathering, research and data presentation, Web 2.0 is about collaboration, creation and interaction.

We have a number of young people in our office. I define young as anyone who had an Instant Messenger account before their seventh grade dance. It has been an eye-opener for me to see the extent to which social networking sites drive their lives … or they drive social networking sites to enhance their lives.

They make plans for the weekend, they hang out, they find dates, roommates, events … you name it. For them, the web is truly a place, serving much the same function that the arcade, roller rink or mall served for prior generations.

But equally eye opening is the virtual absence of verifiable identity. You can be who you want to be in Second Life, and in most of the Web 2.0 world.

As sites like Facebook and MySpace continue to attract nearly everyone under the age of 30 and LinkedIn and others create virtual networking for professionals, what do users risk? Our profiles are often public and Googleable, and we hope that they remain clean and truthful. We assume that our online friends and contacts are actually the people they claim to be, but we have no proof. We trust that we are not being impersonated to others.

Hoping, assuming, trusting … what ever happened to identifying, verifying, and authenticating?

Our new editor, Zack Martin, delves into the state of identity online in this issue's cover story. I 'trust' you will enjoy it. And on a personal note, I am very pleased to welcome Zack to our team. I have long respected his work at *Card Technology* and *IDNewswire* and I look forward to continuing the tradition at *re:ID* and the other AVISIAN ID technology publications. ID

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

Will GrIDsure's pattern-based IDs secure the embattled PIN and passcode?

A new technology that strengthens PINs and passcodes with one-time grids and Personal Identification Patterns (PIP) is explored. Instead of using a numeric-based PIN, users select a pattern. That pattern can be used on a cell phone, ATM, POS, or computer screen for authentication. Executive Editor Chris Corum speaks with the technology's inventors and corporate leaders from GrIDsure on their new pattern-based unique IDs.

Highlights: "We simply asked a question, is it possible to create a new PIN number every time? And, ergo, a new passcode every time you do something. Previously the industry has been looking at tokens and all sorts of things. We sat down around the kitchen table, and I believe in about half-an-hour, we came up with an answer. The answer was to create a choice of squares, at its simplest level, on a grid. And for the user instead of choosing a passcode, they choose a set of squares, and he or she has the option to use a pattern to help remember those squares. And quite simply looking at a similar grid upon authentication, you have random numbers in every cell, and if you have previously chosen all five, six cells, you just read off the numbers that appear in those cells, and hey presto, you have a new code every time."

"The University College London ran a user trial for us, looking to see how well people could remember a pattern as opposed to remembering a static PIN number. They did a pilot study with 50 users … and overall their success rate was in the order of 93 or 94 percent, which compared to a PIN number is very good indeed."

"It gives them a security upgrade and takes passwords, PINs and combinations back to the secure position they were in a few years ago."

To listen, visit *SecureIDNews.com/podcasts* and select "GrIDsure"

Examining the proposed DHS budget with editors Chris Corum and Zack Martin

Executive Editor Chris Corum welcomes new Editor Zack Martin to the AVISIAN editorial team. They recap a recent U.S. Department of Homeland Security press conference on the new 10-print mandate for US VISIT and discuss the proposed DHS budget and what it means for federal ID programs such as US VISIT, WHTI, Real ID and TWIC.

Highlights: "US VISIT alone is asking for $39.3 million for the 2009 fiscal year. They are asking for $106.9 million for implementation of technology for the Western Hemisphere Travel Initiative, which is basically the PASS Card and the enhanced driver license. And they are trying to earmark $2.2 billion for grants, part of which will go to states to comply with the Real ID requirement," said Martin.

"The biometric and ID projects are getting a lot of play in homeland security's budget. On the second page, the third bullet point is about biometrics, about how the US VISIT program is switching from two prints to ten prints at airports throughout the country this year, as well as other initiatives being taken at land border crossings."

"Basically when foreign nationals are coming in through the airport they go through the check-in process and there is a fingerprint scanner on there … and at first they put down their four right fingers, then their four left fingers and then both of their thumbs at the same time. All the while the customs official is swiping the passport and asking them general questions about why they are coming to the states. They were processing people for the media when I was there … it took less than two minutes for a passenger to get through the check-in process."

To listen, visit *SecureIDNews.com/podcasts* and select "DHS Budget"

Talking Registered Traveler with Verified Identity Pass' Charles Simon

Executive Editor Chris Corum discusses the present and future of the TSA's Registered Traveler program with the SVP for Public Policy with Verified Identity Pass. The company is the leader in RT implementations with its CLEAR Card program in place at 14 airports. Topics include current and pending installations, market projections, business models, and potential ties with FIPS 201, TWIC and other card initiatives.

Highlights: "We're now approaching 100,000 members, but we are confident that the market for the program overall is between five and ten million."

"I think we are at that tipping point now. You are now seeing more of the Category X airports coming onboard now and the rate of growth is very, very strong. We are seeing good momentum in both member growth as well as airport growth. Our CLEAR program is now in 14 airports around the country. In the coming weeks, Reagan and Dulles are coming online; Oakland is coming online as well … we are rapidly approaching 18 airports."

"(With regard to whether FIPS 201 or TWIC cards could be used for RT), we have said from the beginning that all of these people should be immediately eligible to get the Registered Traveler cards and that they shouldn't have to go through a redundant security check by TSA since they have already been the subject of even more rigorous background checks to be eligible for their government credentials.

What we think should happen is that these people should get a substantial discount when applying for the Registered Traveler cards and that TSA itself, since they won't have to do a redundant background check, should wave their fee. That's something we have proposed, but it's not something TSA has adopted."

To listen, visit *SecureIDNews.com/podcasts* and select "RT"

Talking NFC with Innovision Research and Technology's Julia Charnock

Executive Editor Chris Corum discusses a number of easy do-it-yourself NFC applications, the current state of handsets and tags, and the NFC Innovation Award winners with Innovision's Julia Charnock.

Highlights: "The NFC Innovation Awards was a really exciting project. What we wanted to do was … see what people would do given the opportunity to experiment with NFC."

"The first winner is 'Health Buddy' and it came from the Lancaster University team. They wanted to use NFC to encourage people to get out of their houses and exercise … it is basically like a personal trainer. They would put tags around the course, it might be a run through some woods or a park, and then as the person goes around the route, they touch a tag at the different locations, and they can get a report at the end telling them how long they took, how many calories they burned, and compare the information to the last time they did it."

"The North East Wales Institute of Higher Education had a vehicle identification application. In the UK we pay road tax and we have to display a tax sticker on our windshield. Basically what they did was they put a tag on the inside of the car window screen so that it could either replace or be used a compliment to the current tax sticker. When the tag is touched, it would provide a unique reference, which the phone could use to receive information from the central database."

"The third-place application was designed so that the user can use their phone to get their prescriptions from the pharmacy. Or when they go to the doctor, the doctor can use their phone to touch and he can get their medical history very easily. They can also use the alarm on their phone to remind them when to take their medication."

To listen, visit *SecureIDNews.com/podcasts* and select "Talking NFC"

Government identity outlook: Finishing what's been started

As President Bush's administration enters the home-stretch there will be a rush to finish many of the identification programs that his administration started.

"An end-of-administration push will help drive 2008 government identity solutions spending to record levels – but we expect few new identity initiatives to emerge this year," says Jeremy Grant, senior vice president and identity solutions analyst at the Stanford Group Company. "Looking ahead to 2009, we forecast flat government spending outside of several key programs, as a new administration takes a year to review and reshape existing initiatives."

Real ID (page 18), the Western Hemisphere Travel Initiative (page 20), US VISIT (page 34) and the FBI next-generation biometric system (page 34) are being covered elsewhere in this issue.

Grant's spring outlook report also highlights efforts by the U.S. Department of Defense (DOD), HSPD-12, the Transportation Worker Identification Credential, registered traveler and a look at what's to come in 2009.

The DOD is intent on using biometrics and other identification technologies to both protect its networks and facilities and serve as a warfighting tool, Grant says. The agency is investing in handheld biometric readers that are being used overseas. The SecuriMetrics HIIDE handheld from L-1 Identity Solutions is seeing significant sales as are some products from Cross Match Technologies.

Efforts to credential all federal employees have picked up, but overall they are still moving slowly, Grant says. Less than 50,000 cards have been issued, but he expects $195 million to be spent this year. As more IDs are issued the need for physical and logical access systems will begin to emerge creating a secondary market for companies.

The TWIC is moving forward with cards being issued at a number of ports and the program will continue to roll out. The TSA, however, has not put as much effort into the Registered Traveler program. Less than 75,000 individuals have enrolled in the different RT programs and unless the program receives a boost from a new administration in the White House in 2009 there probably won't be much movement in this program, Grant says. There is support for an international RT program in Congress but it's unlikely to see much movement this year, he adds.

Grant predicts flat spending from a new administration in 2009. Regardless of who wins the election most programs will remain the same for the year. "By and large, these programs enjoy bipartisan support so there is little threat, in our view, that a new administration would try to gut them," he says.

There are other initiatives the industry will be hearing about in the coming year, Grant says. The "server in the sky" is a program that will have the U.S. exchange biometrics with its allies; US VISIT will consider going multi-modal or veer away from the AFIS model and rely on biometrics stored on the smart card chip on the passport; iris and facial recognition technology will become more accurate from a distance; cheaper and more rugged biometrics scanners will be available; and handheld and mobile biometric units start to become more common by soldiers, law enforcement and border officials.

EU will collect biometrics from non-European travelers

The European Union is considering a proposal that will require all non-European travelers to submit biometrics when entering the region.

From media reports the program sounds similar to the U.S. Department of Homeland Security's US VISIT program. If a traveler needs to enter the EU their fingerprints could be collected when they apply for a visa. For other travelers, such as U.S. citizens, the biometrics would be collected when they first enter the EU. European citizens would be considered "registered travelers," according to the *International Herald Tribune*. Instead of having to go through checkpoints and be interviewed by border officials, they would have their travel documents scanned by machines at automated checkpoints.

The commission's proposals cover the Schengen zone, Europe's internal free-travel area that includes 24 countries. It is unclear whether Britain and Ireland, which along with Cyprus are not members of Schengen, would opt into the program.

The border security proposal will go to the European Commission this week. If approved all EU states would need to approve the measure.

Biometric smart card for Social Security proposed

U.S. Rep. Mark Kirk (R-Ill.) is proposing a new Social Security card that would be based on the same technology the U.S. Department of Defense uses for the Common Access Card.

The new Social Security card would have a photo, magnetic stripe, bar code and microprocessor chip that would contain the user's biometric. Exactly how individuals would ob-

tain the card and which biometric would be stored on it were not specified.

Kirk is proposing the legislation and high-tech ID to help prevent identity theft. The card would also enable employers to validate the Social Security number.

The legislation would require anyone older than 15 to obtain a new card. It's estimated that the new card would cost almost $8 each, compared to the 50 cents they now cost.

UK ID card delayed

The United Kingdom's national biometric identification card program has been delayed, according to press reports.

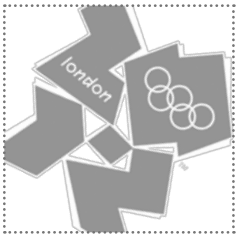
The biometric cards, which will carry fingerprint, iris and face-recognition technology, are expected to cost 5 billion pounds over the next decade. The procurement process began last August.

The Conservative party leaked Home Office documents stating that the ID card project would be delayed until after the next election, most likely 2012. Foreign nationals, however, will start receiving the card this year.

UK-based BAE Systems and Bermuda-based Accenture also withdrew from consideration to be the prime suppliers for the proposed identity card scheme.

London 2012 Olympics to be cash free

The 2008 Olympics haven't even happened yet and Lloyds TSB, a London-based bank, has already started a multimillion-pound contactless card payment trial to evaluate how feasible it would be to have a totally cash-free environment for the 2012 Olympics. The trial was put on the fast track hoping to succeed.



The plan as of now seems to be that in 2012, spectators and participants at the London Olympics will be issued one card to handle everything from getting into the stadium to purchasing food, in and out of the stadium.

"The Olympic committee wants to make the events as cashless as possible, and contactless technology will play a big part," says Kevin Coles, head of business enterprise at Lloyds TSB Cardnet. "We are investing a substantial amount in the new technology."

But Lloyds TSB is not the only bank investing in the technology for general use around London. The 2007 contactless payment card roll-out will have already issued nearly five million cards by the end of 2008, and more than 100,000 merchants are expected to accept contactless payments by then.

The most important factor for the Olympics scheme will be speed, according to Butler Group analyst Sarah Burnett. Unless the transactions can occur faster than cash, there is little hope that people will actually use the contactless cards.

The technology should also benefit retailers by reducing the need for small change and make it easier to track sales figures and popularity of items at the end of each business day.

London Fashion Week goes high tech with O2

O2 launched the first ever fashion industry pilot of NFC technology on mobile phones at this year's London Fashion Week. The first designer and fashion buyer to work with O2 to bring NFC technology to the fashion industry was up-and-coming designer Emilio de la Morena and fashion buyer Two See, the stylish Covent Garden boutique.

The pilot was launched at Emilio de la Morena's catwalk show at the Science Museum. It enables designers to instantly know which designs are likely to be the hottest by getting immediate feedback from fashion buyers attending their show.

As they left the show, fashion buyers equipped with the Nokia 6131 NFC handset registered interest in specific designs in Emilio's collection, simply by touching their phone on specially-designed smart posters featuring the designs. Embedded tags within the smart posters automatically sent a text message back to Emilio indicating the designs in which they were interested.

With the main selling event – and last opportunity to sell the season's collections – in Paris only two weeks later, the designers received invaluable feedback from the London show, allowing them to tailor their collections according to the buyers' feedback.

Roper Industries acquires CBORD

Leading campus card provider The CBORD Group, has been purchased for $367 million by Roper Industries, a company that provides engineered products and solutions for niche markets including water, energy, radio frequency and research/medical applications. "As part of Roper we will have the financial and strategic resources necessary to pursue a variety of new initiatives," says CBORD president Tim Tighe. CBORD's management team will remain intact, according to Roper.

CBORD provides transaction solutions to 750 colleges and universities, representing 4.5 million students; 1,700 major health care licensees; and large corporate campuses, leading supermarkets, theme parks and dining chains. In total, CBORD systems are used by more than 6,000 organizations in the U.S., Canada, Europe, South Africa, New Zealand and Australia. The business will continue as CBORD and will operate within Roper's RF Technology segment, and market its products and services under its current brand names.

CBORD provides complete solutions to the higher education market. The company provides a wide variety of student and employee transactions under a single system, "one card" approach. Its card-based services also include security, onsite and off-campus commerce and student discounts. In campus food service, the company's services include food management software and online ordering. CBORD's health care business provides patient and employee food service.

NFC devices can protect Wi-Fi networks

The Wi-Fi Alliance released a list of more than 200 products that have achieved the Wi-Fi CERTIFIED seal of approval for Wi-Fi Protected Setup. This program, launched in January 2007, helps consumer and small-business users more easily set up Wi-Fi networks with strong security protections.

The organization has also started to test NFC support as an additional Wi-Fi Protected Setup network configuration method. In the NFC method, a user touches a card or token to designated areas on an access point and a client device to connect them. NFC joins two previously tested mechanisms – push-button and PIN entry – to simplify the process of joining devices to a security-enabled Wi-Fi network.

Like the push-button method, the NFC technique may be used to connect devices that don't have a keyboard-oriented user interface, such as cameras, gaming devices and other consumer electronics. Manufacturers will now have even more flexibility in how to deploy Wi-Fi Protected Setup.

Heathrow collecting fingerprints from passengers

Passengers using Terminal 5 at London's Heathrow Airport will have to submit fingerprints and a digital photo before being allowed into the terminal, according to a BAA spokesperson. BAA runs seven airports in the United Kingdom.

The biometric system is used for border control purposes to ensure international travelers who check in for a flight actually board the plane. There is concern that international and domestic travelers will switch documents and tickets in the new terminal. Terminal 5, which opens in March, will mix international and domestic passengers, so all travelers will have to submit biometrics.

Passengers are asked to provide the data before they proceed through security. At the gate, this information is reconciled to confirm the passengers' identity and to ensure that border control regulations are met. The data is used only by airport staff and is destroyed after 24 hours.

The system is already in use at other airports in the UK, including Gatwick, and was introduced in Heathrow's Terminal 1 on February 1.

BART to use 'smart' bike lockers

The Bay Area Rapid Transit (BART) will begin the use of "e-lockers" that, instead of being opened with keys by a passenger who wants to store his or her bicycle before boarding a train, are opened with a card read by a computerized reader embedded in the locker.

Officials of Oakland-based BART say the card-entry lockers can be used by up to five cyclists a week. Passengers can purchase a smart card online for $20. They are charged 3 cents per hour to store their bike, which is deducted from the smart card when passengers return to retrieve them. BART plans to install 198 of its own e-lockers at eight additional stations by July and 220 e-lockers at 12 more stations next year. The district hopes to have 895 such lockers operational by 2012.

APRIL

ISC West 2008
April 2–4, 2008
SANDS Expo Center; Las Vegas, Nev.

NACCU 15th Annual Conference
April 6–9, 2008
Riviera Hotel & Casino; Las Vegas, Nev.

RSA Conference 2008
April 7–11, 2008
Moscone Center; San Francisco, Calif.

NFC World Europe
April 15–17, 2008
Millennium Mayfair; London, England

Security Document World 2008 and Identity Loop 2008
April 22–23, 2008
Covent Garden; London, England

MAY

CTST 2008 and the Smart Card Alliance Annual Conference
May 13–15, 2008
Orange County Conv. Ctr.; Orlando, Fla.

European Supply Chain and Logistics Summit 2008
May 13–15, 2008
Swissôtel; Düsseldorf, Germany

Cardex 2008
May 25–27, 2008
Cairo International Conv. Ctr.; Egypt

JUNE

ISC Brasil 2008
June 18–20, 2008
Transamerica Expo Center; Sao Paulo, Brasil

JULY

NACUBO Annual Conference
July 12–15, 2008
Hilton Chicago; Chicago, Ill.

SEPTEMBER

RFID World 2008
September 8–10, 2008
MGM Grand; Las Vegas, Nev.

Labelexpo Americas 2008
September 8–11, 2008
Donald E. Stephens Conv. Ctr.; Chicago, Ill.

ASIS International 2008
September 15–18, 2008
Georgia World Congress Ctr.; Atlanta, Ga.

e-Smart Conference and Demos 2008
September 16–19, 2008
Science Park; Sophia Antipolis, France

OCTOBER

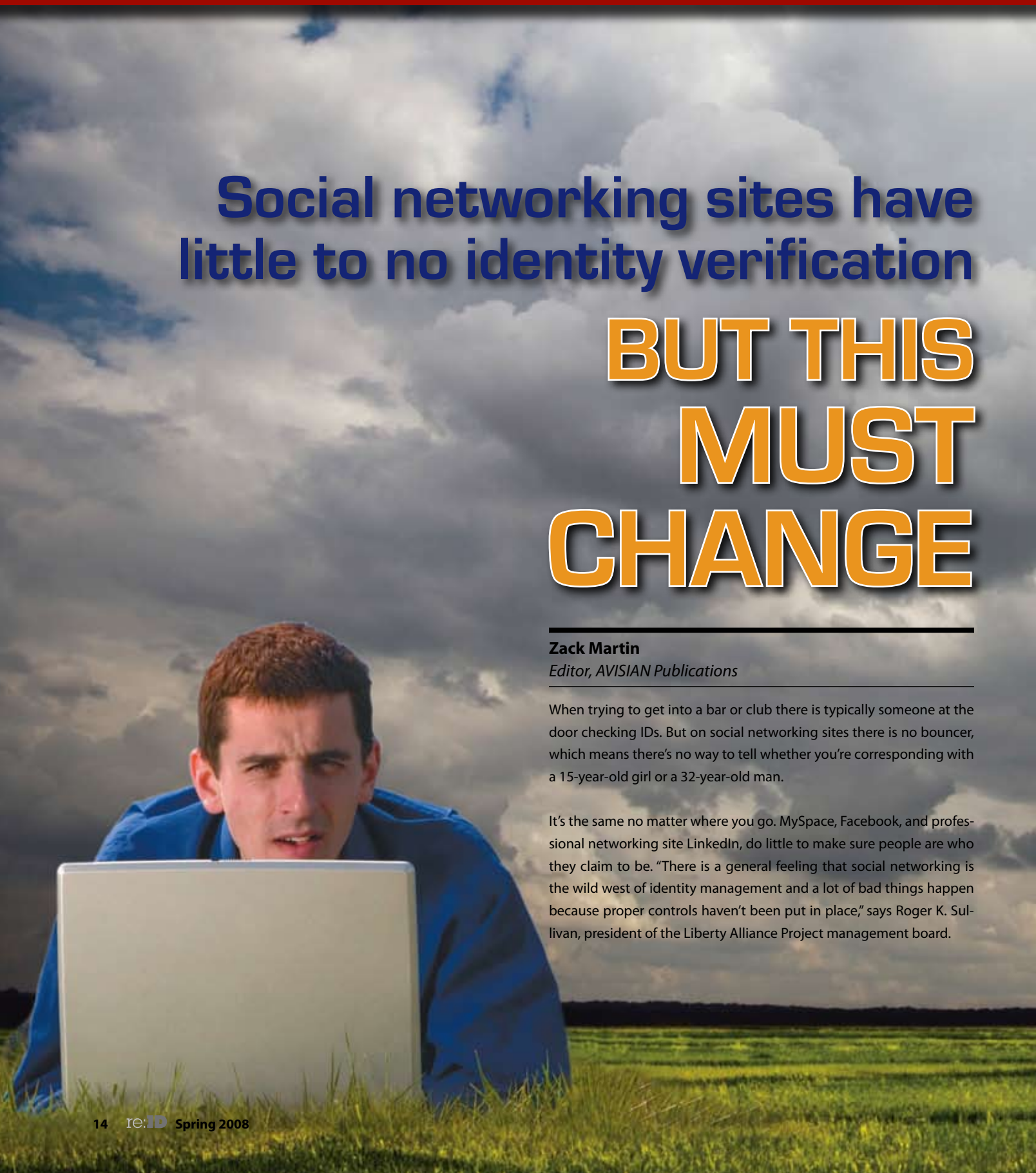
7th Annual Smart Cards in Government Conference 2008
October 22–24, 2008
Ronald Reagan Building; Washington, D.C.

