re:ID

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

CAN NFC LIVE UP TO THE HYPE?

Real ID faces uphill battle • Contactless rides into Boston • Campus IDs go to town • Securing Citrix • RFID in the operating room

CHRIS HART

SHOWTIME
THE LINEUP PT.3
DON'T FORGET ABOUT ME

AVISIAN

Summer 2007

Contents

18 | LOGICAL SECURITY |
Locking down Citrix

60 | RFID | Is RFID in the Operating Room a "Spongeworthy" idea?

53 | CAMPUS | Students monitor laundry progress online via new monitoring solutions and their campus card

34 | INNOVATION | Near field communications is the talk of the ID world but what will it take to turn the talk to action?

26 | BIOMETRICS | Keystroke dynamics: Biometrics at your fingertips
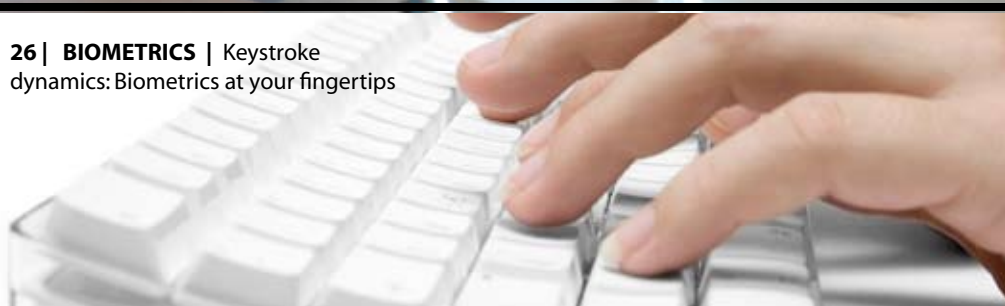
'Compression of time' in identity

Chris Corum
Executive Editor, AVISIAN Publications

I had to prepare two columns for this issue of re:ID. I had been expecting to receive word any day on the GSA's award for what is certainly the most significant portion of the government's PIV card program – the managed services offering. The winning vendor consortium will be issuing and managing credentials for more than 40 agencies and 400,000 individuals. The contract has been highly sought after, to say the least. So I had to have one column if the announcement came prior to press time and a second in case the announcement did not arrive in time.

The announcement was made, and an EDS-led team was awarded a 5-year, $66 million contract. You can read more about that later in the issue. The point for this column is less that it happened than that it makes a wonderful analogy to the struggles we face as an identity industry: things are changing so rapidly that by the time you "get them on paper," they are likely to have changed again. Exhibit one: our article on the 'GSA's pending announcement' that had to be swapped out for the 'GSA's announcement.'

But modern timelines aren't just tough on us as individuals. They beat up on technologies as well.

Our cover story – or series of stories – is a perfect example. We investigate Near Field Communications (NFC), which for most of us is a relatively new technology, attaining ISO standard status less than four years ago. Already, though, some analysts and industry watchers are calling it slow to develop, suggesting that it may not live up to the early hype if significant progress isn't made this year. Our editorial team tends to disagree with this sentiment – as you will read, there is impressive progress on many NFC fronts – but still it highlights the incredible compression of time facing the identity markets.

Technologies, projects, companies and even people must prove their worthiness far faster than ever before. The pace of change is phenomenal. That change can describe societal needs or perceived needs from ID technology. It can describe advancements in technology that supercede prior technologies. Or it can describe external forces such as political whims, economic forces, or media influence.

Any of these elements can abruptly shift direction in identity initiatives, and, as we stated, time is highly compressed. Now imagine that all of these elements are experiencing this massive pressure, making it easy to see why it is increasingly rare for a project or initiative to make if from concept to implementation looking anything like it did at the outset. In fact, it is rare that it makes it to implementation at all.

Keep this in mind as you read about NFC, the Real ID driver license reform, FIPS 201 progress, and many of the other projects covered by our editorial team in this issue. The projects that have made it to these pages are the few exceptions to the rule that made it through today's compressed time.