EDUCAUSE 2008
October 28–31, 2008
Orange County Conv. Ctr.; Orlando, Fla.

NOVEMBER

NACAS 40th Annual Conference
November 2–5, 2008
Hyatt Regency Chicago; Chicago, Ill.

CARTES & IDentification 2008
November 4–6, 2008
Paris-Nord Villepinte Expo Ctr.; Paris, France



Social networking sites have little to no identity verification

BUT THIS MUST CHANGE

Zack Martin
Editor, AVISIAN Publications

When trying to get into a bar or club there is typically someone at the door checking IDs. But on social networking sites there is no bouncer, which means there's no way to tell whether you're corresponding with a 15-year-old girl or a 32-year-old man.

It's the same no matter where you go. MySpace, Facebook, and professional networking site LinkedIn, do little to make sure people are who they claim to be. "There is a general feeling that social networking is the wild west of identity management and a lot of bad things happen because proper controls haven't been put in place," says Roger K. Sullivan, president of the Liberty Alliance Project management board.

The stories range from the tame to the tragic.

A student not happy with an administrator at school creates a profile on a social networking site. Even though the student is a woman she creates a profile that is a man and then flirts with the administrator in order to cause her embarrassment later.

At a Catholic school in the Chicago suburbs, an administrator monitors the popular social sites on a regular basis just to make sure nothing out of the ordinary is happening. She has run into instances where students create accounts in other peoples' names – people who actually exist – and then make false statements. For example, one student set up an account as a real person from another school and made statements about the student's sexual proclivities while giving out her real phone number.

In 2006, a fake profile led to the suicide of a 13-year-old Missouri girl. A classmate's mother originally created the profile to find out if Megan Meier was saying anything bad about her daughter. But then it was used to gain Meier's confidence and then to tear her down. Angry messages went back and forth, and it ended with Meier hanging herself.

There's also the need to prevent pedophiles from contacting children online. MySpace has agreed with different states' attorney generals to adopt better technologies that will help identify underage users so they can be protected from predators, but the social networking site hasn't figured out how it's going to do it.

The vast majority of sites don't do anything to try to confirm the identities of members. The sites also don't want to absorb the cost of trying to prove the identity of their members. Also, identifying minors is almost impossible because there isn't enough information out there to authenticate their identity.

But this may all change. As sites become more scrutinized they will have to take steps to make sure people are who they say. "There will be a trend to use a third party that leverages database information that will be able to vouch for you and provide a more certain level of identification," says Eric Skinner, chief technology officer at Entrust, an Addison, Texas-based digital identification vendor.

There are a handful of vendors that are offering online identity vetting. Most are working with financial institutions, but they see business opportunities with the social networking sites.

eHarmony and others offer optional identity services

Pasadena, Calif.-based *eHarmony.com* is offering identity verification technology to its members, says a spokesperson for the company. The dating web site is using technology from Dallas-based RelyID.

"Many users are new to the whole world of online dating and sometimes need a little more encouragement to get off the fence to reach out to their matches," says the eHarmony spokesperson. "We saw RelyID as another way to help people take that first step."

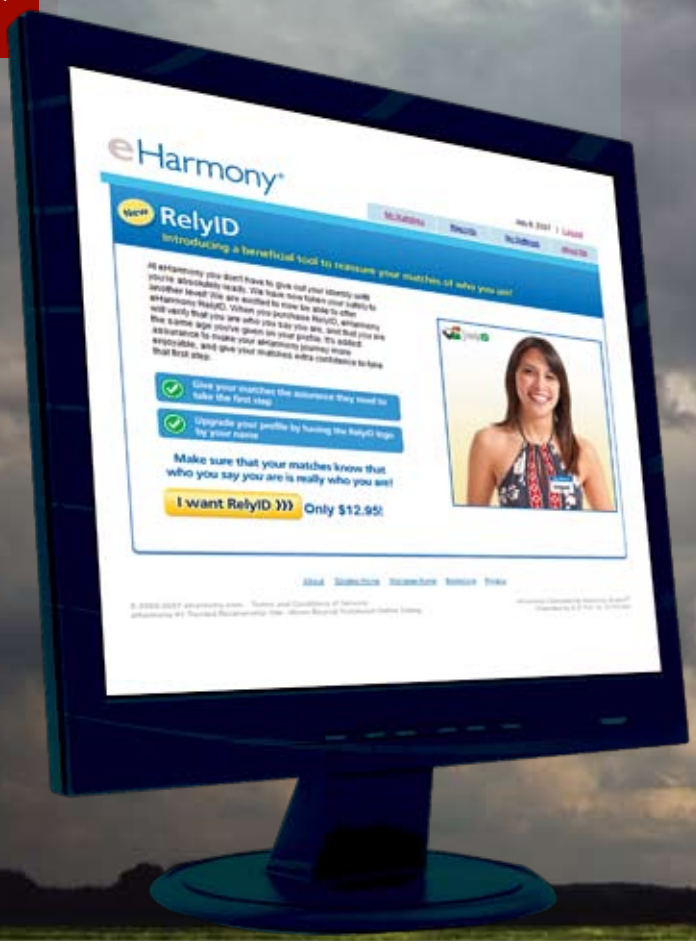
The service is voluntary to eHarmony members and they must pay an additional $5.95 fee to participate. For those members who want to be authenticated, they provide their full legal name, address and date of birth. RelyID's technology then checks public and financial records databases and comes back with a multiple choice quiz based on an individual's personal data, such as names of relatives and latest financial transaction, says Pat Mangacotti, vice president of business development at the company.

If an individual answers the question correctly, the ID will be verified and they receive an authentication badge on their profile. If they don't answer the questions correctly they can come back and take the quiz again within 72 hours, Mangacotti says. If they can't be verified after taking the quiz a second time they can then present government-issued identification to RelyID's customer support team.

Reaction to the service has been positive, says the eHarmony spokesperson. But the company would not say how many members have chosen to use the RelyID service. "In a few cases, where certain customers may have been new to online dating, they have told us that seeing a user's RelyID badge got them off the fence and let them confidently reach out to a particular eHarmony member," the spokesperson says.

Mobile social networking service Funky Sexy Cool is offering identity verification to all its members at no additional cost, says Tim O'Connor, CEO of the New York-based company. But members have to choose to go through the process. Funky Sexy Cool enables members to find other like-minded individuals in the same geographic area to hang out with. For example, a member can send out a message to his friends saying he'll be at a certain club or bar.

"In a few cases, where certain customers may have been new to online dating, they have told us that seeing a user's RelyID badge got them off the fence and let them confidently reach out to a particular eHarmony member."



When first registering for Funky Sexy Cool potential members can click a box that will enable them to be verified, O'Connor says. If they choose to go through the process they will be asked for information, such as full name, last four digits of the Social Security number and date of birth. Funky Sexy Cool is using ID verification technology from IDology Inc., Atlanta.

IDology searches public databases to confirm an identity, says a company spokesperson. The company's technology searches driver license records, property records and similar databases.

To sign up for Funky Sexy Cool a user must already claim to be 18 years old, O'Connor says. The site doesn't require age or ID verification because they don't want too many steps to register for the site. "If you make too many things mandatory people between the ages of 18 and 34 won't join," he says.

O'Connor says there is a need for some sort of age or identity verification, but the companies that run these sites walk a fine line. "I want to be part of a group that enforces age verification," he says. "But if you have registration that is cumbersome and difficult you won't get the members. We're trying to gauge member reaction and see what happens."

Cost is another problem, O'Connor says. IDology charges about 37 cents per ID verification, which doesn't seem like much at first. But when dealing with hundreds of thousands to a million of members the cost rises quickly. "We need to increase ad revenue so we can defer some of that cost," he says.

Minor difficulty

But the problem of identifying minors remains. The technologies that some sites use to prove an identity use public records and databases and minors don't have any information in those

Networking sites could learn a lesson from financial institutions

Legitimate users of social networking sites sadly have more to worry about than whether their friends are who they claim to be. User profiles often get hacked, sending messages to their friends that lead to fake sites where their information could be phished or spyware and viruses could be downloaded.

There are a number of technologies that can be used to prevent a user from being hacked, and analysts suggest that social networking sites look at what banks and credit card companies have been doing, says Eric Skinner, chief technology officer at Entrust, an Addison, Texas-based digital ID vendor. "The people pioneering stronger authentication are the banks," he says. "They are finding stronger ways to authenticate without causing a great amount of inconvenience."

systems. "There isn't a technology that exists today that can confirm a minor's identity online," says a MySpace spokesperson. IDology and RelyID say they wouldn't be able to identify minors with their technology.

It would also be difficult to just confirm age without needing additional information, says Ant Allan, research vice president at Gartner Inc., Stamford, Conn. This would raise privacy concerns, especially when dealing with minors. "The younger you are the less information appears in the databases," he says. "And when you're on the borderline, their identity proofing systems won't come back with anything. Also, someone could be 18 to 21 years old, and they may not have amassed enough information to return a positive result."

Liberty Alliance's Sullivan, who is also vice president of Oracle Identity Management, says it's only a matter of time before social networking sites offer tiers of identification assurance, which could be used to confirm a minor's identity. For example, if a 14 year old wanted to sign up on MySpace without a parents' permission they would be placed on the lowest ID tier. "They would be put into a question mark bucket," Sullivan says.

But if one parent went online and confirmed his child's identity they would be raised up a tier. If both parents did it they would go up two tiers. The parents would be authenticated through public records and online databases.

Eventually there would be a fourth tier as well. A minor would physically go to a trusted source with documents that prove their age and identity. These identity assurance sources don't exist, but it's something the Liberty Alliance is working toward, Sullivan says.

Already authenticated?

But what about those individuals who want to remain anonymous online? They're not pedophiles or out to harm anyone, but they just don't want their true identity revealed.

"There are some social networking sites where people want to be associated with the real world identity and others where they don't," Allan says. "If the folks running MySpace and Facebook insist on some level of identity proofing, it might discourage people from joining.

"The needs here vary and I don't think it's clear cut that social networking sites have to have the same level of authentication and identity proofing as financial services sites."

For social sites there doesn't have to be a strong link to the real-world identity, Allan says. "If you're trying to prevent something obscene from being posted there is recourse through the usual channels like finding their IP address," he says. "For the majority of reasonably well-behaved people it's not so important."

For sites where reputation might hold a bit more importance, such as LinkedIn, there is a type of hierarchical identity proofing that exists on the sites, Allan says. "The network is part of the identity verification," he says. "Once you get a certain number if people it establishes you and is a way of acknowledging your identity. Depending on the rigor people are looking for that network might be enough to confirm a person's identity, but other times you might need something else that can be verified."

LinkedIn, MySpace and Facebook users access the sites with user names and passwords. There are no additional security steps. If a user forgets his email address it's emailed back to him, there are no security questions, such as mother's maiden name or name of high school, to confirm identity.

There are a number of different technologies that financial services institutions are using, some involve the consumer being actively involved while others do not.

SiteKey, from Bedford, Mass.-based RSA Security Inc., is one technology that financial institutions have deployed, including Bank of America and Barclays PLC. When first logging in using the technology users pick an image, text or a phrase. They also answer some security questions. A secure cookie is downloaded to the user's computer registering it and the IP address.

From there on out they see that text and image when they login to the site. If they are logging in from a different computer they will have to answer a security question for additional authentication before seeing the image and phrase.

An RSA Security spokesperson says the company has not talked to social networking sites about using its technology.

There are behind the scenes precautions sites could take as well, Skinner says. If a site notices the same individual logging in from different cities or countries in the same day they could check for any suspicious activity. The same can be done if someone is trying to log in from multiple computers in a single day.

Real ID becoming reality with first deadline Dec. 31, '09

Andy Williams
Contributing Editor, AVISIAN Publications

Despite Real ID opposition, as symbolized by web sites like *realnightmare.org*, an ACLU site, *unrealid.com* and blogs like *stoprealidnow*, the 2005 law isn't going away. The federal government even tried to soften the monetary blow when it issued its final compliance regulations earlier this year. But in the end, it's as U.S. Department of Homeland Security Secretary Michael Chertoff said when the regulations were first rolled out: "The rule is the rule. It was passed by Congress, it was enacted into the law of the land, and I'm obliged to enforce it."

The final rule was released in January and sets uniform standards that are designed to enhance the integrity and reliability of driver licenses and state-issued identification cards, strengthen issuance capabilities and increase security at license and identification card production facilities. The final rule also dramatically reduces state implementation costs by roughly 73%.

Real ID is designed to address document fraud by setting specific requirements that states must adopt to comply. As DHS Sec. Chertoff explained, "people seeking driver licenses must provide to their state Department of Motor Vehicles documents that prove who they are and prove that they are here in this country legally. Second, DMV offices must verify that the documents they are being presented with are legitimate. They have to take steps to protect their own operations and their own databases from identity theft and other corrupt activities. Third, licenses issued by states now must meet tamper-proof standards that will make it much harder to counterfeit or alter a secure driver license. And finally, states have to work together to assure that individuals are not able to obtain driver licenses from multiple states."

The first deadline for compliance is Dec. 31, 2009. By then, states must upgrade the security of their license systems to include a check for the lawful status of all applicants to ensure that illegal aliens cannot obtain the new licenses. Some states are expected to be compliant before that time, says DHS. Compliance will be needed for access into a federal facility, boarding commercial aircraft, and entering nuclear power plants. DHS is making approximately $360 million available to assist states with Real ID implementation – $80 million in dedicated Real ID grants and another $280 million in general funding as part of the Homeland Security Grant Program.

The 73% cost reduction – from an original estimate of $14.6 billion to approximately $3.9 billion – was achieved mainly by giving states greater flexibility in issuing licenses to older Americans. Enrollment will be completed for all individuals less than 50 years of age by Dec. 1, 2014. For all others, enrollment may be extended three additional years to Dec. 1, 2017. At that time, all state-issued driver licenses and identification cards intended for official federal purposes must be Real ID compliant.

Real ID came out of the 9-11 Commission recommendations that the U.S. improve its system for issuing secure identification documents. In the commission's words, "at many entry points to vulnerable facilities, including gates for boarding aircraft, sources of identification are the last opportunity to ensure that people are who they say they are and to check whether they are terrorists." The Commission specifically urged the federal government to "set standards for the issuance of … sources of identification, such as driver licenses" because most of the 9-11 terrorists had legitimate driver licenses.

One of the biggest problems states have with Real ID is its cost even now that it has been slashed 70%. But that's not as much a DHS problem as it is a congressional one. State groups, including the National Council of State Legislatures, the American Association of Motor Vehicle Administrators and the National Governors Association are still evaluating the final rules but, in a joint release, said they are at least happy that DHS has backed off on some of its more stringent requirements as well as relaxed some of the compliance dates.

"Governors, state legislators and motor vehicle administrators are pleased that many of the regulations seem to reflect comments and recommendations submitted by the three groups to DHS, including extending compliance deadlines and giving states flexibility to manage their systems and make them more secure," their statement says.

"DHS also recognized that the implementation cost was an issue by making changes to reduce costs to states. Their estimate remains significant at $3.9 billion. To date, however, Congress has appropriated less than three percent of the projected costs to assist states."

The NCSL has issued a series of "briefings" reviewing each of the requirements, including the deadlines, ID verification, physical security requirements of DMV facilities, requirements for a Real ID-compliant card and more.

Janice Kephart, former counsel to the 9-11 Commission who now runs her own company, 9-11 Security Solutions, says that one cost-saving move is the paring down of "the number of ID documents that driver license offices will need to authenticate. Once scanned, the docs can be used for online renewal."

"Most of the cost we were seeing had to do with the renewal cycles being shortened. That's now out of the picture. We're also not dealing with the need for extra personnel, so states' concerns about customer service have been eliminated," she says. Once Real ID is fully implemented, "there will be a greater connectivity among states." That means states will be able to more easily check with each other to verify that the applicant doesn't already have a license in another state. "I foresee there will be a lot more confidence in the system," adds Kephart.

"What states have to do now is decide whether to get on the bus or not. The bus is going to leave the terminal so they have to decide by May 11, the act's original deadline, whether to ask for an extension."

One problem the NCSL had was the delay in final regs. At the time of issuance – Jan. 11 – states had just 120 days left to comply unless they asked for an extension to Dec. 31, 2009. "All states have to do is say 'yes, we want an extension,'" says Kephart. "Most states which want an extension have an intent to comply, so by then we'll have a pretty good idea of who's in and who's out."

"If they states don't ask for an extension then they have to comply with Real ID by May 11," adds Jeri Owen, vice president of marketing for Beaverton, Ore.-based Digimarc, which supplies driver licenses to 32 states.

Requesting the extension may simply be delaying the inevitable. Kephart says that within three days after the final rule was released, 18 states had already requested an extension.

She's also seen indications that some of the original states that had flatly said they wouldn't comply will eventually come around.. Maine, Montana, New Hampshire, Oklahoma and South Carolina legislatures even adopted laws saying they wouldn't.

"It will be a huge burden on a state's citizens if they don't comply," says Kephart. The license its citizens possess would no longer serve as identification for getting on an airplane. "That means people from that state would have to come up with a different form of identification," Chertoff said. Or worse, they may find themselves being detained and questioned. "So it's going to be inconvenient. There's no question the law creates a very powerful incentive for states getting on board with this process. It doesn't make states do it, but convenience and common sense strongly counsel in favor of beginning to move down the path towards this secure form of identification."

"When push comes to shove I don't think there will be any state that won't comply," says Kephart.

She says the new rules "have given states a tremendous amount of flexibility. DHS also provided a 27-page best practices section on privacy to go along with the rules so states have a best practices to follow," she adds.

"One of the reasons I trust the rules so much is because the folks who authored them are former DMV heads, so they know what DMVs can and can't do."

To help, first with data comparing and later with state compliance, some $50 million has been requested by the feds to support implementation of the Real ID Act to develop an information sharing and verification "hub" capability. This "hub" will allow states to quickly and electronically verify document information with the source agency (both federal and state). In addition, the hub will facilitate state-to-

state exchanges of driver license information. Grant funding to assist states with implementing requirements of the act has also been requested under the State and Local Grant Program within the Federal Emergency Management Agency.

One Real ID option is the Enhanced Driver License that includes a radio-frequency identification chip (See passport card story, below). Washington State is already deploying the cards and other border states are considering it. In order to obtain one of the enhanced driver licenses an applicant must prove citizenship, one of the primary Real ID motivations. States issuing the enhanced driver licenses will be compliant with Real ID.

Digirmarc, the company supplying the enhanced licenses to Washington State, has been preparing for Real ID since 2005, says Owen. The company has in place a range of Real ID compliance scenarios, but there is one ingredient still missing from the regulations, "a visual security marker," she adds. That would allow law enforcement or other agencies to immediately recognize the validity of a license. The marker could be something as simple as a hologram to one more sophisticated. In any case, it has to be one that can't be counterfeited.

To those privacy zealots who continue to rail against Real ID – the *realnightmare*, unrealid and stoprealidnow folks – "They clearly did not read the regulations," says Kephart. "If they did read them, they ignored what they said because they're saying things that are completely opposite of what the regs require. I've been dealing with them for a year and I have no tolerance for people who misuse the facts to push their own agenda. That's blatantly wrong."

To those same objectors, Chertoff argues: "Most of these objections are really grounded in misinformation … We are not going to have a national database. Real ID does not require that states start to collect additional information from applicants that they have not already created. We are not going to wind up making this information available willy-nilly. In fact, the steps we are taking under Real ID will enhance and protect privacy rather than degrade and impair privacy."

After the dust has settled, although that may be nine years from now, Kephart thinks Real ID will still be considered a "huge win" for the American people. That's obvious from polling that shows 70% to 80% of people favoring it.

"I think Real ID meets what the 9-11 Commission recommended," says Kephart. "It is a huge improvement over where we've been or where we are now. Who would have ever thought it would be 2017 before this was put in place. But we initially thought it might be rejected and this would have been the only recommendation from the 9-11 Commission that would have failed. From my point of view I don't think we could have asked for anything more than what we have right now."

Pass another travel document

New Passport Card introduces new technology, new set of issues

Another type of travel document has joined the fray: the Passport Card. The ID card is being touted as an alternative to the traditional passport book, but is an additional technology that customs and border officials will have to be prepared to read.

The technology used in the card could become widespread as states bordering Canada and Mexico are considering issuing an enhanced driver license that contains the Passport Card technology. Washington State is already taking applications for the new ID document. But some say the technology used in the card is insecure and could lead to the tracking of citizens.

The Passport Card uses radio frequency identification technology. While RFID comes in many different flavors – some can be read from a great distance while others can only be read from less than an inch – the type chosen for this project is in the former category. It 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 number that acts as a pointer to a record on a secure database that will contain the cardholder's photo and other biographic information. As a cardholder approaches the border crossing the card is placed on the dashboard and is read as he approaches the checkpoint. When the car pulls up to the border official he will already have reviewed the information and there is little left to do before the passenger can go on his way.

The need for the Passport Card came out of the Western Hemisphere Travel Initiative. WHTI is part of the Intelligence Reform Terrorism Prevention Act of 2004, which requires citizens from the U.S., Canada and Bermuda to have a passport or other designated document that establishes the holders' identity and nationality when entering the U.S. from a land or sea border crossing. The Passport Card is $45, cheaper than the $100 for a Passport book.

The RFID chip used in the Passport Card is similar to the technology being used in the NEXUS, SENTRI and FAST programs run by the U.S. Department of Homeland Security. NEXUS is a program that enables pre-screened travelers from the U.S. and Canada to expedite their travel at airport and land border crossings. SENTRI is a program in place at the U.S./Mexican border enabling quicker crossings at border checkpoints. FAST is a program for truck drivers that have been prescreened to take advantage of fast security lanes when crossing northern or southern border crossings. There are 400,000 participants in these programs.

The U.S. State Department is issuing the Passport Cards. Applications were accepted as of Feb. 1 and the first documents will be sent out in the spring. General Dynamics Corp., Falls Church, Va., received the potential five-year,

$99.3 million contract to issue Passport Cards for the State Department.

But states bordering Mexico and Canada may be the bigger market for these cards. As of mid-February, Washington State has booked more than 11,000 appointments for residents who want an enhanced driver license. Vermont and Maine are also reportedly considering enhanced driver license programs.

Washington began accepting applications for its program in late January, says a Washington Department of Licensing spokesperson. The new ID costs an additional $15 on top of the $25 license renewal fee.

To obtain one of the new licenses, applicants must undergo an interview in which they present a certified birth certificate and other identity documents. Confirming the residents citizenship is the new aspect of the process, says Andy Mallinger, director of product management at Digimarc Corp., the Beaverton, Ore.-based Company that is providing the driver licensing systems to the state. But it's a provision that all states will have to meet if they are going to comply with Real ID, (see story, page 18).

After the resident is approved he receives the new ID card in about a week, the spokesperson says. The enhanced documents are produced at Digimarc's central processing facility.

While the Passport Card is similar to the NEXUS, SENTRI and Fast programs, customer and border officials will also have to be prepared to read other identification documents as well. Electronic passport, traditional passports and Permanent Resident Cards, or Green Cards, all use different technologies.

While traditional passports will eventually be replaced by ePassports there is some question as to why Homeland Security decided not to use the contactless technology used in the new passports, says Randy Vanderhoof, executive director at the Smart Card Alliance.

"It's forcing the creation of duplicate infrastructures at the border to read these new documents while there are already 15 million people who have ePassports," he says.

"The insanity of this is considering what will happen at the border," Vanderhoof says. "Some people will have ePassports, some will have traditional passport, some will have enhanced driver licenses and some will have the new Passport Cards. You're going to have to separate people as they queue up in line."

Vanderhoof says the industry questioned the use of long-range RFID for this program.

"The information on that tag is free-read. It is not encrypted," he says.

And while the only information available from the chip is just a serial number, it could still be used to track that individual without his knowledge, Vanderhoof says. For example, sensors could be set up in a business district to track where individuals are at different times of the day.

Washington State is combating this potential problem by giving cardholders sleeves that prevent the card from being read, says Roland Fournier, senior product line manager at Digimarc.

SESAMES winners may offer a glance at what's to come

SESAMES 2007

MES SESAMES SESAM

SESAMES winners are often predictors of the future. For example, Sony's FeliCa technology, a past winner, is now one of the dominant contactless solutions in Japan and is making inroads in other parts of the world. The 2007 award winners, presented at the annual CARTES show in Paris last November, included a web-centric, browser agnostic software application, a new two-chip SIM geared for mobile phones that could give a boost to NFC implementation, an application enabling users to make secure bank card payments via Internet Protocol Television and even an application looking to produce an alternative NFC-style application – tags that can be affixed to cell phones.

Despite the transport strike, CARTES and Identification 2007 set a new attendance record of 20,109, a 3% increase over the previous year with 147 countries represented.

There were also a record 211 applicants in this year's SESAMES contest with the Hardware category setting the pace featuring 39 applicants, followed by e-Transaction with 34, Banking/Finance, 34, and Software, 31. Just one company this year took home two awards, Oberthur Card Systems, which gathered top honors in the IT Security System and Mobile categories.

IT Security

The company's smart USB token, called Cardblade, is cut and punched into a card body like a SIM plug. It can be manufactured with standard card equipment and customized with any graphics or text. It can be inserted into a USB port and provides security and strong authentication including an e-signature. Also, due to its contactless interface, it can be used for physical access control or any other contactless application such as transport or payment.

Oberthur beat out two other finalists in the IT category – Sagem Défense Sécurité with its Ypsid e-1 authentication device designed to fight ID theft on the web and Vasco Data Security with its Digipass 840cv, smart card-based e-security system for the blind and visually impaired.

Mobile

In the Mobile category, Oberthur won with its SIMphonIC FlyBuy Duo, a Java Card that can work on either 2G or 3G networks, and provides a platform for rolling out 3G applications. The FlyBuy is a two chip SIM: one (U)SIM and one payment certified chip. It can be immediately deployed for mobile payments with NFC mobile phones, complying with the needs, according to Oberthur, of both banks and mobile operators. Oberthur says the FlyBuy Duo was designed "following an intensive study of the NFC Mobile Payment ecosystem's specific needs."

The other three finalists in the Mobile category were the BlueSky Positioning/AGPS SIM, which claims to be the world's first assisted-GPS module for SIM cards; Gemalto's MySharedProfile, a tool for strengthening social networking through dynamic updates of phonebook content; and Simulity's Smartcard web Server Script, a program that enables web application designers to use smart card security features and more in web pages even if they don't have Java programming knowledge.

"Innovation at Oberthur Card Systems has again been recognized, this time for its solutions in mobile payment and NFC, but also in identity," said Philippe Geyres, Oberthur Card Systems CEO. This marks the third straight year that Oberthur has won a SESAMES award. The company was nominated in three other categories in 2007.

Banking/Finance

Atos Origin Company's winner in Banking/Finance/Retail was its Secure Internet Payment Solutions Internet Protocol Television project (SIPS IPTV) that enables users to make secure bank card payments via interactive television channels.

According to Atos, an international information technology services company, SIPS is designed for content providers already offering services via the IPTV channels run by Internet access providers (IAPs), major TV networks or retailers which have negotiated with their IAPs for the delivery of interactive services over their IPTV channels or the IAPs themselves, which could offer the payment system to future IPTV services in addition to their own invoicing systems.

With SIPS IPTV, users access a secure interface that lets them make card-based payments with their remote control, without having to connect to a web site, call an interactive voice server or call center, or send a letter or email. Atos says that there are currently 3.8 million IPTV subscribers in France, a 120% increase over the preceding year.

2005

2006

2007

OWN THE ENTIRE COLLECTION

900+ pages of ID technology insight just $250

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

For the first time, AVISIAN is offering all back issues of their industry-leading *re:ID magazine* in a packaged set. You receive three year's worth of top-notch news and insight – 12 issues of *re:ID* and 3 issues of *CR80News magazine*. Plus you get password-protected access to our online library with more than 1000 feature articles.

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

AVISIAN

re:ID

SUBSCRIPTION OPTIONS

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

My job title is:
❑ CEO/President ❑ EVP/VP
❑ Director ❑ Manager
❑ Other _____

My primary job function is:
❑ Management
❑ Sales/marketing
❑ Operations/development
❑ Administration

My relationship to ID technology is:
❑ End user ❑ Manufacturer
❑ Reseller ❑ Consultant
❑ Solution Provider/Integrator
❑ Other _____

My primary market focus is:
❑ Government ❑ Corporate
❑ Financial ❑ Transportation
❑ Education ❑ Retail
❑ Other _____

My primary application focus is:
❑ Physical security ❑ Computer security
❑ Payments ❑ Transit
❑ ID issuance ❑ Logistics
❑ Other _____

Number of employees in company:
❑ Under 25 ❑ 25 to 99
❑ 100 to 499 ❑ 500 to 999
❑ 1000 to 4999 ❑ 5000 to 9999
❑ More than 10,000

Annual sales volume:
❑ Under $1 million ❑ $1-10 million
❑ $1 -25 million ❑ $25-100 million
❑ More than $100 million

In the next 24 months, I expect to be involved in a decision to purchase:
❑ Physical security products
❑ Logical/computer security products
❑ Biometric products
❑ ID issuance hardware and/or software
❑ Smart cards (contact or contactless)
❑ RFID systems/components

Subscribe for FREE to *re:ID magazine* and keep up-to-date with the latest news and insight from the world of identity management, biometric, and advanced ID technology. (Free subscriptions available to approved U.S. addresses only. *International subscribers pay $200 per year to cover postage and handling costs.)

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

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

Name _____

Job title _____

Company _____

Address _____

City _____

State/Province _____ Zip/Postal Code _____

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

Phone _____

Email _____

Signature _____ Date _____

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

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

❑ SecureIDNews ❑ ContactlessNews ❑ CR80News ❑ RFIDNews

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

ES SESAMES SESAMES

The other two finalists in the Banking/Finance/Retail category were both Oberthur products – its MoneyIC Visio Fly, a dual prox and mag stripe card designed for non-EMV markets such as the U.S., and its SIMphonIC FlyBuy Duo.

Hardware

INSIDE Contactless' payment platform, the MicroPass L4-2G, which is intended to provide an optimum card read distance with minimal power consumption, took first place in the Hardware category. INSIDE's microprocessor-based contactless payment platform consists of chip hardware and an open operating system designed to meet multi-payment brand and multi-application requirements.

According to INSIDE, more than 35 million MicroPass chips have been shipped to the company's card manufacturer partners for issuers in the U.S., Canada and other regions adopting contactless payments.

"We are proud that our MicroPass intelligent payment platform has been recognized as the leading hardware platform in the industry by the SESAMES jury members," said Rémy de Tonnac, INSIDE CEO. "This award demonstrates how contactless and NFC technology are going to change consumers' daily lives."

INSIDE beat out two other finalists – BlueSky's AGPS SIM and NXP Semiconductors' ultra-thin SmartMX smart card IC, which is 50% thinner than the industry standard and can allow, for example, passport printers and smart card manufacturers more flexibility in design solutions.

Software

Another company nominated in several categories and which walked away with the crown in one – Software – was French smart card manufacturer Gemalto with its web application solution and service which can connect to any smart card regardless of platform or browser. SConnect eliminates the need for middleware and, according to the company, works seamlessly with existing infrastructures, allowing applications to leverage smart cards for security and personalization.

The other two finalists in that category were Gemalto's UpnP Smart Card designed to enable connectivity among consumer electronics and mobile devices, and ViVOTech's ViVonfc Suite 2.0, an application platform for NFC-enabled cell phones, allowing issuers, service providers and retailers to provide coupons, gift and loyalty cards, tickets, payment and promotions on a customer's cell phone.

Identification

A Malaysian company, Iris Corporate Berhad, took first place in the Identification category with its mobile terminal designed for the next generation of chip-based ID cards. Called the IRIS ST4ex, it's a smart card reader designed to offer instant check results on various electronic travel documents and identity cards. Ruggedly-built with long lasting batteries, it has various applications and offers a choice of connectivity – USB, LAN, GSM, Bluetooth and IRDA. It is currently being used in Malaysia to monitor a diesel subsidy program where fishermen buy diesel using a smart card. In Nigeria it is used as an electronic voter registration system.

Iris bested three other finalists in the Identification category: DS Consulting's contactless card reader with two physical levels of communication security; International EFT Systems' Smart Pen Mouse that includes a .NET smart chip that can serve as a pointing device; and Sagem Défense Sécurité's MorphoPath, a motion-detection device that can be installed in existing electro-mechanical security gates at airports or other areas needing extra security.

Transport

Australian company UltraPay, which specializes in mobile wireless payments and authentication with a focus on in-vehicle solutions, won SESAMES' Transport category with its MT3000, a mobile card reader designed for the taxi and limousine market. Melbourne, Fla.-based Hydrix developed the reader, which accepts both contact and contactless cards. The MT3000 POS terminal is a wireless biometric payment terminal and, according to Hydrix, the first mobile payment terminal to achieve the new VISA/MasterCard PCI PED security standard as well as EMV Level 1 and 2 approvals.

The two other finalists in this category were ERG Group's Systems5000-UTA ski service pilot which is currently being used on the bus system that serves Salt Lake City ski resorts, allowing customers to use smart cards for fare payment and ski resort access. The other finalist was Kentkart Edge Electronik's KV150 Validator, a smart card reader for transportation, parking, exhibition and event ticketing.

MES SESAMES SESAM

Health Care

In Health Care, MXI Security's Stealth MXP, a USB-powered portable security device, took first place. The Stealth MXP is a FIPS 140-2 Level 2 validated security solution allowing health care workers to carry up to 4 GB of data with transparent embedded hardware encryption. The MXP also allows organizations to store users' digital identity credentials, making sure its strong biometric authentication prevents unauthorized access to critical resources, such as patient records.

"We are proud that MXI Security's Stealth MXP was recognized as the best portable security application for the healthcare marketplace, an industry where health systems, hospitals and healthcare workers know that the privacy of peoples' medical information is a priority," commented Gerard Reusing, president, Europe and Asia, for MXI Security.

"To a larger extent, it is increasingly important that industries such as biotechnology and pharmaceuticals protect the sensitive personal identifiable information and intellectual property-related data that employees access and carry daily."

The other two finalists were aZensys Industries' PIM, a mobile personalization platform that allows organizations to issue smart cards regardless of place or time, and Xiring's PRIUM-3S, a desktop reader designed by and for healthcare professionals. According to the company, it is the first three-slot reader that secures transactions with three signatures and three cards at the same time.

e-Transaction

In the e-Transaction category, NXP Semiconductors walked away with the top honor for its secure Display-on-Card inlay solution which combines a display module with a smart card controller. The solution supports three operating modes: stand-alone with a battery and multiple buttons, with an antenna for contactless, and with a contact interface for terminal operation. The other two finalists were Tagattitude's Audio Tag, which won in the Loyalty category, and Unipay's MaâtCard, a prepaid bank card that can be used for several functions, including transferring funds, and purchasing products online.

Loyalty

Tagattitude's Audio Tag, the Loyalty category winner, bills itself as "technology that can transform any existing mobile phone into a secured payment tool." Called Near Sound Data Transfer (NSDT), this technology offers electronic signature, one time password, and cryptographic key management to secure electronic transactions and strong authentication services. NSDT uses the audio channel and the security features of any standard mobile phone and, the company says, is compatible with all existing mobile phones worldwide.

Two other finalists in the Loyalty category were Gemalto's Dexxis Instant Issuance application which enables banks and retailers to issue personalized cards at their branches or point-of-sale, and Oberthur Card Systems' PayPhone based on a USB key contactless solution, allowing for secure online transactions.

CARTES and the accompanying SESAMES awards for 2008 will be held Nov. 4-6.

e-Government 2.0: Leading the way for digital transformation

Editor's note: *Following are excerpts from a 2007 report entitled* e-Government 2.0 … Identification, Security and Trust … Exploring European Avenues. *It was commissioned and co-authored by Gemalto. The report gives an overview of what European countries are doing in the realms of identification and security.*

Eric Legale, secretary-general of the World e-Democracy and Electronic Administration Forum, summarizes the report's objective in the preface: "The strength of this report is that it finally gives us real reason to hope for a new universal era of renaissance with the now inevitable development of the Knowledge Economy and Society. The fact that identity is at the heart of this transformation is only more evident as it is simply a question of renewing and sometimes reinventing the relation between the individual and the community."

Eric Billiaert and Etienne Veyret, *Gemalto*
Youval Eched, *YeMA Consultants*

Governments today are faced with ever stronger demands from citizens and businesses that their needs be taken into account.

One of the challenges of the modernization of public services involves managing this information subject to a strict observation of citizens' confidential data and their right to privacy or – at the very least – the possibility for everyone to control the use of their personal data.

Public services must maintain their principle of equality and universality in the face of a public that demands personalization and individual responses to the complexity of their needs on a daily basis.

Citizens' trust is particularly dependent on their need to feel their personal data are protected and kept confidential … electronic identification contributes to this need.

A revival of democracy

We live in a demand-driven world and there is now a strong trend towards soliciting the opinion of citizens regarding how society functions on both a local and national level. In Europe, in Asia and in South America, politicians are increasingly acting based on the opinion of citizens present in online debates, but the most popular use of new media in this trend remains the practice of e-Voting.

Participation is increasing with numerous schemes being adopted in countries like Estonia, Belgium, France, Spain and Brazil. However, other schemes – such as those in Ireland and Great Britain – have been scrapped due to security failures.

Indeed, Estonia's commitment to the web for e-Voting is clear. After the local elections in 2005, in which this Baltic State with some 1.4 million inhabitants became the first country in the world to use online voting, it continued its strategy with its parliamentary elections in March 2007.

The chance to change one's mind

Thanks to the Internet, Some 940,000 Estonians were able to vote in advance preceding the Sunday national poll. By inserting their ID card into a reader attached to a PC they were able to access a secure web site where they could vote and sign the vote electronically.

If the citizen made a mistake, or they thought they'd been influenced while voting by people around them, they were able to vote again on the Sunday, by deleting their online vote and using the traditional secret ballot. In 2005, only 30 voters out of 9,317 changed their minds during the local elections.

According to Tarvi Martens, director of operations for Estonia's certification body, "the Estonians have nothing to fear from online voting. They already have trust in their financial transactions on the Internet; they send their tax declarations online and do money transfers via electronic banks. Why should they not trust voting online?"

Over 30,000 Estonians – 3.13% of the electorate – voted electronically. The Estonians believe it is just a question of time before critical mass is achieved.

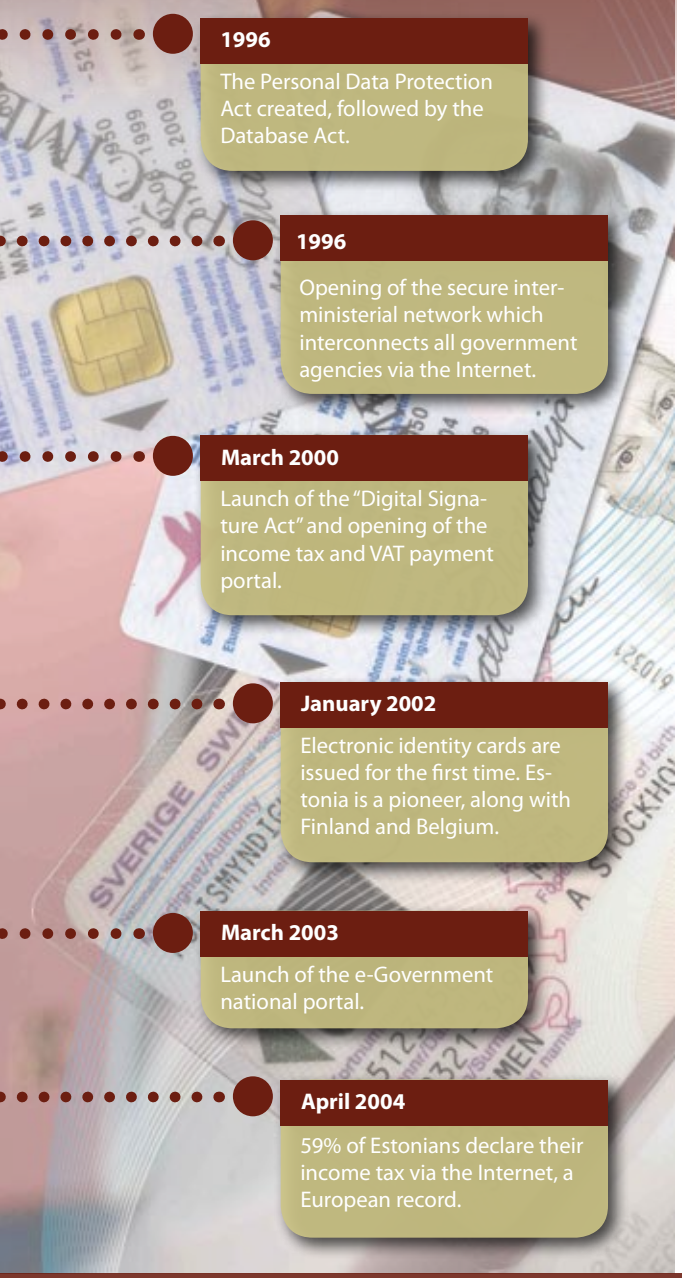
e-ID: A key to e-Government?

Over the past ten years, the number of private and professional digital exchanges has increased from 100 million to some 15 billion sent every single day. But despite this familiarity, citizens are aware of the relative

Tiny Estonia leads the e-ID revolution

The Republic of Estonia's 1.3 million citizens formally declared their independence in 1991 after years of Soviet occupation that had begun during World War II. The then Soviet Union, involved in its own internal problems that were slowly leading to its disintegration, was in no condition to argue. Estonia joined both NATO and the European Union in 2004.

Today, the Northern European country, which borders Latvia to the south and Russia to the east, is described by the Gemalto e-Government 2.0 report as a "shining example" in the e-ID revolution.



1996

The Personal Data Protection Act created, followed by the Database Act.

1996

Opening of the secure inter-ministerial network which interconnects all government agencies via the Internet.

March 2000

Launch of the "Digital Signature Act" and opening of the income tax and VAT payment portal.

January 2002

Electronic identity cards are issued for the first time. Estonia is a pioneer, along with Finland and Belgium.

March 2003

Launch of the e-Government national portal.

April 2004

59% of Estonians declare their income tax via the Internet, a European record.

fragility of electronic media, and expect the same levels of security and trust they know in the physical world. This has given rise to a demand for guaranteed identification of senders and receivers.

In 1997, the very first secure electronic identity cards were produced, and called e-ID cards. Many projects soon emerged, but in Europe, it was Finland that deployed the first operational prototypes, quickly followed by Estonia and Belgium. French and Italian "city cards" also offered a similar basic technical approach at around the same time.