We'll see you at Cardtech Securtech in San Francisco. Stop by our booth and say hello. Our team will give you a demo of our newest ID technology web site, FIPS201.com.
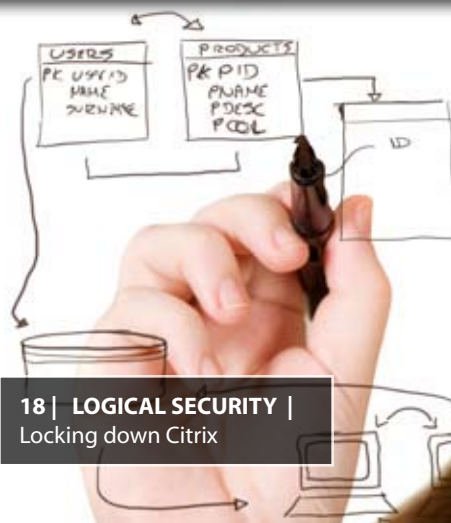
With driver license reform likely to cost billions, Real ID will require state and federal partnership to deliver on promise

Andy Williams
Contributing Editor, AVISIAN Publications

While some of the more costly elements that could have been forced on states to comply with the Real ID Act haven't materialized – at least in the proposed rules that have come out of Washington. Still, there is anxiety over the act itself, its cost, and whether states can meet the compliance deadline that's now less than one year away. One person who helped draft the recommendations for establishment of the Real ID Act believes states should stop worrying about complying and work at developing a partnership with the federal government that would make Real ID execution simpler.

The Real ID Act of 2005, passed by Congress last year, prohibits federal agencies (and airlines) from accepting state-issued driver licenses or identification cards unless they meet minimum security requirements – such as including common machine-readable technology and certain anti-fraud features. It also requires verification of information presented by the license applicant, who must also supply evidence that he is a citizen or a legal immigrant. The act requires standardized driver licenses by May 11, 2008, although states will be able to apply for an extension until December 31, 2009, according to proposed Real ID compliance rules that were issued in March.

Poll: nearly three-fourths of Americans support Real ID

A UPI/Zogby poll released in mid-April shows that 70% of Americans support national driver license standards as called for in the Real ID Act, while about 25% oppose it. However, half (51%) said they oppose any federal law that would require a national ID card containing biometric information, such as finger-prints, while more than 44% said they would support implementation of such a card.

According to UPI, opponents of the Real ID Act said the poll reflected the absence of a national debate on the issue, and that the opposition from a growing list of state legislatures to the new law was a better gauge of U.S. opinion.

The Act came about from 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." That's particularly evident since many of the 9-11 terrorists had fake driver licenses.

The biggest concern from the states, once Real ID was enacted, was that it would be expensive, costing billions of dollars – some have warned – to implement.

Promoting a state and federal partnership rather than repeal of the Act

Janice Kephart, former counsel to the 9/11 Commission and currently president of 9/11 Security Solutions, believes a partnership between states and the federal government is needed to assure Real ID compliance.

"I feel so strongly that the commission recommendations have tremendous validity. It's now defunct, and there is no way to drive this forward," she said of her reasoning for continuing to stay involved in security areas. "I feel I need to keep pushing these recommendations as best as I can. There has been a lot of misinformation on border issues and a misconstruction of 9/11 recommendations. I feel the record has to be kept straight."

Her latest white paper, *Identity and Security: Real ID in the States*, is an attempt to provide states that question Real ID with reasons to seek a federal partnership rather than a repeal of the Act, as some 16 states have proposed.

She notes that Real ID is one of the only 9/11 Commission recommendations that rely heavily on the states for implementation, and successful execution of the Act requires a partnership between the federal government and the states.

Real ID Act's recommended 2D barcode security isn't good enough, says smart card industry

The 40-page proposal's recommendations fall short of endorsing highly secure contactless ID chips

Marissa Torrieri
Contributing Editor, AVISIAN Publications

State governments may be fuming over the Real ID Act's tight implementation deadlines and a lack of federal funding, but smart card developers are taking issue with its security requirements – or lack thereof.

On March 1, the Department of Homeland Security filed a notice of proposed rulemaking for the "Real ID Act of 2005," which sets forth minimum document requirements for driver license and identification card issuance for United States citizens. This most recent revision pushes the deadlines back for states to start issuing these driver licenses.

Under the new proposal, states may file for an extension by February 1, 2008, to start issuing Real ID-compliant licenses on January 1, 2010. By May 10, 2013, all licenses and ID cards must be compliant.

Though the proposal outlines measures for card application and issuance, state governments are complaining that it doesn't call for additional funds to offset the cost of upgrading existing card reader systems (referred to as Machine-readable Technology, or "MRT"). Section 202 (b) (9) of the Act requires states to include a common MRT with defined minimum data elements for the driver licenses and identification cards. The proposed regulation would mandate the use of the PDF-417 2D bar code as the common MRT technology standard.