In December 1999, all European players signed the "e-Signature" directive, to enforce the use of cryptography and certificates to give a legal validity to e-Communications and e-Contracts.

Beyond their usage for digital signatures, or as city cards, these IDs also offered a range of other applications, such as physical access, social security, driver licenses, healthcare, payments, banking and transportation solutions. But if they were eventually to replace traditional ID documents, they had to work as a travel and physical ID document, as well as be valid in other countries.

The cards also aimed to provide access to a maximum number of e-Government services, but this became somewhat complicated as identity has a wide variety of interpretations from one country to the next. And the establishment of numerous regulatory frameworks also slowed down the interoperability and mutual recognition of these documents between member states.

Experience has shown that e-ID has become a real lever for the success of e-Government. This is particularly evident in countries where the communication that accompanies the modernization of relationships with citizens and businesses has demonstrated that e-ID is first and foremost an efficient tool for exercising and protecting citizens' rights.

e-ID in full expansion

Beyond the traditional physical security, payment and online applications of the e-ID card, new areas are being tested where the card can provide added benefits to citizens and businesses:

- Monitoring, records and prevention in healthcare (Belgium, France, Germany, Portugal and Southeast Asia);
- Help for children in danger (Belgium);
- e-Ticketing for local transportation networks with periodical global billing (Estonia, Spain and Belgium);
- Securing purchases in extended enterprises (France, Belgium, Italy, etc.);
- Access cards to secure private or public spaces or public garages;
- Professional cards to provide the link with a person's qualifications and mandates, particularly in regulated professions like lawyers, notaries, auditors, bailiffs, doctors, surveyors, registrars, pharmacists and vets;
- e-Voting, e-Participation and free Internet access for citizens wishing to attend local council meetings online (Estonia, Belgium, France, Barcelona in Spain, etc.).

The smart card with its incorporated microprocessor is considered to be the safest authentication media to guard against identity fraud and efficiently protect citizens' personal data. It is the media of choice for access to e-Government applications. It can also be used in many other applications including payment cards, e-Purse applications, signatures, authentication, identification and ticketing solutions.

It is important to adapt to local culture in relation to ID documents. Some countries may find it easier to launch a driver license-based e-ID project. In these cases, an element of complexity emerges – particularly in Europe – because one must chose between ICAO compliance for travel documents and conforming to the new European Directive on Standard European Driver Licenses which do not place the photograph in the same spot. As specifications are not finalized yet, the 'Driver License' directive may offer optimal convergence.

For example, in Sweden, 3 million electronic identification cards have been distributed mainly by banks. One million users are generating 2.5 million transactions a month using the authentication and signature services. The national smart-card based ID card is one possible support with mobile phone and personal computer.

e-Government: the front office of a "service-oriented" state

At the end of football world cups, it is customary to name a "dream team" of the best players on the planet. If we were to have a similar approach for e-Government, compiling all the best practices observed, the ideal site would:

For the Individual/Citizen

- Organize and facilitate learning. In Estonia, for example, e-Government is currently included in the civic education of young people at school.
- Promote the service, facilitate information gathering and knowledge, organize communication in the same way modern private-sector service providers manage their customer relations. In Belgium, web sites, brochures, ideas contests, radio adverts, 24/7 help lines and local coordination have all been used.
- Organize access to and presentation of the site on the basis of needs, with an access by end-use and by rights field. The State's back office has its own structure, but this must be hidden from now on. When we order a car, the manufacturer does not tell us about the difficulty involved in swapping parts from one production center to another. This is normal. It is the same for government bodies.
- Coordinate and pool information to ensure accessibility and responsiveness, and meet the demand for real-time services which is becoming widespread. Offer the possibility of face-to-face communication as well as electronic services in the interests of promoting e-inclusion and solidarity with the most disadvantaged.

For government bodies

- Drastically reduce unnecessary bureaucracy, undertake necessary re-engineering work, ensure interoperability of processes and migrate from a paper-based culture to an electronic culture. This may represent something of a revolution, but it is a necessary transition.
- Prioritize the need for transparency, whose effect on uptake and success is proven and undeniable.
- Emphasizing the protection of individuals' privacy and personal data is essential to obtain their trust and ensure the success of e-Government. The use of e-ID, essential if this challenge is to be met, must be designed with this approach in mind.
- Using banks as partners for payment and including them in the Network of Trust as vectors for the promotion of e-Government accelerates the implementation process.
- Using as many local and proximity applications as possible to promote the daily use of e-ID – a gateway to e-Government – will boost uptake. Cooperation between states and local authorities enables the emergence of local authorities to be emphasized as well as their contribution to e-Government on a national scale.

SecureIDNews

October 2005

First e-Voting attempt for local elections occurs on Oct. 16. Nine thousand Estonians choose to vote from home using their e-ID.

May 2006

Banks, telephone operators and the Ministry for Economic Affairs and Communications sign an agreement to jointly launch the "Computer Protection 2009" program to make Estonia a world leader in terms of protecting citizens and their privacy through the generalized use of e-services that require e-ID authentication.

July 2006

The university online registration portal is opened and is accessible from the citizens' portal.

March 2007

Estonia becomes the first country in the world to vote via the Internet in its general elections. 30,000 voters, or 3%, choose to vote this way.

May 2007

Estonia announces its citizen SIM card, including an identification certificate delivered by the state for mobile telephone identification. Estonia is now on the same level as Finland, which had launched its initiative in 2005. The program includes cooperation and interoperability with Finland.

June 2007

2006 annual economic growth is reaching 11.4%.

CTST gets a makeover with help from Smart Card Alliance

The technology show, scheduled for May 12-15 in Orlando, Fla., is rebranding from CardTech/SecurTech to CTST, and it has a new partner. The Smart Card Alliance has joined forces with SourceMedia, CTST's producer, to manage the show's content.

It's as if the Alliance is returning to its roots, since the CTST conference was originally a joint venture between smart card pioneer Ben Miller, the conference founder and former chairman, and the Smart Card Industry Association, a vendor group that merged with the Smart Card Forum to create the Smart Card Alliance. CTST was founded in 1991 and purchased in 1998 by Faulkner & Gray, now SourceMedia.

"We decided the brand name should stay but it's not just about cards anymore. A lot of great things are happening. People are paying by waving their telephones," says Dan Rubinetti, vice president of conferences and events at SourceMedia.

SourceMedia's conference group produces 50 to 70 conferences a year but it is also a large business-to-business media company, publishing more than 30 trade publications, including *Cards & Payments*. The New York-based publisher also produces email newsletters, web seminars, and virtual trade shows.

The new CTST partnership was Rubinetti's idea. He approached Randy Vanderhoof, executive director of the Smart Card Alliance, at last year's event in San Francisco. "Randy was always a contributor to our event and I told him that I thought we were missing an opportunity to combine my group's ability to execute shows along with his knowledge base," he says. "We're good at putting on events and Randy lives and breathes this industry every day."

"As we began to evaluate the direction we were going with the Smart Card Alliance annual conference, we realized there was a lot of overlap with CTST," says Vanderhoof. "One of our limitations is that we lack the resources to put together a full conference and exhibition. We saw an opportunity to link up with SourceMedia and thought it was a good fit for the Alliance. Our strength is in industry connections and contacts and both organizations complemented each other. We knew that combined we could put together a larger conference event."

Like CTST, there had also been "an increasing expansion of the Alliance's annual conference into areas beyond smart cards, for example, smart cards and how they impact on different markets that are undergoing evolutionary changes and convergence," adds Vanderhoof. "We had previously run our government-focused events in the spring, usually before CTST, then our annual conference in the fall. With this change, we've moved our annual conference to CTST and our government event to the fall, which will remain independent."

Under the partnership, which will be active for at least two years, the Alliance will control the program content and will support the marketing and exhibition portion of the conference, says Vanderhoof.

SCA's 180 member organizations representing some 1,300 people will receive a 10% discount on exhibition space, sponsorships and a registration discount, says Vanderhoof.

The rest of the CTST makeover comes in the way the conference is laid out this year, and in its name, says Rubinetti.

Officially, the conference is listed as CTST The Americas 2008, to incorporate both North America, including Canada and Mexico, and Latin America, where the Alliance also is active. Listening to Vanderhoof explain what's on tap in May, it appears the hardest decision is what to attend.

The conference's overall theme is the future of payments and security, which have been the two primary drivers in the industry, says Vanderhoof.

"We're opening it up to payments and the mobile market more," says Vanderhoof. "Previously, CTST was more security-focused but now we're trying to bring everyone together to see this convergence. This is a great opportunity to learn what the other markets are doing."

The conference will be laid out in four major tracks covering identification and policy, payments and applications, mobile and NFC and security and access control. Two "mini-tracks" will highlight emerging technologies and Latin American innovations.

"We looked at the payment market and felt there were two complementary tracks – traditional bank payments and advances in contactless – and mobile and NFC as the new emerging payment platform of the future," says Vanderhoof. "We built two separate tracks to cover each of those topics. They're organized around identifying the application, identifying the users or implementers of the technology and then highlighting the users of the technology and where it's being deployed."

The other half of the agenda is built around identification and security. "In the ID and policy track, we'll be looking at ID policy and its use in electronic governance, such as passports and HSPD-12, driver licenses, privacy and security," says Vanderhoof. "We've also included healthcare under that track."

In security and access control, the track will investigate the deployment of physical and logical security both in government and enterprise markets, he adds. "We're including some of the changes in technology around different forms of radio frequency, access control, PKI, and some of the new standards developing," Vanderhoof says.

For those who want to understand the cutting edge technologies that are leading to new developments, this mini-track would be for them.

"The sixth and final track is on Latin America. This CTST is not just a U.S.-centric event but one for the Americas," says Vanderhoof. "We've developed some content specifically for those coming from Mexico, Brazil, Columbia and other countries to have a session on their markets. Those will be presented in Spanish and Portuguese. Latin America has recently seen a large uptake of smart card technology."

So why should someone attend? "One of the cool things is that you'll have your choice of these different tracks. You can create your own conference experience. If we can bring them that good solid content, show them best practices people will come away with a good knowledge of what's out there," adds Rubinetti.

"With so much convergence talk happening across industry verticals, particularly in the payments and mobile arenas, attendees can choose to focus on one track, or mix and match sessions from different tracks to get a broader perspective on the market," adds Vanderhoof. "The mobile and NFC track is an exciting new addition to CTST, and timely, with pilots ramping up all over the world enabling consumers to pay for goods and services with a wave of a mobile phone."

Keynote speaker will be *New York Times* technology columnist and Emmy-winning CBS News correspondent David Pogue, who will speak at the CTST luncheon May 14.

"David Pogue is the authority that consumers look to for an informative and entertaining look at all of the newest technologies and trends," says Vanderhoof. "Recent initiatives in the smart card industry, particularly

Participate in AVISIAN's video coverage at CTST

Schedule an appointment to "go live" with the AVISIAN Video Team at booth #1101

Do you have an exciting new product offering? Do you want to discuss the future of the industry and your company's role?

re:ID and AVISIAN Publishing are proud to serve as the official video partner for CTST 2008. Our team will be on the show floor capturing the action in streaming video and audio formats – to be broadcast online at *SecureIDNews.com*, *ContactlessNews.com*, and other AVISIAN publications.

Contact us for more information and to schedule an interview slot during the show. We're looking forward to introducing an new, exciting element to the CTST experience.

For more information, please contact:
Angela Tweedie
angela@AVISIAN.com • 850-391-2273

in contactless and mobile payments, are built around consumers, and their success depends on consumer awareness and adoption. David understands how consumers think."

There will also be keynote executive roundtable sessions each of the conference's three days, says Vanderhoof. "The first day is on the future of smart cards. Executives from each of the four major smart card companies – Oberthur, Giesecke & Devrient, INSIDE Contactless and Gemalto – will answer questions on how each of the vertical markets – transit, payments government identity and security and mobile – are adopting smart cards differently," he adds.

The second day roundtable will focus on the future of payments and how the ecosystem is evolving. That session will feature speakers from MasterCard Worldwide, Verifone, First Data Corp. and Monitise Americas, says Vanderhoof.

The third roundtable, on CTST's closing day, will look at the future of security, "and how the pieces will fit together," he says. That one will feature speakers from Infineon Technologies, RSA Securities, ActivIdentity and GlobalPlatform. "We'll look at the security market ecosystem, middleware and digital certificates, enterprise-wide security and open and interoperable standardization."

These three sessions are free to everyone at the conference, he adds, as is the Smart Card Alliance networking reception on May 12. "At this event, we'll announce the winners of our Outstanding Smart Card Achievement awards. Three OSCAs will be issued: one for individual leadership, another for issuing organization and a third for outstanding supplier.

CTST 2008 will feature an expanded and revamped exhibit hall. Last year there were 122 exhibitors but more are expected this year. "We've certainly got space for plenty," Rubinetti says of the Orlando Convention Center.

SCA will have its own exhibit space, "where we're going to have presentations from each of our industry councils on display," says Vanderhoof.

There also will be three pre-conference day-long workshops on May 11 at the convention center. The first will cover technology and payments applications and is sponsored by the Smart Card Alliance; The GlobalPlatform Value Proposition for Identity Management and a seminar on the Open Authentication Architecture for the Universal Adoption Of Strong Authentication, sponsored by the Open Authentication Initiative, rounds out the pre-conference sessions.

Conference attendees will also have a chance to win a two-year lease on a Mercedes SLK, a contest sponsored by Infineon. CTST's largest sponsor is Oberthur, which is handling the registration area. In addition, G&D will have a pavilion that will give those with exhibit hall-only passes, rather than those with a full registration, a taste of the CTST education sessions.

"It will be set up like a mini-auditorium on the exhibit floor. Anyone with access to the exhibit hall can sit and enjoy these sessions on different topics. Our technology tours of the exhibit area will also begin there," says Rubinetti.

For more information and to register go to *www.ctst.com*.

L-1 Identity Solutions acquires Bioscrypt

Acquisition is part of ongoing effort to become a one-stop shop for identity needs

Jennifer Slattery
Contributing Editor, AVISIAN Publications

The acquisition of Toronto-based Bioscrypt Inc. is the latest purchase for the Stamford, Conn.-based company, L-1 Identity Solutions. Over the years the company also acquired Viisage, Identix, Integrated Biometric Technology, SecuriMetrics, Iridian, SpecTal, ComnetiX, McClendon and Advanced Concepts Inc. "L-1 is the first true consolidator to emerge in the biometrics and identity space," says Jeremy Grant, senior vice president and identity solutions analyst at the Stanford Group Company.

L-1's all-stock purchase of Bioscrypt is estimated to cost the company $43.8 million and is expected to be approved by Bioscrypt's board of directors by the end of March.

The acquisition will increase L-1's product offerings in the fingerprint physical access control market. Bioscrypt has more than 400 global customers and an installed base of more than 260,000 access control units. Customers include Kronos, Honeywell, Lenel and ADI. Identix, one of L-1's previous purchases, had competed against Bioscrypt in the physical access control markets but exited the market, Grant says.

Bioscrypt also has one of four fingerprint scanners that has been approved by the Transportation Security Administration for use in airports for access control.

Grant says Bioscrypt's 3D facial recognition technology is one that has "impressed" him. 3D facial recognition uses infrared light to scan an individual's face and maps the contours. Theoretically it addresses some of the limitations of standard 2D facial recognition. The Venetian Macao-Resort Hotel has deployed the technology for employee access control.

Bioscrypt's VeriSoft security software is now included on more than 20 million Hewlett-Packard computers.

The addition should help Bioscrypt expand its product presence, says Matthew Bogart, vice president of marketing at Bioscrypt. "L-1 helps us advance our business significantly. We will be able to have expanded product offerings beyond just biometrics and multi-factor authentication."

L-1 appears to be setting itself up as an identification super power, but the company still faces some opposition, Grant says. "L-1 faces stiff competition, both from other biometric and identity vendors, as well as from major systems integrators that are in the midst of assembling their own integrated identity platforms," he says.

Grant predicts 23% compound annual growth for U.S. government spending on identity systems between fiscal years 2007 and 2009. "Growth in identity and biometrics solutions will be significant over the next ten years as dozens of countries, states and localities implement enterprise-class systems," he says. "Outside the United States, major projects are going forward in the areas of national ID cards, ePassports and visas, voting, law enforcement and border management."

L-1 has been active with a number of contract wins. The company recorded orders of more than $60 million, including $6.3 million in purchase orders from the Department of State for passport printers, and a $3.7 million deal to modernize Panama's National and Voter Registration ID system. L-1 declined to be interviewed for this story.

DHS budget includes funds for biometric and ID projects

Zack Martin
Editor, AVISIAN Publications

President Bush is asking for $390.3 million to fund the US VISIT program for the 2009 fiscal year. Other biometric and identification programs, including Real ID and the Western Hemisphere Travel Initiative, were also highlighted in the U.S. Department of Homeland Security's budget-in-brief.

But the overall budget is a mixed bag for security and identification projects, according to Jeremy Grant, senior vice president and identity solutions analyst at the Stanford Group Company.

Real ID and the FBI's Next Generation Identification (NGI) program are the only notable winners in the 2009 fiscal year budget, Grant says. Real ID gets its first-ever support in a White House budget, with $50 million in dedicated funding and a separate pool of grants funds available to states.

Total NGI system spending is forecast to rise 9% – but actual spending growth on the biometric aspects of the system will likely exceed this number as the program gets into full swing in 2009. Lockheed Martin Corp., Bethesda, Md., was awarded the contract by the FBI in February.

The $390.3 million for US VISIT is an 18% cut from the previous year, Grant says. US VISIT, which is upgrading to 10-prints in 2008, matched more than 160,000 travelers against its watch list in the 2007 fiscal year. Latent print identification identified 129 previously unidentified individuals. The US VISIT fingerprint watch list is 3.2 million sets of prints. The program also began remote biometric identity verification. Working with the U.S. Coast Guard, US VISIT extended biometric verification to remote locations where no information technology infrastructure existed.

A priority for the 2009 fiscal year, which begins Sept. 30, 2008, is creation of a comprehensive exit portion of US VISIT. The agency is asking that $42.6 million of the $390.3 million be used to help create this portion of the system. All citizens are fingerprinted as they come into the country, but attempting to confirm their exit with biometrics has been more difficult. Some travelers have used their biometric when leaving the country while others haven't. The agency will also look at a biometric exit solution at land borders.

Integrating the US VISIT fingerprint database with the FBI's IAFIS is another priority for the agency in the coming fiscal year. The agency is requesting $4.2 million to aid in this incorporating the two systems.

DHS is asking for $106.9 million to support implementation of technology to support the Western Hemisphere Travel Initiative (WHTI) at land border crossings. The funds will go to complete infrastructure improvements at the top 39 land ports of entry covering 95% of the land border arrivals.

In FY 2008, DHS received $225 million to develop the primary vehicle application, install hardware and make the necessary lane modifications to implement WHTI at 13 high-volume ports. The FY 2009 increment would pay for the completion of infrastructure improvements at the non-Radio Frequency Identification point of entry (POE) and pays for program management and support of the previously installed POEs.

As a part of WHTI, some border states are implementing enhanced driver licenses so residents can use one ID for both purposes. The new licenses are equipped with RFID chips so they can be used for identification at land border crossings.

DHS signed agreements with the states of Washington, Vermont, New York and Arizona to enhance the security of their state driver licenses and potentially satisfy Real ID requirements or serve as alternatives for entry at land and sea borders.

In order to comply with Real ID, states will have to verify a resident's citizenship. DHS' Bureau of U.S. Citizenship and Immigration Services is asking for $50 million to develop an information sharing and verification hub that can enable states to verify source documents with other state and federal agencies.

States can also request grants to meet Real ID requirements. DHS is asking for $2.2 billion for the Homeland Security Grant Programs, Infrastructure Protection Grant Programs, Emergency Management Performance Grants Program and Assistance to Firefighters Grants. The Transportation Worker Identification Credential is slated for $26.6 million in funding for the next fiscal year. Since October, 7,000 port workers have enrolled in the TWIC biometric credential program.

More than 750,000 longshoremen, truck drivers, port employees and others requiring unescorted access to secure areas of ports will ultimately be required to obtain a TWIC.

US VISIT rolling out 10-prints at airports

Foreign nationals coming into some of the busiest international airports in the U.S. will have ten fingerprints scanned instead of two.

The new fingerprint scanners have been rolled out at George Bush Intercontinental in Houston, O'Hare International Airport in Chicago, Boston's Logan Airport, Hartsfield Jackson Atlanta International Airport and Washington Dulles International Airport. The system will be introduced at four other airports by the end of February.

There are signs that greet travelers when they enter the check-in area at O'Hare telling them they will be asked to place their right four fingers on the scanner, then their left four fingers and finally the two thumbs.

US VISIT began collecting the two index fingerprints of visitors to the U.S. in 2004. Ten prints give the U.S. Department of Homeland Security more information to work with and the ability to check other government databases.

Now when the visitors are scanned at the airport their information is checked against a watch list of 3.2 million prints. Eventually the US VISIT database will be able to query the FBI's IAFIS fingerprint database, which holds approximately 55 million sets of prints, in real time as well. Currently that search is done at a later time.

O'Hare is the latest airport to make the switch to 10 prints following Boston's Logan Airport last week, Hartsfield Jackson Atlanta International Airport earlier in the month and Washington Dulles International Airport in November.

US VISIT officials are analyzing data from those sites and seeing how taking the additional prints impacts the time at the checkpoints. During a demonstration of the system at O'Hare, four passengers from Tokyo went through the new procedures. It took less than two minutes for all passengers to get through the entire check in process with the longest taking approximately one minute 44 seconds and shortest taking one minute, 12 seconds.

O'Hare Customs and Border Protection officials are using the L-Scan Guardian fingerprint scanners from Cross Match Technologies, Palm Beach Gardens, Fla. The Identix Touch Print 4100 Enhances Definition Device is also being used at some airports.

Match-on-Card has gained new interest for FIPS 201 and TWIC

Consuelo Bangs
Senior Program Manager Access Control Solutions, Sagem Morpho Inc.

Match-on-Card (MOC) with secure messaging (SBMOC) has the potential to become part of the Federal Information Processing Standard 201 (FIPS 201) and may prove useful for the maritime Transportation Worker Identity Credential (TWIC) program.

MOC is the process of sending a biometric template from a live capture device to the card. The card processor receives the biometric template and matches it to the reference biometric template stored on the card. Secure messaging is the process of encrypting the biometric template created by a biometric sensor and sending it to the card for decrypting. What makes this significant is the protection the secure messaging process provides to personal identity information (PII) as it is transmitted across a contactless interface using radio frequency technology.

Identity verification access control applications over the past ten years have steadily migrated from contact readers to contactless readers to read data from an identity credential card.

FIPS 201 requires a PIN be entered before the biometric template may be accessed through the contact interface. It also prohibits reading and transmitting PII data across a contactless interface due to concern that data may be "sniffed" or stolen as it is passed along the RF interface.

This has created a disconnect between operational environments and the specifications of the FIPS 201 standard. When the maritime community, implementing the TWIC card based on FIPS 201, stated that contact readers and PIN entry were unsuitable for the harsh marine environment, the TWIC biometric reader specifications were modified to allow contactless readers. To address the security concern, specifications were developed to require that individual keys for encryption and decryption be written onto a magnetic strip and be accessible from the chip on the card through a contact interface.

A DHS sponsored demonstration of Match-on-Card technology caught the attention of both NIST FIPS 201 and TWIC program management. What captured their interest was the execution of MOC as a separate application in concert with the Personal Identity Verification (PIV) application on a certified FIPS201 card.

This resulted in a NIST feasibility study of MOC technology with secure messaging in which two separate tests were conducted. One focused on performance accuracy and speed of match-on-card algorithms. The other focused on the speed of match-on-card algorithms when using encryption to protect the live biometric template sent to the card for matching (SBMOC).

Performance accuracy and speed testing has moved to a second Phase (MINEX II) and is in progress. The aim of the SBMOC feasibility test was to determine if electronic verification in less than 2.5 seconds was attainable while still meeting functionality, biometric accuracy and security requirements. NIST reported that 17 cards from four suppliers met the goal.

Match-on-card technology would replace PIN entry when authenticating the cardholder to the card. The successful performance of secure messaging with match-on-card may influence NIST to modify the FIPS201 standard to include the transmission of PII information across the contactless interface. This would eliminate the need for individual privacy keys to be written to the TWIC card.

Security programs push forward with biometrics?

Catherine J. Tilton
VP Standards and Emerging Technologies, Daon

This has been an interesting year for biometrics, with a number of high-profile government programs being awarded and/or deployed, both within the US and internationally.

In the US, the Transportation Worker Identification Credential (TWIC) began deployment for maritime workers, the US Registered Traveler (RT) program was rolled out to numerous airports, the US VISIT program is scheduled to begin its ten-print pilot by year end, and many anxiously await the award of the FBI's Next Generation Identification (NGI) system this year as well.

Internationally, the EU Biometric Matching System (BMS), Japan VISIT, and UK e-Borders awards are noteworthy, and all eyes are on the UK as it moves forward on its biometrically-enabled National Identity Scheme (NIS).

Commercial sales are also up with some impressive milestones (e.g., Authentec's 25 millionth sensor), but it's still not where we'd like to see it overall, such as being embraced by the financial sector.

We also saw an increased focus on interoperability. Testing for both general technology performance and interoperable performance took a leap as the EU announced the results of its Minutiae Template Interoperability Test (MTIT), the US MINEX testing program was extended and MINEX II initiated, and the results of the FRVT/ICE tests were reported. Look for this trend to continue as NIST has announced an upcoming Compact Iris Interoperability Test (CIIT) 2008.

'Qualified' or 'Approved' product lists also moved forward in 2007, the Personal Identity Verification (PIV)/FIPS 201 and Airport Access Control programs in particular.

Another area that saw a rise was in the area of biometrics at a distance and/or for moving targets, with no less than four different iris products in this category shown at BCC this year. Face and iris continue to show the most promise, but research continues in other modalities (and mixed modalities) as well. This is part of a larger trend related to improving the overall usability of biometrics – how to make them more intuitive and usable by real people in real operational environments.

As Service Oriented Architecture (SOA) based systems gain popularity, especially among the larger programs, so does the use of biometric middleware. This trend gained ground in 2007 and promises to continue in 2008 as end users and integrators seek openness, flexibility, scalability and specific technology/vendor independence. In fact, many of the programs mentioned above have selected such an architecture.

Standards work continues to press ahead but with more focus on conformance and conformity assessment. Additionally, a flurry of revision and amendment projects reflect feedback into the standards (improvements and corrections) based on usage. (Note the implication that at least some of the standards are moving from existence to adoption.) At ISO, several new standards were published in 2007 (e.g., vascular data format) and new projects initiated (e.g., for voice and DNA formats) that will move towards completion in 2008.

Privacy continues to be a concern in the development and deployment of biometric systems, both from a perception and political viewpoint, as well as in due diligence in designing adequate protections into the system as a whole – both technical and procedural. Ground can be gained in this area if sufficient attention is paid to it.

The role of biometrics in IT security and identity management has not yet settled itself out. Look for more work in this area and hopefully more dialogue between the biometric community and the greater security and identity worlds that have not yet fully embraced biometric technology.

The bottom line: biometrics had a reasonably good run this year, but still has significant untapped potential (especially in the commercial market). Perhaps 2008 will bring the epiphany we seek.

Newly approved FIPS 201 products

TRANSPARENT CARD READER

Cherry Smart Board G83-6644
Cherry Electrical Products
Cherry Smart Reader SR-4044
Cherry Electrical Products
Cherry Smart Terminal ST-1044U
Cherry Electrical Products
Cherry Smartboard G83-6744
Cherry Electrical Products
SafesITe PC Twin Smart Card Reader (GemPC Twin)
Gemalto
SWH Multi-Technology RM Reader w/Keypad & Display
Tyco International
SWH Multi-Technology RM Reader with Keypad
Tyco International
Paragon II Enhanced User Station/C
Raritan Americas Inc.
SafesITe Contactless Reader (GemProx-PU)
Gemalto
SafesITe PinPad Smart Card Reader (GemPC PinPad)
Gemalto
Dell Latitude D430, D630,D830 with o2 Micro Smart Card
Dell Inc.

ELECTROMAGNETICALLY OPAQUE SLEEVE

Credit Card Guard
JBM Envelope Company

FINGERPRINT CAPTURE STATION

Dactyscan84
Green Bit Americas Inc.

TEMPLATE GENERATOR

Aware XM
Aware Inc.

TEMPLATE MATCHER

Aware XM
Aware Inc.

SINGLE FINGERPRINT CAPTURE DEVICE

CSD200 single finger livescan capture device
Cogent Systems Inc.
HiScan
Biometrika srl
FS88 USB2.0 Single Fingerprint Scanner
Futronic Technology Co Ltd.

CRYPTOGRAPHIC MODULE

Luna CA4
SafeNet Inc.
Luna PCI Cryptographic Module V2.2
SafeNet Inc.
Luna PCI Cryptographic Module V2.2 (Signing/Backup)
SafeNet, Inc.
Luna PCM (Key Export with Cloning Mode)
SafeNet Inc.
Luna PCM (Key Export with SIM Mode)
SafeNet Inc.
Luna PCM (Signing Mode)
SafeNet Inc.
Luna PCM (Signing with Backup Mode)
SafeNet Inc.

VISIT FIPS201.COM TO RESEARCH AND COMPARE APPROVED PRODUCTS

INTRODUCING ...

FIPS 201.com

THE PREMIERE RESOURCE FOR COMPLIANT CREDENTIALING

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

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

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

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

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

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

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

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

Contact: **Angela Tweedie**
AVISIAN Marketing Coordinator
850-391-2273
angela@AVISIAN.com

AN AVISIAN ID TECHNOLOGY RESOURCE

NFC IN LONDON

NFC technology is sound, the interface is good, the partnerships have been formed, but …

WILL CONSUMERS USE IT?

Ryan Kline
Contributing Editor, AVISIAN Publications

The widely talked about London launch of contactless payment devices is only a little over half of a year in, but London is making news again with its Near Field Communications (NFC) trial. Started in November 2007, major players in the telecommunications, banking and transit markets have come together to test NFC payments in both transit and retail environments.

"If you want to make something happen, you have to work as a team. At this moment it is really important to interact with one another," says Gerhard W. Romen, head of NFC market development for Nokia. "This partnership is about making something happen, and that is what we are all committed to do and show here."

Romen says everyone comes to these trials with a goal of learning a few things and hopefully getting one step closer to commercially rolling out the standard-based NFC technology. ABI Research predicts that half of all mobile handsets will support NFC by 2010.

"It's not a revolution – it is really an evolution," says Romen.

The purpose of this NFC trial is really examining the customers' attitudes and opinions about the technology. This is not a trial to determine if the technology works, but to see if the customers want to use it. "We think the benefits will be for the customers," says Sue Doyle, the marketing director for Transys, the consortium in charge of the Oys-

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

London's NFC ecosystem:
A look at the players making it all happen

Transit operator

Transport for London (TfL)

Transport for London was created in 2000 as the integrated body responsible for London's transport system. The agency manages London's buses, the Underground, the Docklands Light Railway and the management of Croydon Tramlink and London River Services.

Transys

TranSys is a consortium of Cubic, EDS, Fujitsu and WS Atkins, which operates the Oyster card for Transport for London.

Mobile operator

O2

A leading mobile services provider in the UK, O2 has been a leader in NFC testing throughout much of Europe.

Phone Provider

Nokia

Nokia is a founding and active member of the NFC Forum. The device manufacturer wants to create an interoperable environment with other members of the NFC Forum, where the tags within smart objects and devices can communicate with each other using clearly defined and published interfaces and tag formats.

Tag Provider

Innovision Research & Technology

Innovision supplied all participants with a NFC tags for the trial.

ter card. "This should make their lives even easier than the Oyster card did." There have already been more than 10 million Oyster cards issued accounting for 38 million trips a week using Oyster. This makes up nearly 80% of all Underground and bus payments. Transys is also looking for new ways to deliver their product.

O2, the mobile phone service provider in the trial, also sees the benefits of NFC. "The aim of the trial is to test the widest possible uses for NFC technology on the mobile device," according to an O2 spokesperson. "Oyster cards are probably the most common and widely accepted use of contactless technology for consumers so it is essential it be included for this to be a comprehensive trial."

Most people agree that Near Field Communications has its advantages, and the most common one is simplicity. The deciding factor is not that the consumer decides to use NFC because it is cool, but they want to use it because it's convenient and simple. Behind the simplicity is technology. The difficult part is making sure the technology is so easy to use that the consumer doesn't even think about what exactly is happening in the phone.

"The real beauty of NFC lies in its role as an enabling technology that opens up various forms of communication and transaction in a very comfortable, user-friendly way," says Heikki Huomo, CTO at NFC tag manufacturer Innovision. "In the same way that people use a straightforward switch to light a room, or turn a handle to open a door, NFC allows people to use the simple act of touching or placing their device close to something to initiate the desired service. This makes using any form of electronic 'service' and other interactions more accessible to more people, whatever their age or ability.

An example of the simplicity brought by NFC is when two people want to exchange electronic business cards using a Bluetooth wireless connection between their mobile phones. With NFC, setting up the connection is simply a matter of touching their phones together. There's no need for the users to get their phones to scan the local area to locate and then identify the other's phone, no need to enter pass codes or other settings, and no risk that they establish a connection with the wrong device.

Financial Partners

Barclaycard

Barclaycard has 9.6 million retail customers and can be used to pay for goods and services in over 24 million outlets in more than 200 countries, and to withdraw cash from 600,000 cash machines and banks worldwide.

Visa Europe

Visa operates the world's largest retail electronic payments network and is one of the most recognized global financial services brands.

Another part of the simplicity is having a device that's easy to use. The phone used in the trial is the Nokia 6131 NFC, Romen says. "But the phone isn't a phone anymore," he says. "Suddenly it is a mini computer that some people still call a phone."

The phones enable users to securely view their balance over the air and also add extra security to the phone. For instance, some of the payment applications allow the users to add a security question or PIN to protect certain areas within the phone. The liability is the same as any other credit card with a maximum exposure of £200.

"The nice thing is that anything that is currently in a physical wallet – in a paper or plastic format – can be 'digital' on mobile phones with NFC," according to the O2 Spokesperson."

But what if the battery on a device goes dead? If the battery dies, the NFC technology can still be used for another 2 hours, according to the O2 spokesperson.

"You can turn the NFC functionality on and off," says Mr. Romen. "If your phone powers down, you can still use the functionality for payment. When the phone powers down, there is still some juice left in the battery. The payment takes that remaining energy, and when you touch the turnstile, it pulls from that and it works."

Single wire protocol yet?

The preferred standard single wire protocol (SWP), a specification calling for a single-wire connection between the SIM card and an NFC chip in a cell phone and established by the NFC Forum is not being used yet, according to the O2 Spokesperson. "These types of phones will be used for future phases of the trial," the spokesperson says. "We are using phones for the trial that store the applications on the handset itself rather than the SIM card. Once users validate that they are happy with these applications we will test with the preferred SIM architecture."

Following the London launch of contactless payments, this NFC trial may bring some interesting feedback that should help the possibility of NFC becoming commercially available. At the end of the six-month trial, there will be an evaluation, Doyle says, but the earliest anything more could happen with Transys and NFC would be 2009.

But the data in the technology's usability will be most important. One particular aspect is attempting to perfect the device's Graphical User Interface (GUI). Polishing the GUI on the phone for payments and making it easy to reload and check balances over the air may seem like small steps, but these small steps will in turn assist in overcoming large barriers, says Romen.

More information will become available after the trial has concluded in May 2008.

> "The nice thing is that anything that is currently in a physical wallet – in a paper or plastic format – can be 'digital' on mobile phones with NFC."

MAY 12-15,2008 ORLANDO, FL

Smart Card Alliance ANNUAL CONFERENCE @ ctst 2008 THE AMERICAS

Pre-conference Workshops

The Alliance will host a full-day educational session providing in-depth training to prepare attendees for the topics to be presented at CTST conference. Other industry organizations – GlobalPlatform and OATH – will also host pre-conference workshops.

Main Conference

The Alliance has developed a terrific lineup of speakers and education for CTST 2008, enabling you to personalize your experience from six distinct educational tracks.

Smart Card Alliance Networking Reception

Join Alliance members and industry leaders at the Alliance Networking Reception, open to both members and non-members (fees apply for non-members). Take advantage of this evening to build new contacts and renew old friendships while we celebrate the partnership between the Alliance and CTST 2008.

Smart Card Alliance Members Pavilion

Located at the CTST Exhibition Center, members and non-members can learn about the Alliance Industry Councils, web resources, on-line training, white papers and publications, and more.

Visit us online at: http://www.smartcardalliance.org/pages/activities-next-conference

Giesecke & Devrient: It's a family affair

Company takes pride in its 155-year history, as well as its bright future

Andy Williams
Contributing Editor, AVISIAN Publications

G&D prides itself on being the world's number two producer of smart cards. But G&D is about more than just smart cards. For one, its genealogy dates back to 1852 when two men first created the company. For another, it prints banknotes, a lot of them for a lot of countries throughout the world. And for many, like the Federal Reserve in the U.S., it delivers the systems used to count and sort those banknotes and to weed out counterfeits.

But probably the most unusual element about the 155-year old company with offices spread throughout the world is this: You won't find it on any stock exchange. It's privately held, owned by one woman who is a direct descendant of one of the company's founders.

G&D began June 1, 1852 when 21-year-old Hermann F. Giesecke (1831-1900) and Alphonse Devrient (1821-1878), then 31 came together to create Giesecke & Devrient.

According to the company's history, it started in Leipzig and within a short period, the partners had developed it into a leading money-maker – literally – thanks to some groundbreaking inventions in Guillochier, anti-counterfeiting, and printing technology.

One of the descendants of the Devrient family line was Jutta Devrient who married Siegfried Otto. G&D's current owner, Verena von Mitschke-Collande, is a daughter from this marriage. Coincidentally, it was Otto, a former Russian prisoner of war who was the son-in-law of the last G&D chairman, Ludwig Devrient, who brought G&D back from near oblivion after World War II. When it appeared the Soviets might be assuming control of the company, Otto moved the company from Leipzig to Munich and initially set it up in an attic.

Unlike the company's founders, Otto did not even have access to a printing press. But he displayed an incredible talent for improvisation. He and his employees first acquired the contracts and then obtained the equipment needed to fulfill them. Six months later, contracts in hand, "operations commenced in a building at Munich's Riem airport. It was here, with a total workforce of 28, that the foundations were laid for an international high-tech company."

Today, while G&D still prints banknotes and produces banknote-processing systems, it has branched out into many other industries – it has 53 subsidiaries and offices around the world – it refers to itself as an "international technology group."

By the end of 2006, the Munich-based company had roughly 8,300 employees, approximately 4,900 of them outside Germany with revenues totaling nearly 1.3 billion euros, about U.S.$1.9 billion. For comparison, G&D had 4,254 employees generating revenues of 676 million euros, $979 million, 10 years earlier.

A five-member management board, which includes chairman and CEO Karsten Ottenberg, run the company. Three of the board slots are filled by the men who operate each of the company's three business units: Michael Kuemmerle, Cards and Services; Hans Wolfgang Kunz, Government Solutions; and Walter Schlebusch, Banknote. The fifth is its CFO and director of labor relations, Peter Zattler.

"It's somewhat fascinating to have this family ownership over such a long period of time," commented Kuemmerle, whose Cards and Services unit includes payment cards, SIM cards and now, Near Field Communications.

While banknote printing and processing has been G&D's bread and butter over those 150-plus years – the company now prints banknotes for some 80 countries – when credit cards, or as Kuemmerle calls them, "plastic money," first made their wide-spread appearance in the 1970s, it only made sense for G&D to investigate it as a new source of business.

"As we are a printer of physical money, we looked at virtual money. The result was an upcoming market of interest to G&D," he says. "Basically we supply, as a global leader, the major banks worldwide. We're present in 53 countries, including the U.S."

One of the areas G&D was instrumental in developing was the Eurocheque Card in the late 1960s that was linked to a person's checking account. "If you wanted to write a check, you first had to show your Eurocheque Card," says Kuemmerle of this precursor to the debit card.

"It's still the brand uppermost in people's minds in Germany," he adds. "Even today, if you go into a retail store, the cashier might still ask if you want to pay with your EC Card. It's a real brand name that has been internalized in the population's mind. That's what we're still producing but it's being treated as a debit card."

Identity documents and more

Kunz's areas of oversight include ePassports and identity documents. His government solutions business unit covers both government ID cards and security solutions for those countries G&D services.

G&D is involved in numerous projects spanning the globe. "In Ontario, Canada we're producing health cards and driver licenses. We produce chip-based passports for Macedonia, a project including electronic passports, ID cards and driver licenses."

"Then," he adds, "we have other countries like Egypt where we're supplying 53 million secure national ID cards. We have set up a factory there for card production and personalization. In Taiwan, we were the first company to supply a health card with a chip. We've also supplied the Austrian and German health card systems with chip-based cards. In the transit area, we have customers around the world, for example the Washington D.C. Metro. And we are supplying contactless transit tickets for London and Beijing."

He adds: "In addition to this we provide consultancy for countries about security issues and public key infrastructures – for digital signatures – besides printing security documents, government checks, stock certificates and other certificates of important value that need to be very secure so they can't be altered."

One company, which Kunz oversees, is Secunet Security Networks, a German IT company in which G&D holds a majority stake. It has a primary role in many of these projects. "Secunet offers high level security systems, especially for governments including software with cryptographic technologies and secure networks," explained Kunz.

G&D also is actively looking at the driver licenses markets. "Right now, we're actively promoting our driver license products internationally," Kunz says.

The U.S. driver license market holds particular appeal to the company as states investigate new technologies, adds Steve Reber, CEO of G&D North America (GDAI), Dulles, Va.

G&D's North American office was established in 1990, initially to sell, produce, and support banknote-processing systems for its North American central bank customers. "We supply the high speed systems to the Federal Reserve that sorts banknotes that come in from banks, finds bills that need to be removed from circulation or to determine if any of the bills are counterfeit," says Reber. " These high-speed recognition systems can sort 40 notes a second, then strap the notes."

In the mid-1990s, G&D's U.S. division expanded to include cards and card systems. In 1997 the company acquired Cardtech, a card manufacturing company in Twinsburg, Ohio. Its offerings now include solutions for governments and government agencies, wireless operators, financial institutions, the health care industry, protected access, electronic identification and public key infrastructures. During this same period, GDAI began offering its banknote processing systems and solutions to the commercial banking, transit, armored carriers and casino markets to verifying deposits and count money.

In December 1999, GDAI opened its new 134,500 square foot production facility in Dulles. In 2006, GDAI and G&D Cardtech were merged to form Giesecke & Devrient America Inc., and is now one of the G&D Group's largest subsidiaries.

One market the company isn't going after is the U.S. government ID programs mandated by HSPD-12. "At the moment, we do not focus on the government ID programs" because of the ever changing regulations. "We decided to focus on other parts of the business – transit, payment cards, credit, debit, gift cards, driver licenses and telecommunication, providing SIM cards for GSM phones," says Reber.

In dollar terms, the U.S. company has been rapidly growing, he says. One of the company's bigger markets is transit cards, which are produced at the Twinsburg plant. "We're a leading supplier of contactless transit cards in the U.S.," he says. "That market has been growing, as more and more cities move in that direction."

Actively working with NFC

With Near Field Communications, a technology invented by Sony and NXP Semiconductors, slowly beginning to make itself heard, G&D has also positioned itself to be a major player in that field as well. It's a member of the NFC Forum, an organization designed to encourage the technology's deployment, and offers several products and services to the ecosystems, such as NFC-enabled SIM cards, secure flash cards to be used as a secure storage medium in handsets, and the development and installation of security-sensitive applications, for example mobile payment applications.

Key to that latter area is a joint venture G&D entered into with cell phone manufacturer Nokia. The company is called Venyon and its purpose is to develop and operate a secure service platform for the over the air (OTA) transmissions of applications, such as credit cards and transport tickets to consumers' NFC-compliant mobile devices.

Venyon is the company that will load security-sensitive NFC-applications, such as for mobile payment or ticketing, over the air securely, adds Kuemmerle. The reasoning behind this is simple. "We must make sure when we load a credit card applet onto an NFC cell phone, it actually ends up on your phone and that we can verify that it did. G&D is very well prepared for this because we're coming at it from a security technology prospective."

The Turkey project is a case in point. Mobile provider Turkcell and Garanti Bank have launched an NFC trial for mobile payments involving a contactless MasterCard PayPass credit card application stored on an NFC-enabled SIM card provided by G&D. Venyon is handling the secure uploading and administration of the payment function over the air.

"We are bullish about NFC. We're seeing a big market potential and we're always looking to be at the cutting edge," says Kuemmerle.

"NFC is the technology that merges identification, banking and transit applications in the mobile device," he adds. "These markets are converging. Our stakes in this market are very important assets, in that we are a trusted partner for secure downloads over the air and for providing a secure platform for sensitive NFC applications. In a nutshell, we're working on different architectures for this secure platform, whether SIM-based, embedded or removable. We are basically providing all the architectures to serve an emerging market."

Innovations help G&D continue to grow

With security at the forefront of G&D's worldwide business, it's not surprising that most of its major developments have been in this area.

"One very important innovation we developed is a laser protected image," says Kunz. Many photos produced today are done with inkjet printers or other technologies "which are easy to counterfeit. But the laser technology has a big advantage. The information is burned into multiple layers of the card. We can actually improve the security of a color photo on the card in such a way so we can see if someone has tried to alter a photo."

As he further explained, the laser-protected image combines the high security of laser technology with the optical advantages of color photos. The image is broken down into grey and color components. The color components are applied in a thermotransfer process on the card body, after which the grey scale components are adds in perfect register by laser. A counterfeiter can try to manipulate the colors, but not the laser-burned part of the image. "You could see immediately that someone has tried to alter the photo," says Kunz.

Another G&D innovation is the material used to produce cards, particularly identity cards. "Polycarbonate, which is used for many cards, is a reliable material but it's not very flexible," says Kunz. "G&D has now developed a unique material that combines the long life attributes of polycarbonate and the flexibility of PETG. By combining both materials the physical characteristics of the final card can be adjusted according to the specific requirements."

Another development from G&D is in the way antennas are applied on contactless cards. Normally the antenna is actually wired to the contactless chip, but G&D developed conductive ink that can serve as a printed antenna – which means it won't break – thus severing the connection with the chip. "We've industrialized this technique for cards and passports," says Kunz.

The retail area is another market G&D is exploring. "One of the newest things we're doing in banknote processing is getting into the retail market with cash handling equipment," adds GDAI's Reber. "This is equipment that would be in the cash room in a store."

He adds: "There is also a general movement towards self-service terminals for ordering and cash payments. We can extend this to restaurants." For example, a customer could go into a fast food establishment, choose his order from a kiosk and pay for it there. Similar systems, although not necessarily produced by GDAI, are already in use at a few college campuses.

While some – primarily contactless card makers – are pointing towards the day when cash may no longer be needed, the reality is that the amount of cash in circulation has actually been increasing "about 3% or 4% a year," says Reber. "Checks have been in decline also in the U.S., but I think when we get to the point where people start using their NFC phones, this could be an interesting payment method for small amounts" and could lead to a decline in cash usage.

Adds Kuemmerle: "We see definitely a dynamic and growing market here in payments, not only in transitioning from magnetic stripe to EMV, but especially for contactless and dual interface payment cards. And in the telecom area, there will continue to be a strong demand for SIM cards worldwide."

As to the NFC market, "there are a couple of hurdles that have to be overcome, such as the need to standardize the ecosystem to get the market started," he adds. "We expect the first significant move of the NFC market in 2008 and then a gradual growth over the years to come."

A flooded SIM market

One of the things SIM manufacturers have had to face over the past couple of years is the demand for low-cost SIMs from emerging markets such as China and India. "The dramatic price erosion for SIM cards seen in 2006 leveled off in 2007, but it is hard to predict what the future will bring," says Reber. "Anyway, G&D is carefully looking after its cost structure and therefore can offer suitable products for each market requirement at competitive prices."

"We believe you will always have a low-end market for SIM cards, but you need to develop a high-end one to give mobile operators more opportunities," says Kunz. In other words, he adds, in the future, manufacturers won't just be selling SIM cards, but offering value-added SIM-based services.

The future

"In the future the security of the SIM card will have an important role because mobile phone customers are going to use more and more applications beyond normal telephoning," says Kunz.

There will also be increased demand for secure identity cards. "We're going to have new national ID cards in Germany with a chip and this national ID card should not be composed of a lower technology than what's on our current electronic passport," he adds. "We already have developed the technologies required to participate in this market."

That sort of "can do" spirit, which began for G&D in those gloomy post-World War II days when Siegfried Otto first took firm hold of the company's reins, continues to this day. But one wonders if Otto would even recognize what he fought so hard to revitalize. Obviously that small 28-employee strong company has achieved a success that even he could not have imagined.

Security industry veteran Joe Grillo joins XceedID team

Contactless company to benefit from new board member's deep industry ties

Joe Grillo

In the spring of 2007, one of the most influential names in security shocked the industry when he announced that he was leaving the company that he had helped build. As the year came to a close, he resurfaced announcing that he would join the board of directors of a small, entrepreneurial competitor to his former employer.

Joe Grillo began his career at HID in 1993. He was instrumental in the company's growth and then managed its sale to security powerhouse ASSA ABLOY in 2000. Following the acquisition, he was named HID's CEO and would ultimately take the same role for ASSA ABLOY's Identification Technology Group, ITG.

Last year, Grillo announced that he would leave ITG. "It was totally my decision, it was time to do something different," he explains. "All the years I spent at HID and since the acquisition were fantastic nothing but great relationships."

For much of 2007, he enjoyed some quiet time and thought about next steps. "I took a lot of time off," he says, "looked at a couple of buyout opportunities in the other RFID space – not security or locks or cards and readers – but with tightening of debt markets the opportunities were not pursued."

Then a chance meeting at a trade show set in motion this new direction. He bumped into a former colleague from HID, John Menzel, who too had left the company to pursue other avenues. Menzel founded card reader manufacturer XccedID in 2003 and had been enjoying success as a nimble alternative to the larger manufacturers in the space.

What was the outcome of the meeting? Grillo became both an investor in XceedID and a key member of its board of directors.

The enthusiasm in Grillo's voice is palpable when he describes the new challenge. "The entrepreneurial smaller company was appealing," says Grillo. "Where we are brings back fond memories to the early days at HID. There is excitement, stress; every order is a big order. Taking on the industry, the world, the competitors."

He also is bullish on the company's technology and how it works with customers. "They are doing really good things on the technology side. We help clients move from low frequency, proximity technology with its relative lack of security, data rate speed, to a multifunction capability. Our XACTT™ technology is at the forefront of being able to move people to the next generation in a way that offers open architecture."

"We are incredibly excited to have him in our corner," stresses Menzel. "We did a pretty good job with some of the larger partners and resellers early on, but we have been focusing on adding additional value partners to the list. We are looking for Joe's expertise to expand that internationally."

Perhaps most importantly, Grillo has enormous respect and reach in the industry and brings a formidable ability to attract investors. Menzel concurs: "We have been profitable since early on, but to take it to the next level, we will need to raise investment. Joe can attract capital to do that. We have had several major industry players approach us about various forms of investment, but the time wasn't right."

"John has grown the company without overly leveraging the organization," adds Grillo. "We want to pick the right type of partners and investors."

When asked if he was there to help sell the company, Grillo says that there is always a right time to exit, "but my advice has been to keep on growing the business, and those things will work themselves out." He has actually suggested the company look at acquisition opportunities.

In the coming months, we will see the initial impacts of Grillo's involvement. He is serving as a non-operational board member and is an investor.

But he is doing other things as well. Foreshadowing an event to come, Grillo noted, "I fully expect to be taking on a full-time operational role in the future … in the non-security, non-lock RFID world. The XceedID effort is something to do in the extra hours I have each month." Indeed, he accepted the position of CEO for RFID company Digital Angel early in 2008.

Still, Menzel is clearly pleased to have his involvement. "He has skin in the game and he is in it to see it be successful. I feel like we have got the best available guy in the industry on our team now." ID

Three challenges to unlocking an NFC world

Manuel Albers
Director, Regional Marketing Americas, Identification, NXP Semiconductors

Near Field Communication (NFC) has been steadfastly moving towards mainstream since its inception in 2002. In the U.S., expect 2008 to be the year that NFC breaks out and changes the way consumers live, work and pay. Here's what to look for in the coming months …

When I talk about the NFC landscape, I am constantly asked what is the key trigger that will set off the chain of roll-outs we have all been expecting? I think that trigger has already been pulled, and in the next year or so the question for many operators is not if they will implement NFC solutions, but when. With the forming of Moversa, a new joint venture between Sony and NXP Semiconductors, another critical step in the chain toward the commercial availability of NFC has been linked.

As a company, Moversa will drive the global adoption of contactless smart card applications by producing chipsets supporting both Mifare and FeliCa, the two most widely implemented contactless technologies. This venture is expected to lead to simplified and lower-cost integration of mainstream contactless protocols into NFC phones.

As the use of contactless solutions in mobile payments and transport ticketing expands globally, consumers will be able to easily, quickly and securely access content and services via their mobile handsets.

But it takes more than a great technology solution to change the way consumers pay. What we have learned is that it takes a complex ecosystem of providers, handset makers, carriers, retailers, suppliers, public transport authorities, governments and a whole melee of parties to deliver the kind of simple and intuitive technology that consumers are seeking. That kind of change does not happen overnight, and it is far from simple. So what are the challenges ahead?

1. Market Fragmentation. Right now the market is fragmented and leveraging established contactless infrastructure choices in deploying NFC applications will be critical. In Asia and Europe, proliferation of the use of contactless technologies will be driven by transport. In the U.S., however, mobile payments will be the market driver, with 2008 being the year that the first commercial roll-outs of NFC are expected to hit. Universal standards and mandatory security evaluations for payment applications across different regions will shape handset architectures, trust provisioning infrastructure and roll-outs.

2. Market implications. Segmenting the pie and demonstrating the true ROI of NFC will lead to the need for carriers, banks and retailers to carefully examine where and how to implement NFC technology. Defining revenue streams from new applications – like buying a movie ticket through your mobile phone via an NFC-enabled poster – will be easy for consumers but requires that payment and ticketing be streamlined. Network operators already recognize that solutions such as NFC enable them to add greater value and added services to respond to decreasing voice sales and are eager to implement new revenue streams.

In conjunction with this, the movement in mobile banking will be symbiotic to the growth of mobile payments. Looking at market size, by 2010 close to 35 million U.S. consumers may use mobile banking features compared to 1.7 million in 2007 (Aite Group, 2007). We believe a good number of these transactions will be contactless. Jupiter Research estimates that worldwide payments by mobile phone may reach 22 billion USD by 2011 with a compound annual growth rate of 82% from 2007 onwards.

3. Ramping up to demand. ABI Research predicts NFC-enabled mobile phones will reach 292 million units in 2012, roughly 20% of handsets that will be sold that year. Based on the market size, rapid infrastructure implementation will be critical to executing the commercial roll-outs of NFC in the U.S. and overseas. Once initial roll-outs begin in the U.S., the implication is that NFC will act as a market driver in the smart card industry, enabling service providers such as mobile phone operators, transportation network operators and credit card companies to accelerate the roll-out of even more advanced contactless services to mobile phone users. In order to keep up with the market, mass adoption will require a well thought-out time-to-market approach for vendors.

So what are things to look for in the future from this technology? One is continued innovation and implementation of new applications to make use of this new technology, as developers begin to enrich the application space and come up with new and creative uses for NFC.

From a technology perspective, some interesting trends we see include the use of NFC in applications ranging from printers to digital photo frames to NFC-enabled grocery shopping, where products can be bought and paid for on-the-go. By simplifying the digital Bluetooth, Wi-Fi, and/or Wireless USB pairing, NFC will also complement companion products that have already been successfully implemented into the mass market. The possibilities here are endless.

Getting NFC into the hands of consumers has been a long journey but since its birth in 2002, strong partnerships have been built along with an entire ecosystem of members from handset makers to banks. The NFC Forum, since its inception, has grown to over 110 members, and represents strategic partnerships with the leading companies around the world. As the contactless infrastructure at POS continues to emerge in all regions – such as the MasterCard PayPass, Visa payWave, and Amex Blue – growing evidence indicates that the stage has been set for an NFC-enabled world, and that the trigger of inevitability will take its course.

Second generation ePassports pose unique challenges in 2008

Developing inspection infrastructures top priority to ensure security and viability

Mike Bond
Security Director, Cryptomathic

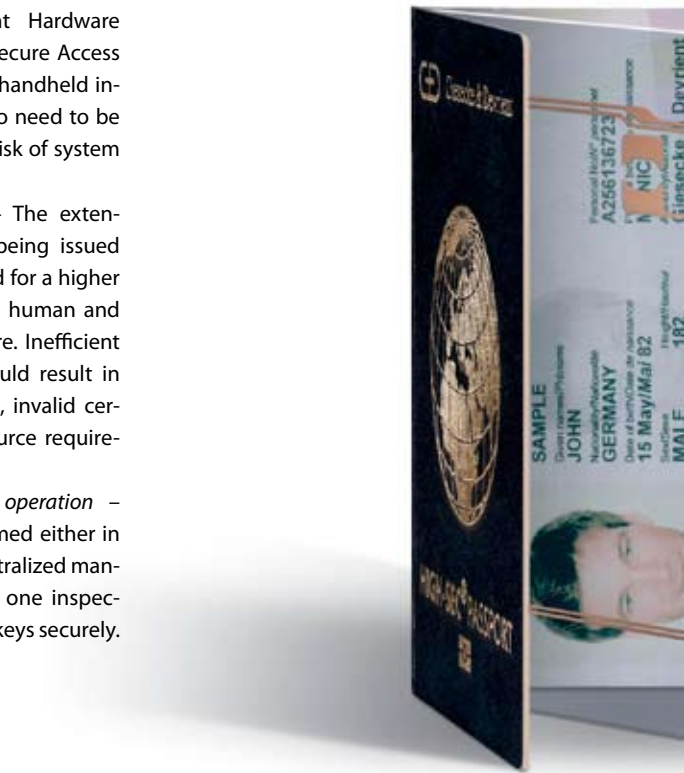
Throughout 2007, the global ID and security markets were heavily focused on developing the technology and systems to issue second generation ePassports with Extended Access Control (EAC). This has included new infrastructure for biometric acquisition and enrollment and new technology for security, cryptography and biometric data quality assurance. Since Germany became the first country to commence live issuance of EAC ePassports on Nov. 1 2007, the industry is preparing itself for a brand new challenge in 2008. Thoughts are now turning rapidly to the need to develop and deploy associated inspection infrastructures. This is a key industry priority for 2008.

Inspection systems will allow border control authorities across EU nations to view the electronic information available on EAC ePassports (for example a photo of the passport holder), acquire biometric data that is unique to the passport holder (such as a fingerprint), and cross reference the captured biometric data with a reference copy. Ultimately, the role of the inspection system is to facilitate the recognition of illegitimate documents by border control inspectors and to match travelers to travel documents, thus preventing passport fraud and deterring travel on counterfeit papers.

Introducing a flexible, scalable and interoperable infrastructure for inspecting second generation ePassports with EAC will not be without its challenges. Key issues to consider will include the following:

- *Interoperability* – Countries with reciprocal agreements have to be able to authorize each other to securely access the biometric information of native citizens. All EAC inspection systems must participate in an interoperable Public Key Infrastructure (PKI) for inspection, which must be refreshed on a daily basis to retain access to biometric data held in the EAC ePassport.
- *Flexibility* – The infrastructure has to operate efficiently in dynamic environments, e.g. busy airports or sea ports. This may impact the form of ePassport reader devices chosen and the supporting technology.
- *No best practice or benchmark* – There has been no other PKI initiative globally of a comparable size which can rival the EAC ePassport scheme for the sheer scale of cryptographic processing and infrastructure requirements. Decisions made will not have been 'tried and tested' before.
- *'Privilege to inspect' as opposed to 'right to inspect'* – Access to biometric data on the new EAC ePassports must be limited to only approved authorities or countries. A nation's infrastructure therefore has to be able to guarantee secure data exchange without interception from unauthorized parties, and has to be validated and audited by other countries, in order that it can be trusted with secret cryptographic keys that allow the extraction of biometrics from ePassports.
- *Document Verifier Certificate Authority* – An EAC ePassport chip authenticates an inspection system before allowing access to sensitive data. During this process, the inspection system sends certificates to the chip which validates the information. These certificates must be updated on a regular basis to ensure that an inspection system can continually access the biometric data held on EAC ePassports. Cryptographic keys must therefore be stored securely in tamper-resistant Hardware Security Modules (HSM) or Secure Access Modules (SAM) for portable, handheld inspection systems. Checks also need to be put in place to mitigate the risk of system theft.
- *High volume management* – The extensive volume of certificates being issued externally will result in a need for a higher level of management – both human and automated – than ever before. Inefficient software implementation could result in delays in certificate issuance, invalid certificates, and expensive resource requirements.
- *Centralized or decentralized operation* – Cryptography can be performed either in a central system or in a decentralized manner. In a centralized system, one inspection system server maintains keys securely. While this offers a cost-effective solution and has security advantages – it is easier to monitor and protect a central server – it raises concerns over the bulk storage of biometric data. In a decentralised system, each ePassport border lane or mobile reader device is able to separately maintain its own keys and certificates. While this is a more expensive option, it does offer flexibility and mobility of reader devices, which is essential in certain environments such as sea ports.

These key issues barely scratch the surface of the complexity and scale of the task ahead. What is easier to see, however, is the wealth of opportunities for eSecurity solution and hardware vendors who have the knowledge, ability and desire to help shape the EAC inspection infrastructure that has to be in place to help EU nations use EAC ePassports by June 28, 2009. Many nations have their procurement processes well underway, but comparatively few vendors have started to make announcements about specific technologies and solution components for EAC ePassport border control. The big movement towards the development of a second generation ePassport inspection infrastructure is likely to start in earnest as the industry heads into 2008.



New Extended Access Control scheme improves ePassport security

Eric Skinner
Chief Technology Officer, Entrust

The next 12 months will witness a remarkable change. Specifically, 2008 will see the emergence of new and more sophisticated electronic passports across the globe, particularly in European Union (EU) countries. New information technology is emerging to better protect and verify the personal information contained in these documents.

The use of ePassports to more accurately ensure and verify the identities of travelers has gained momentum across the globe in recent years, with more than 40 countries currently issuing some type of electronic passport. And for good reason.

Security concerns, developing technologies and emerging standards have prompted national governments to pursue the issuance of machine readable travel documents containing a chip that stores information that can be verified against the data on the passport, thereby improving border control.

To facilitate interoperability across countries, the International Civil Aviation Organization (ICAO) has set global standards for ePassports. Since the ePassport contains sensitive personal information, security and integrity are critical. Therefore, the use of digital certificates and a public key infrastructure (PKI) have become integral to securing and verifying this data. In 2008, countries will begin to implement a new standard for digital certificates providing this functionality in preparation for a new generation of ePassport.

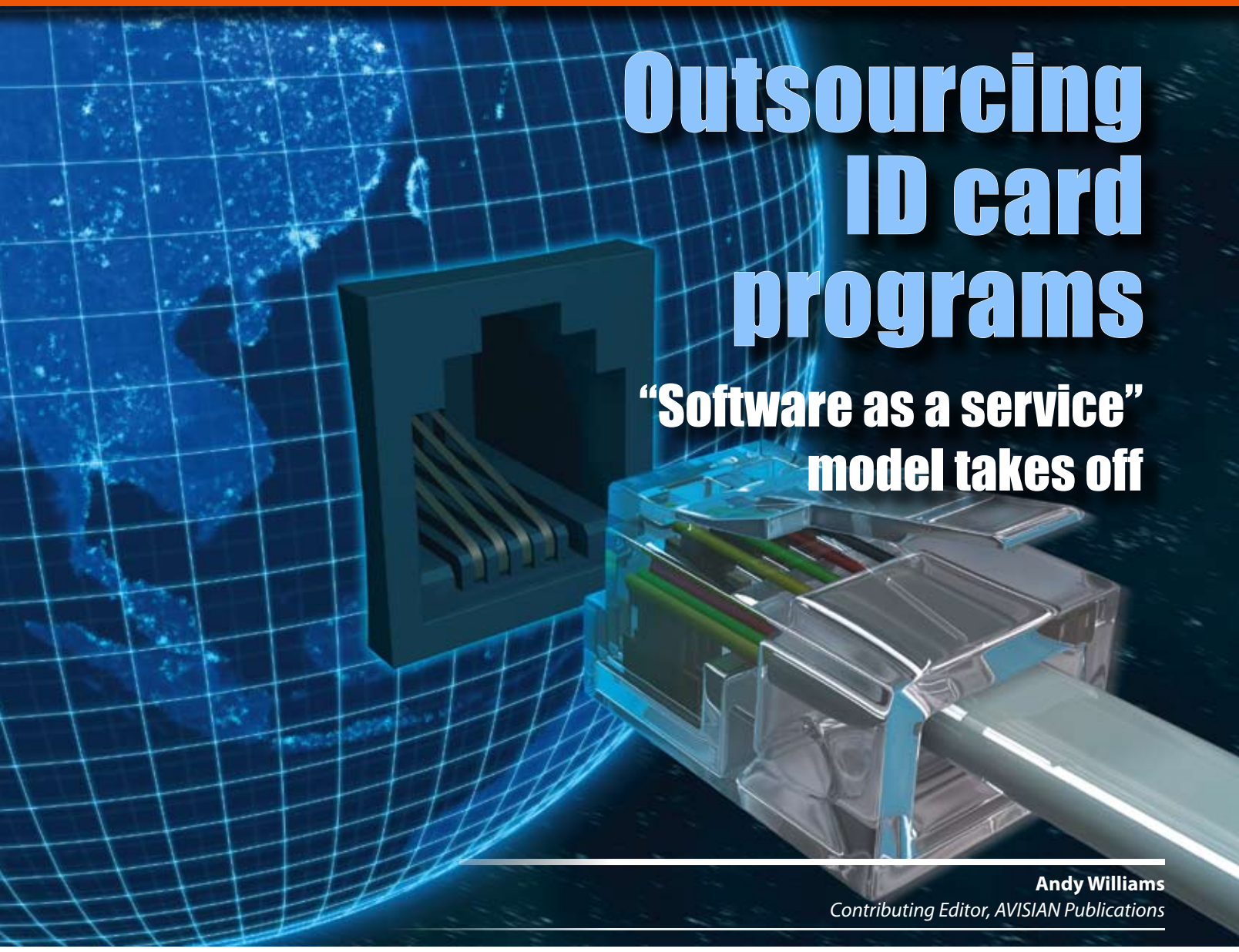
The initial generation of electronic passports in use today – throughout the EU and other countries – contain data protection under a scheme called Basic Access Control. In 2009, the EU countries will be required to add biometric data to the ePassport in the form of digital fingerprints. The strength of the security and verification around this data is evolving to protect this personal information through capabilities for Extended Access Control (EAC).

EAC is the process defined for ensuring that only authorized entities are able to access biometric data (such as an iris scan or fingerprint) stored on the contactless chip on an electronic passport. EAC also includes the authentication of a passport inspection station to the contactless chip, as well as the authorization of that inspection station to access the protected biometrics.

EAC provides a higher level of security during the verification process of ePassports. Not based on the X.509 standard, EAC will leverage a new type of certificate established by the ICAO known as a card verifiable (CV) certificate.

These next-generation passports will be required by all member EU nations by June 2009. The U.S. has yet to standardize on an EAC strategy.

While the remainder of the world has not yet established a timetable for implementing EAC, there is general agreement that the privacy of biometric data on electronic passports is critical. Broad adoption of measures such as those provided by EAC can be reasonably expected over time.



Outsourcing ID card programs

"Software as a service" model takes off

Andy Williams
Contributing Editor, AVISIAN Publications

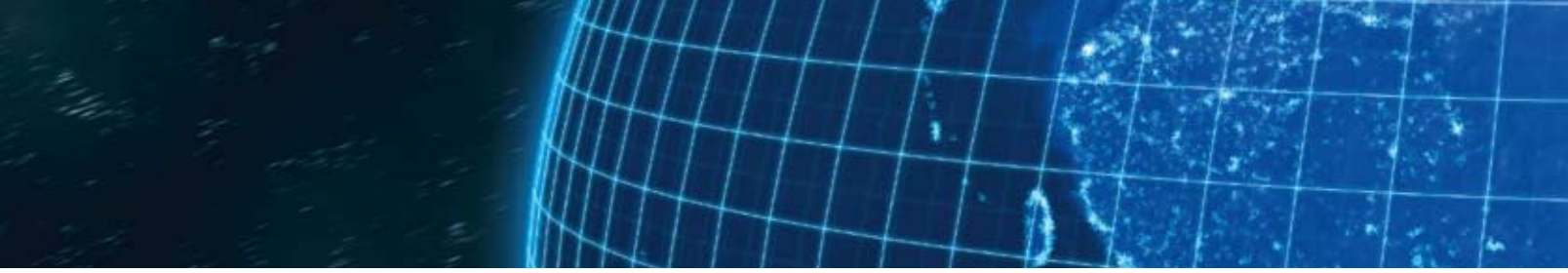
Colleges and universities aren't that different from corporations. Educational institutions are under the same pressure to keep costs down, and anything that can be done to help institutions save money piques their interest.

That's one of the big selling points of a relatively new concept called software as a service, or SaaS for short. Many may know it by its precursor: application service provider, or ASP.

But SaaS better defines what the service actually is: software, or systems built on that software that you don't actually own or maintain. It's basically rented. But it has many advantages over actually diving headfirst into a system that you must learn from the ground up and then manage. And what do you do when it's time to upgrade or, worse yet, some bugs surface that bring down your system?

Taran Lent, vice president of product development for campus card provider CardSmith says the company offers an alternative to the own and self-operate model. "We are a managed service provider, which is very different from selling software and leaving the rest to the client to figure out. We provide a web-based technology solution from a national processing center combined with outsourced management services."

For another campus card provider – Ireland-based SmartCentric Technologies International – SaaS fits perfectly into its ongoing philosophy



of reducing ownership costs, says the company's CEO, Kieran Timmins. SmartCentric introduced SaaS in the U.S. for the first time in the fall of 2007 at Loma Linda School of Dentistry in California. The company is in talks with two or three other schools as well.

"There are no up-front investments in terms of specialized hardware and in terms of maintenance and upgrades. That can all be managed at our secure facilities," says Timmins. "From our point of view, we're offering customers a more effective way to get involved."

"What does it really cost to deliver a service to your customers?" asks Lent. "You have to factor in software, hardware, staff, software license fees, maintenance, mandatory life cycle upgrades, etc. We think the total cost of ownership for self operation is pretty darn expensive for the college. With the SaaS model, we can deliver the same service or better at a 70% or greater savings."

CardSmith supports "everything from the operating system, software updates, and ongoing system administration," Lent says. "In the old model, schools needed to send three or four people off to system administrator school for one to two weeks. In our model we do all of the heavy lifting for the client. There are no servers or software that the school needs to deploy locally. The school just needs to plug card terminals into standard Internet jacks around campus and they are in business."

He adds: "There is no expensive hardware or software to buy, install and manage. And there is professional program management versus assembling and training a team to run the daily operations. And it's pretty hard to run a program with less than two people. Most quality card programs have three to five, which is a big annual budget line. With our service, we take a lot of the expenses associated with software and hardware off the table."

"This (SaaS model) is major for us," adds SmartCentric's Timmins. "The main selling point for SaaS, besides reducing cost of ownership is that it allows for an easy implementation."

This was evident with the company's deployment at Loma Linda. The school is a pre-doctoral, four-year institution with 400 students. It also has a dental hygiene program with more than 500 additional students.

California institution benefits from SaaS smart card solution

Loma Linda deployed SmartCentric's Password Wallet. Each faculty member is issued a smart card with a chip containing the user's profiles. These are the ones who have to authorize treatment plans or check off a student's work. "They simply feed the smart card into a card reader and enter a four-digit PIN," says Marina Moore, computer information system director at Loma Linda.

Password Wallet is an application SmartCentric launched in 2006 and is just one of many modules in its SmartCity Suite. "Password Wallet allows you to take any application that runs on a user environment," says Timmins. It captures all the necessary passwords required to access a system's various services. He says that before Password Wallet was installed, professors at Loma Linda often had to enter a password multiple times.

"When you insert the smart card, it retrieves the password from the card, and all you have to do is enter your PIN. If, for example, you have 10 applications you normally use, you'll be logged into all of them at once," says Timmins. "Loma Linda was looking for an application allowing them to simplify putting in a secure user ID and password."

"Our doctors – about 200 of them – love it," says Moore. "They're dentists and are very clinically oriented. The last thing they want to do is go to a computer and type something, such as their name and password, like they had to do in the past. And they had to do that for each level of treatment that needed authentication."

"One of the major reasons, the defining reason, that we went with SmartCentric was that it integrated very well with our patient management system." She adds the producer of their patient management software found SmartCentric for the college.

"It really is seamless," adds Timmins. "We could have installed this remotely, but Loma Linda was a new customer and we wanted people on site so if there was a problem we could handle it right away. We recently did an upgrade for them. We sent them an email that we were going to do it, and then later told them it was done. The only thing they noticed was that there was a slight difference on one of the screens."

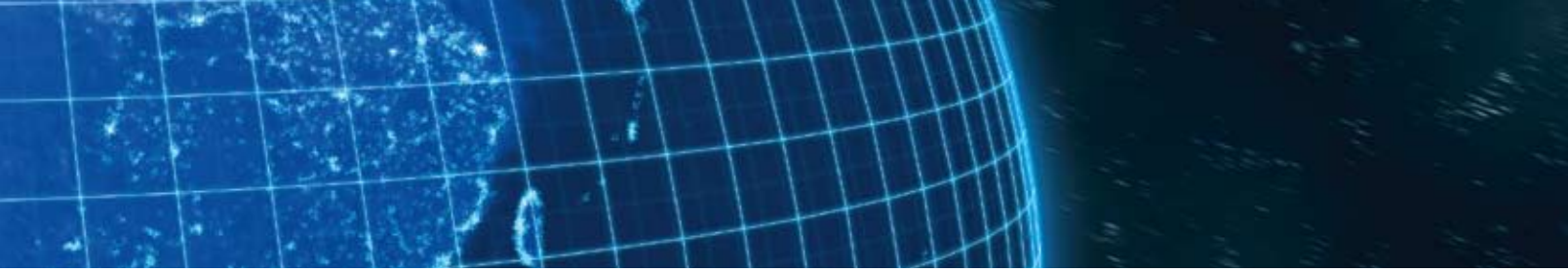
SaaS is advantageous for two reasons, says Timmins. "Obviously there's the cost savings. But it also encompasses all the necessary high security that's needed. That's the same security they would have received had they bought the entire SmartCity Suite. With SaaS you only have to pay for what you're using."

"We like the fact that we can scale up and use the card for other purposes, like for the cafeteria, and for copies," adds Moore. "Our first goal, though, was to just roll it out."

Timmins says SmartCentric is "talking to our clients worldwide about using SaaS for ePurse, logical access and other SmartCity applications. Every option we can offer as a traditional software install is now available through SaaS."

A higher level of service with SaaS

With an SaaS model, CardSmith's clients can also outsource key management functions such as customer care, program marketing, website



development, payment processing, merchant relations and daily operations, says Lent. "For example, we provide a live agent customer help desk, so if a student or parent needs support, they can call CardSmith ,and we'll provide that support on behalf of the schools. It's our phone that rings, not the school's," he adds.

"I used to manage the Dartmouth College campus card operation. Its office hours were 8 a.m. to 4 p.m. If you needed support, that's when you got it," says Lent. "With the SaaS model, you can offer professional level customer care to students and parents around the clock. We track call volumes and wait times and make sure all calls are answered within 30 seconds. This is a higher level of service than is possible if a school only has one or two customer care employees."

As with SmartCentric, CardSmith's clients can "pick and choose the services they need. It depends on the scope of the program and what kind of appetite the school has for self management. Some want to handle the marketing and care themselves so they're only outsourcing the technology while others outsource 100% of their program."

He adds: "Outsourcing services is a general trend in higher education. Schools outsource many services such as dining operations, vending, laundry and bookstore today to specialized third-party providers. Now schools have the option to outsource their campus card operations as well."

One downside, if it can be called that, is that since SaaS relies on Internet-communications, so if the Internet is unavailable, services can theoretically be impacted. "In reality, terminals can operate when the local network or Internet are down in a special offline mode," says Lent. "And if you think about it, most credit and debit card commerce in North America is processed over the Internet and phone lines every day, so the model is mature and well proven outside of higher education."

Software updates, as SmartCentric's Timmins pointed out, are also pretty seamless and easy using SaaS. "If we want to add a new feature, since we manage everything centrally, it's easy to perform a global software update," says Lent. "With other companies, if they have 800 customers, each behind a different firewall, they need to create a software patch and let their customers know it's available. Someone on campus then has to test it and roll it into production. Software release cycles in the traditional paradigm are a big and costly process to manage and are ultimately reflected in the price tag."

An ideal fit for small to mid-sized institutions and community colleges

Lent sees SaaS as ideal for the mid- to smaller-sized schools, or for those just getting started in the campus card area. "Most of the schools we talk with do not have resident staff resources with card program management experience," says Lent.

"We also see schools with IT departments that are stretched thin, are overworked and are on tight and shrinking budgets. The last thing they need is to be responsible for one more complex system. With us, because there is no local system, we are able to manage the infrastructure for them. All they need to do is to plug their terminals into the Internet."

Then there are the two-year institutions that have no, or very limited, card programs. "Now there is a way for community colleges to participate and to have a full-featured program," says Lent.

"What we see with community colleges and with private high schools is that they see the benefits of a cashless campus, but at what price?" asks Lent. "Usually up front costs are too great, and they don't have that kind of budget. Now that we've taken a lot of the complexity out of the service model, we're making it more available and affordable for smaller schools. In fact, we do business with several community colleges and private high schools already, and I believe there are many more that will follow in the years to come."

Lent says some schools "start really simple, maybe with just dining and the bookstore, then next year they'll add self service like laundry, vending and copying. If a school asks us to implement everything, we can deploy a school in about 12 weeks, including all applications. Our model lends itself to very rapid implementation cycles. We leverage the schools' existing campus network to transport transactions to our processing center. The school has the responsibility of issuing the cards since they are a security credential on campus in addition to being a financial device. Although there are a lot of moving parts, we have worked very hard to simplify things."

Timmins agrees that SaaS would be "an ideal solution particularly for smaller schools. It would be a good fit for them. We've done some research in talking to our customers around the globe. All the things we've seen suggest this is something folks would want. It takes away the need for a specialized staff and minimizes hardware requirements."

Lent will be the first to admit, though, that SaaS isn't for everybody. "For schools with big investments in traditional systems and existing staff, the economics to change may not exist, at least in the short term. But, with the increasing cost trajectory of software licensing and mandatory upgrade cycles that can cost $100,000 or more, some self operators may think twice, especially if their programs are not performing at optimal levels."

And of course, he stresses "for the schools that are still without a campus card program, the small and medium-sized schools, SaaS and program outsourcing is a wonderful new alternative to help them offer a high impact and professional service to their campus quickly and without all of the usual cost and administrative headaches."

Speed Customer Data Entry with IDWedge™

Automatically Fill Any Windows Form with Driver License Data

Enters in name, address, city, state, and zip code from driver license

2-3 minutes **vs** **2-3 seconds**

- Save 3 minutes per customer
- Minimize data entry errors
- Works with any existing Windows application
- Reads licenses from 49 states, Canada and Military IDs
- No software develpment required - simple 15 minute setup
- Helps detect fake IDs

Pays for itself in time savings and reduced data entry

TOKENWORKS®

IDWedge and TokenWorks are Trademarks of TokenWorks Inc.

Hotel Registration • Casino VIP Cards • Credit Card Applications • Hospitals • Health Clubs

FOR MORE INFORMATION:800-574-5034 /www.idscanner.com / sales@tokenworks.com

Loosening of credit card rules opens door for instant issuance of Visa & MasterCards on campus

Issuing combined student IDs and bank cards on campus reduces the time it takes to get these multifunction cards into students' hands, and it enables them to begin using the card the moment they exit the campus card office. But if that card was a branded Visa or MasterCard product, this hasn't been possible for most issuers.

Visa and MasterCard rules made it all but impossible to issue branded products from a campus card office or bank branch. The rules were put in place to curb fraud and counterfeiting and they did so by requiring that cards be produced only in secure, approved facilities. A campus ID could be a Visa or MasterCard product, but it would have to be produced offsite at a secure printing facility.

This presented a major challenge to campuses. The student ID card is needed immediately for dining, access, library and privilege control – so it was not practical to tell a student that they would receive their card by mail in the coming weeks.

Adding to the challenge, the rules also required that the cards be embossed. Embossing of the numbers and name are a legacy requirement from the days of the manual "zip zap" machines used by merchants prior to electronic point of sale devices. Even after the new POS devices became mainstream, some small merchants continued to use the manual technology and others relied on the embossed characters when the POS was down. Though the technology to create embossed cards is available in desktop machines, it is not a common item in campus card offices.

So, most campuses opted to instantly issue a non-branded product that works as a debit card but in the more limited ATM networks or with merchants specifically signed by the bank partner.

Such was the tale of instant issuance. But as Bob Dylan says: the times, they are a-changin.'

MasterCard and Visa have loosened some of these rules and opened up the ability to produce cards onsite. The rules outlining secure facilities have become less stringent, making it possible for cards to be issued at bank branches and other locations that have reasonable security and good inventory controls. The associations are also considering doing away with the embossing requirement.

So how would instant issuance work in a campus card environment? In most cases, the campus' bank partner would receive a supply of blank card stock with the Visa or MasterCard brand already imprinted. These cards would then be run through the card printer in the bank branch on campus.

Printer manufacturers rise to the occasion

Seeking to support this emerging opportunity for instant issuance, HID-owned Fargo Electronics developed a new card printer geared primarily for the banking, credit union and retail industries. But it's a printer that can just as easily be installed in a university campus card center, says Steve Blake, HID Global's director of business development.

ISC WEST | APRIL 2-4, 2008 | SANDS EXPO AND CONVENTION CENTER | LAS VEGAS, NV

Meet the latest and most challenging demands on security at the event that industry professionals rate as the best, ISC West.* ISC West puts you face-to-face with new technologies and upgrades, networking opportunities and education. ISC West helps you perform your best with over 950 providers of security products and services. Experience the breakthrough solutions behind Urban Security and Smart Home in two key feature areas. Plus, feel secure knowing relevant topics from design/installation to incident management at top-notch ISC Education.

ISC WEST
INTERNATIONAL SECURITY CONFERENCE & EXPOSITION

Reserve your place at the center of the security universe.

REGISTER TODAY AT:
www.iscwest.com/Avisian

SPONSORED BY: SIA | PRODUCED BY: Reed Exhibitions | ENDORSED BY: CAA | CORPORATE PARTNERS: ASSA ABLOY, AXIS COMMUNICATIONS, DSC, HID, Honeywell, SAMSUNG ELECTRONICS, gvi | ISC EDUCATION PARTNER: PELCO

** based on 2007 post-show research*

Welcome to the center of the security universe.

Security professionals rate ISC West the #1 security event in the country.

Code: AD45

In one printer, a campus can produce a card that is both the student ID and the Visa or MasterCard branded debit card.

"Many campuses that have bank card relationships offer students a variety of financial services during the registration or orientation process," he says. "But issuance of a branded debit card is different from issuance of an ID card."

However, more banks and credit unions are doing instant issuance at their branches, he adds. "Customers can apply for a debit card and get it immediately. What we have is a bank card printer based upon the HDP5000 platform, which utilizes reverse transfer printing to produce a card that has brilliant and true high definition colors, similar to the pre-printing process," says Blake. Called the Fargo HDPii – for instant issuance – the new printer will eliminate the need to preprint batches of cards since that can all be accomplished onsite.

The printer was launched earlier this year following a large pilot at TD Banknorth. That trial involved "46 of our printers. We're anticipating roll-outs in the U.S. and then Canada," says Blake. The printer will produce a flat card as opposed to the traditional embossed debit card with raised letters. "It can be customized at the branch, starting with a blank white card," he adds.

While no branch bank on a college campus is using HDPii right now, "our next step is to approach banks and colleges that have campus card programs. They can kill two birds with one stone: do student issuance and a branded debit card all in one step. From the bank side, it's a tremendous opportunity. If you can get cards into the users' hands faster, they'll start using them sooner."

Blake says the industry term for this is "shift and lift." The shift part comes in moving the initial transaction up sooner. "If a card is sent in the mail, you might get it anywhere from five days to two weeks after application. If you're instantly issued a card, you can use it right away." The lift part describes the activation, or non-activation of the card itself. "When a debit card is ordered, probably 40% of the time it won't be activated," he adds.

The printer will produce debit, credit, gift and prepaid cards. Fargo is seeking Visa and MasterCard certification, with initial focus on debit cards. He says several banks "have approached us and our software partners about moving forward with major pilots involving instant issuance. Many of these already have great relationships with schools."

Prices start at $6,995 for the HDPii with magnetic stripe encoding, dual-sided printing as well as the physical and data security additions to meet Visa and MasterCard regulations. There is also an optional dual contact and contactless smart card encoder. "Reaction to the HDPii has been fantastic," he says. "Customers are delighted because they're getting a card immediately." It's instant gratification in the purest sense. Banks also like the idea of this shift and lift. They'll generate more revenue, and that's resonating extremely well."

He also believes colleges will like this new breed of printer. "They're always looking for ways to better take care of students and the instant issuance of a branded debit card will further separate that college from another.

To emboss, or not to emboss

Datacard Group is also involved in instant issuance of MasterCard/Visa-approved cards.

Mark Andersen, head of Desktop Product and Industry Marketing for Datacard Group, says the company has several varieties of instant issuance solutions. "We offer technology options for personalizing embossed, indented and flat credit/debit/prepaid cards. The Datacard150i desktop card personalization system embosses and indents preprinted credit/debit/prepaid cards. The new Datacard FP65 financial card printer personalizes flat debit cards or pre-embossed cards via direct-to-card printing technology. And the Datacard RP90 Plus card printer also personalizes flat cards via retransfer printing technology."

The Datacard 150i system is MasterCard- and Visa-certified to personalize credit/debit/prepaid cards, he adds. Still, he says, the instant issuance market has primarily involved embossed and indented cards. "There is a trend toward issuing flat debit cards, though MasterCard and Visa credit cards are generally still requiring embossing and/or indenting. Many believe the additional security provided by indenting will remain a requirement of branch issuance card programs (even if the embossing goes away)."

In the 2007 Banking Survey conducted by *CR80News,* instant issuance was mentioned as something more and more banks are considering. U.S. Bank has is instantly issuing a Visa-branded ID card at the University of Wisconsin Eau Claire, says Whitney Bright, vice president, campus banking.

And, Wachovia reports that colleges and universities continue to express interest in Wachovia's Visa Check instant issuance program in association with its ID Cards, says William Caldwell, assistant vice president, campus card relationship manager for Wachovia. "Many of these programs want the benefits of a card with added flexibility for its cardholders which handles their financial needs, not only on campus, but anywhere Visa is accepted," Caldwell adds.

The key to instant issuance is in the solution, more than in the printer

According to many in the card printer industry, the technology to produce branded financial cards is virtually no different than the normal card printer sitting in your office. It is the processes surrounding the storage, management and issuance of the cards and the software that link the financial issuance systems to the card production system that are different.

Kathryn Lodato, director of Americas marketing and worldwide marketing services for Zebra Card Printer Solutions, says its products can print "on-demand cards that are encoded to act as MasterCard, Visa or debit cards." But that involves cards that already have the financial information encoded. If the card isn't embossed, a Zebra printer can produce "on-demand cards that can be personalized," she adds.

"Zebra Card is working with some of our reseller partners to offer solutions for banks for instant issuance of personalized payment cards," she says. "This is software dependent and the Zebra Card reseller partners are the providers of the total solution."

Andy Matko, team leader of Magicard, says some of its printers "could issue MasterCard/Visa branded credit/debit cards, but they are not at this stage MasterCard/Visa certified."

"In most campuses it's a closed system – their own financial system – but that's increasingly becoming more public. Creating financial bank cards can be done. It's just choosing the right encoder or software to do that. We don't make the badging or financial software, but we work with other companies to do so," Matko adds.

Evolis recently "closed one of the largest projects for instant issuance for debit cards in Korea," says the company's managing director, Geraldo Talavera. "We sold 10,000 printers to multiple banks."

"What Visa and MasterCard certify is the process the bank implements … but those will change from country to country (and bank to bank)," adds Talavera. "What Visa and MasterCard care for is that the process is secure and compatible with the infrastructure."

Evolis is also involved in instant issuance projects with banks in Latin America and Asia in their attempts to reduce fraud. "The cost they save to mail the card pays for the printer," he says. "I think in the U.S., we'll get to this."

His system would work at universities, but the bank would have to pre-encode the cards. "Once it gets to the university, it would finish encoding the card," he adds. "In most cases, our printers don't have to be certified for printing or encoding because the vital information will come pre-encoded from the bank itself."

Rob Miskelly, business manager for Team NiSCA, the U.S. business unit of Kanematsu based in Japan, concurs noting "management of the cards and the printers is on the bank side. Printer manufacturers are hardware vendors."

Understanding RFID Part 5: RF Characteristics

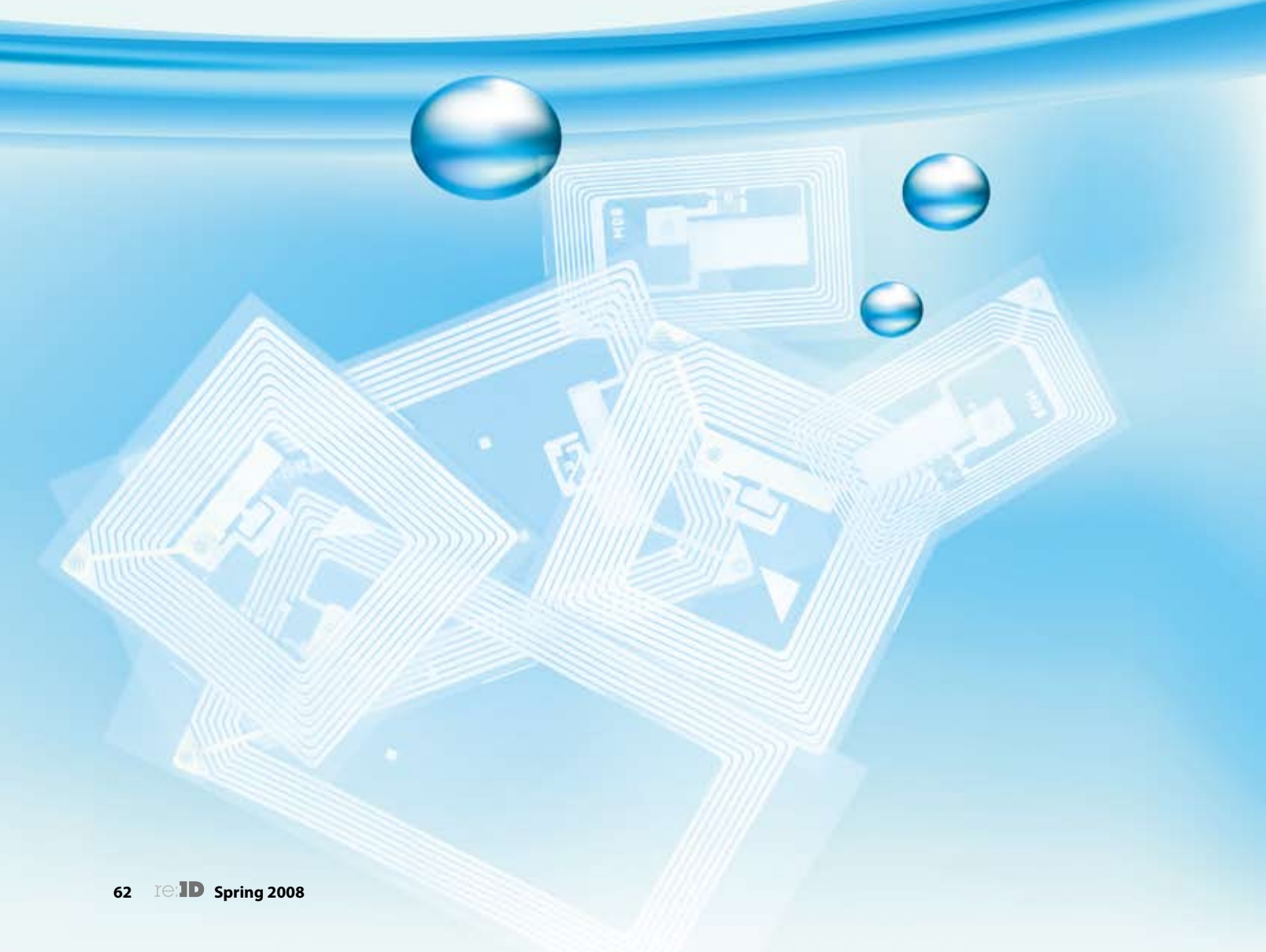
Jerry Banks and Les G. Thompson
Co-authors of RFID Applied

Under ideal conditions, the popular Squiggle RFID tag from Alien Technology can be read at a distance of approximately 20 meters. But what happens if it is placed behind a glass of water? What about placing it to the side, but adjacent to the glass of water? How about placing it in the water?

Answers to these and other questions will appear later, but suffice it to say that the readability of a tag is impacted by the placement of the tag and its ambient environment.

When we discuss passive RFID tags with an audience of people that have never seen a tag, we say first that reading the tags is impacted by the release of radio frequency waves in the ambient environment. We ask for examples of ambient environmental factors in the room in which we are making the presentation. Any ideas?

Here is a hint: Typically, we are making a presentation using PowerPoint. So, there is a computer and a projection device involved. Both of those emit radio frequencies.



2,500 of your partners (and competitors) from the advanced payments industry will be meeting in Orlando in May.

Will You Be There?

ctst 2008
THE AMERICAS
Smart Card Alliance

MAY 12-15, 2008

ORANGE COUNTY CONVENTION CENTER
ORLANDO, FLORIDA

SIX NEW TRACKS ON:

- Identification and Policy
- Payments and Applications
- Mobile and NFC
- Security and Access Control
- Emerging Technology and Innovations
- Latin America

KEYNOTE SPEAKER:

David Pogue
New York Times
Technology Columnist and Emmy Winning
CBS News Correspondent

AVISIAN

OFFICIAL EVENT VIDEO SPONSOR

To sponsor or exhibit contact Chris Frey at christopher.frey@sourcemedia.com or 212-803-6568.

MORE CONTENT. MORE NETWORKING. MORE VALUE.

Download the agenda at www.ctst.com

Table 1. Frequency Classifications

Designation	Frequency	Wavelength
ELF – Extremely low frequency	3 Hz to 29 Hz	100,000 km to 10,000 km
SLF – Super low frequency	30 Hz to 299 Hz	10,000 km to 1000 km
ULF – Ultra low frequency	300 Hz to 2999 Hz	1000 km to 100 km
VLF – Very low frequency	3 kHz to 29 kHz	100 km to 10 km
LF – Low frequency	30 kHz to 299 kHz	10 km to 1 km
MF – Medium frequency	300 kHz to 2999 kHz	1 km to 100 m
HF – High frequency	3 MHz to 29 MHz	100 m to 10 m
VHF – Very high frequency	30 MHz to 299 MHz	10 m to 1 m
UHF – Ultra high frequency	300 MHz to 2999 MHz	1 m to 10 cm
SHF – Super high frequency	3 GHz to 29 GHz	10 cm to 1 cm
EHF – Extremely high frequency	30 GHz to 299 GHz	1 cm to 1 mm

Source: Banks & Thompson for AVISIAN Publications

How about the cell phones in every attendee's possession? What about the lights and the dimmer switches? Even in an innocuous place like an auditorium, there are ambient sources of radio frequency that interfere with the very weak signal that a passive RFID tag can generate.

So far, you have some speculation that moisture has an impact on the Alien Squiggle tag. And, you have been told that ambient sources of radio frequency waves impact RFID tags, particularly passive tags that don't have a power source.

We aren't selling the Alien Squiggle tag. But, why are there so many different RFID tag designs? For that, we turn to the subject of frequencies.

For convenience sake, the entire RF spectrum has been segregated into bands of frequencies that tend to share common characteristics. *Table 1* describes these classifications. You should notice that as the frequency of the wave increases, the length of the wave decreases.

In the previous article, "The black art of RFID antennas," we discussed how to construct a tag based on a target communication frequency, but we did not discuss why a company like Texas Instruments or Alien Technologies would create a suite of tag products, each tag targeting a different frequency. The simple answer is that radio waves at different frequencies interact with their environment differently.

Imagine that you are standing in a large open room. If you were to sing a variety of notes, you might eventually sing a note that seems to fill the room with sound much more than the other notes. The note that you found is produced by a sound wave that has the appropriate wavelength to resonate perfectly in the room. This is why most people think that they can sing better in the shower.

If you were to change the environment, the note required to produce a resonating sound would change. For instance, if a wood table was placed in the room, the note that resonated before may not resonate like it once did. Another note may be found that resonates in the room better than the previous note. Sound waves are analogous to radio waves in this respect.

In the world of RFID, the wood table in the previous example may be analogous to another type of material such as paper, water, metal or cloth that can change the environment. Upon further examination, the previous example is more complex than it seems. Why did the resonant frequency change when the table was placed in the room? The answer is that the table impeded the propagation of the sound waves. There are hundreds of factors that could influence why the wave was impeded, but the two most common are that 1) the sound wave was absorbed by the table, or 2) the sound wave was reflected by the table which disturbed the other waves that were bouncing around the room. Like waves on a pond, sound and radio waves can cancel each other if they collide.

The two most common environmental conditions on the minds of RFID practitioners are water and metals such as iron, lead and aluminum. The pharmaceutical industry is worried about water because many drugs contain some type of moisture. The manufacturing industry is concerned with metal because assembly lines are usually made of metal, and the products also may be made of or contain metal.

Why is water such a problem for RFID tags? The truth is that water is not a problem as long as the correct frequency is chosen. Microwave ovens are tuned to the resonant frequency of water so that they can absorb the energy from the radio waves and heat up our food. The oven produces radio waves at the 2.45 GHz frequency (microwaves). These waves have a wavelength of 12.24 cm. As the waves pass through the water in the food, the water molecules rotate to align themselves with the wave. The molecules rotate with each wavelength. This oscillation causes the increase in temperature.

The structure of water molecules is perfect for interacting with this frequency. Other wavelengths would not cause the water molecules to rotate. For RFID, the absorption of energy has a negative consequence unless it is being primarily collected by the antenna attached to an RFID tag.

The microwave example illustrates why choosing a frequency in one of the higher bands such as UHF or SHF would not be a good choice for applications of RFID near water where HF bands work better. The trade-off with employing a lower frequency is that there is a decrease in the data transmission speed between the reader and tag as the frequency decreases.

HF RFID tags are most often used in close proximity to water. These types of tags have coil type antennas, which are designed to work best at lower frequencies.

Some RFID tag manufacturers, like IPico, have created dual-frequency tags to combat these issues. As the name implies, dual-frequency tags transmit at two different frequencies. These types of tags can achieve higher transmission rates when communication is possible at a higher frequency, yet the tag can always

be read, even when placed in a glass of water because it can transmit at a lower frequency. These tags are more robust and more expensive.

Experimenting with RF tags and water

With this knowledge we can answer the questions posed at the beginning of this article. The Alien 9540 Squiggle tag adheres to the EPC Gen 2 standards and communicates at a frequency of 915 MHz. From what we have learned about the effects of water on radio waves in the UHF band, we can deduce that the water will attenuate the signal and energy.

The electromagnetic field required by the tag will weaken as the tag is moved closer to the water until the tag will no longer operate unless the reader is extremely close to the tag. The exact effect cannot be determined with respect to the reduction in read range for a tag when measured outside of a controlled environment such as a laboratory.

It is certain, however, that if a tag is placed in the water there will be a significant reduction in its read range. Now, what if a tag worked at the lower frequency of 13.56 MHz in the HF spectrum? We can predict that the tag will operate better than the UHF tag, but a tag that operates at 125 kHz could be read at a much further distance if it were submerged fully in the water.

At our request, the Electro-Optical Systems Laboratory at the Georgia Tech Research Institute conducted an experiment using the Alien 9540 Squiggle tag. As shown in Table 2, their tests demonstrated that the tag is affected by water, as we would expect.

Table 2. GTRI Test Results Using the ALN-9540 RFID Tag

Test	Placement of the Tag	Maximum Read Distance
1	Without the presence of water	19.4 m
2	Next to a glass of water	7.1 m
3	Behind a glass of water	6.9 m
4	In a glass of water	0.29 m

Source: Banks & Thompson for AVISIAN Publications

The impacts of metal on RFID

Some types of metal also influence a radio wave. There are many elements on the periodic table that are classified as metals. Most of them are not used on a day-to-day basis. This discussion will pertain to the more common metals that an RFID tag may come in contact with such as iron, aluminum, and copper. Ferrous metals, such as iron are often regarded as having the worst effect on electromagnetic radiation because they are, for the most part, magnetic. Non-ferrous metals, like aluminum and copper, are not magnetic and interact better with electromagnetic radiation. Not all ferrous metals are magnetic and vice versa.

Metal (the kinds mentioned above this qualification won't be repeated every time we say the word "metal") can affect radio waves in several different ways. First, radio waves cannot penetrate these metals. If RF waves cannot penetrate a metal, the metal is said to be opaque to radio waves. It is interesting that these metals do not need to be solid to completely stop a radio wave.

RF engineers work in sterile environments known as Faraday cages. The Faraday cage has walls made of highly conductive metal mesh or screen that have holes smaller than the RF wavelength being tested. If the holes are small enough and the metal is thick enough, all radio waves will be absorbed and distributed along the surface of the screen.

Metal can detune a radio wave. Detuning occurs when the amplitude and/or wavelength of the wave is skewed if the wave comes in contact with the metal. Once the wave is detuned, it cannot couple with the RFID tag. In addition to detuning, the RFID waves form miniature RF eddies where they intersect the metal. These eddies effectively cancel out the wave such that it either dissipates completely or the wave is impeded to the point that it cannot couple with the tag.

Metal may also absorb some of the radio wave. This is known as parasitic capacitance. Just like water, the metal diminishes the strength of the radio wave by absorbing some of its energy. In active RFID systems, where energy is abundant, the metal can become a conduit for the RF energy. It is not uncommon for a gas or water pipe to channel a radio wave down a hall into another room or to another floor of the building. These types of occurrences can be very challenging for active tag real-time location systems because active tags transmit with so much more energy (wattage) than passive tags do. Any metal objects such as pipes or handrails can become secondary antennas for the active tag's transmissions.

Understanding the characteristics of RF can aid in the successful planning and implementation of an RFID solution. The basic physical principles of RF are a necessary tool in the RFID practitioner's tool belt. It is important to remember that real world environments are much different than RF labs. Passive RFID systems are much more susceptible to harsh RF environments than active RFID systems. Even so, dynamic environments can cause even the most robust RFID systems to stumble unless they are designed correctly.

About this article

We would like to thank Gisele Bennett and her group of researchers at the Electro-Optical Systems Laboratory at the Georgia Tech Research Institute for conducting the water readability tests referenced above.

This article is the fifth in an ongoing series that explains the principles of RFID. It was created for *RFIDNews* by Jerry Banks, Tecnológico de Monterrey, Monterrey, Mexico and Les G. Thompson, Lost Recovery Network Inc., Atlanta, Georgia. The authors are two of four co-authors of *RFID Applied*, John Wiley, 2007, ISBN-10 0471793655; ISBN-13 978-041793656.

Protecting an endangered species with RFID

Tags help track the well being of manatees at a Puerto Rico research center

How do you take the temperature of a 500-pound sea cow? St. Paul, Minn.-based Destron Fearing Corp. has the answer.

If you thought taking a squirming child's temperature was difficult, consider what researchers must go through to get a temperature reading on a 10-foot-long, 500-pound manatee that lives in the water. Fortunately for the manatees and the researchers, technology developed by a company associated with the livestock industry, Destron Fearing, has attempted to make the job much easier.

Microchips, similar to those already being used in horses, llamas and alpacas have provided a better solution to managing the health of these mammals at the Puerto Rico Manatee Center. Although their origins go back 45 million years, manatees – or sea cows – are edging closer to extinction. In an effort to preserve them for generations to come, the folks at the Manatee Center are doing their most to protect these gentle, plant-eating mammals. Between 1990 and 2006, the center has rescued and cared for 26 manatees, mostly calves that were orphaned or separated from their mothers.

According to Dr. Tony Mignucci, center director, one of the challenges his staff faces in bringing the manatees back to health is finding a way to get accurate temperature readings. Because manatees have large molars, they chew up anything put in their mouths, so getting an oral reading isn't practical. Of course, you could always "go south" to get a temperature reading, but that has its challenges as well.

"We wrote to Destron Fearing and they kindly donated microchips and two Pocket Reader scanners for us to test," says Dr. Mignucci. "We microchipped all the animals we had and then started taking temperatures and recording how they were doing. Now we take readings every day."

A manatee has the chip implanted when it is still a calf and easy to handle. Each time it comes to the surface or is bottle fed, a staff member scans the Pocket Reader over the back of the manatee's neck to get a reading. The manatee doesn't feel a thing and the staff members don't have to perform any pro wrestling moves. The technology alleviates the stress for everyone involved, most importantly for the manatee.

Taking temperature readings is one component of the overall health assessment of each animal with the ultimate objective of releasing the animal back into the wild. The procedure includes weaning the animals from milk to an herbivorous diet one year before their release. Three months before the big day arrives, there is a progressive acclimation to salt water. From there, the manatees are released into a sea pen with sea grasses to eat to help them become accustomed to living on their own. Following their release from the sea pen, the manatees are then monitored for one year via radio tracking.

Being able to understand and foster these great mammals is essential to their preservation. Currently, there may be as few as 2,500 manatees left in the United States. And with a slow reproductive rate – mothers only have one calf every two to five years – it is critical to do all that can be done to protect these gentle creatures of the sea.

Source: Ad Farm

PIVMAN

Handheld device
by DAP Technologies
www.daptech.com

Is he legit? Are you sure?

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

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

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

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

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

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

TSGP
PSGP
IBSGP
BZPP
SHSP
UASI
LETPP
MMRS
CCP
EMPG

CoreStreet ENABLED

174_0207

CORESTREET®

Access Solutions

Logical Access Solutions

Networked Access Solutions

Convergence Solutions

Issuance Solutions

Asure ID® Photo ID Software

Fargo® Card Printers

Embedded Technology Solutions

HID Partner Solutions

Food and Animal

Government

Logistics Technology Solutions

Contactless Payment and Public Transport Solutions

HID Global, the worldwide leader in access control, now offers a full range of solutions for secure identity.

For years, you've counted on HID to provide innovative technology and dedicated support. Now, we've expanded our offering to include everything from the design and production of credentials to IP-based access control to embedded technologies. We believe the future of security lies in our open platforms, simple connectivity and rock-solid reliability. So no matter what secure identity solutions you need, look to HID. We're giving you the green light.

hidglobal.com

HID

ACCESS choices.

Please visit us at ISC West, booth 13075