According to many smart card industry leaders, the PDF-417 2D barcode standard isn't much more sophisticated than the existing ID technology used on today's licenses.

HSPD-12

in one neat package.

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

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

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

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

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

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

©2007 Lenel Systems International, Inc.

LENEL
A UTC Fire & Security Company

"Neither the federal government nor the states can implement this important national security measure on their own. They're going to have to work together," she added.

She sees the federal government as providing assistance in "procurement in terms of hardware/software and printing machines. For those who want to comply, the federal government can assist them (states) by setting out a menu of compliance options, so the states don't have to figure things on their own. The federal government is trying to drive down costs so states can buy at cost."

One of the key ways the feds can help is with the data it has on file. "The federal government holds data that states normally don't have, such as a determination if an alien is a foreign resident, if he has legal status, his Social Security number data, passport data. These are databases that can be checked when an applicant applies for a new driver license," said Ms. Kephart. "Sharing information on a real time basis with the states is necessary."

Real ID, as proposed by the new rules, is certainly capable of being implemented by the states. "All the technology is there," she adds, "the government is making sure that only technology that's proven and capable will be required in the rules."

Debunking myths and addressing funding

In her Real ID missionary status, she has also gone out of her way to debunk so-called "myths" about Real ID. "Real ID does not invade our privacy, it doesn't create a national ID card, and states can opt in or out if they want to," she said.

She does agree, partly anyway, with one of the common complaints … that costs will be prohibitive. It will be expensive, she said, but the Department of Homeland Security will enable states to use up to 20% of the state's Homeland Security Grant Program funds for Real ID. "In the last grant round, roughly $250 million was provided to states, meaning that about $50 million is available for Real ID compliance.

DHS has another $34 million in another grant program expressly created for this purpose," she added.

This helps but will only make a dent. According to Ms. Kephart, "states have estimated they need an initial $1 billion in start-up costs, and the total costs have been estimated at around $11 billion. More funding is absolutely required."

Implementing Real ID is not just a government responsibility either, she said. "The ability to verify an individual's true identity is one of the cornerstones of our national and economic security. As such it's everyone's responsibility, for our nation is only as strong as its weakest link."

Establishing minimum standards but encouraging states to do more

"What Real ID really does is set the bar at a certain place that many states are already meeting but some are not," she added.

The proposed 2D standard, says Neville Pattinson, Vice President of Government Affairs and standards for Gemalto, would be easily thwarted, and wouldn't make the cards much better than they are today. In fact, it would defeat the main purpose of the Act: to raise the level of difficulty of counterfeiting the card and stopping fraudulent behavior.

"Adding a smart card chip to an identity document, as many U.S. programs already do, is the proven way to increase the difficulty to fraud the document, to protect the privacy of the machine-readable zone, and to ensure the ID is being used by the bearer, and to open up the possibility to enable e-government services using digital credentials in the chip," says Mr. Pattinson. "Printed bar codes are frankly obsolete and non-workable in today's increasingly demanding and capable digital society."

But Jonathan Frenkel, Director of Law Enforcement and Information Sharing Policy for DHS and one of the government staff members who helped draft the proposal, said the Real ID Act's security requirement is only intended to establish a minimum standard.

"The proposed rule actually identified a variety of technologies that DHS considered to satisfy the common machine readable technology requirement of the law, and went through the rationale of why DHS chose a 2D barcode standard," Mr. Frenkel said. "Of course anyone who disagrees is free to file comments saying why they believe a different technology should be the one used as the minimum across the country. Nothing in the proposed rule would prevent the state from adding additional technologies beyond those minimum standards."

Cost was a factor in determining the minimum technology requirements to impose upon states, Mr. Frenkel said.

But Mr. Pattinson said the benefits – genuinely secure IDs instead of ones that give consumers a false sense of security – outweigh the additional costs. Furthermore, the cost for immensely better security only amounts to a few dollars more per card.

"Smart card technology adds a small additional cost to the cards," says Mr. Pattinson. "You're talking about $3 more to add that chip … if it's a higher end chip, it's $4 more."

Furthermore, the cost of the driver license itself is very small compared to the back end costs of building the system and infrastructure, says Tres Wiley, Director of eDocuments at Texas Instruments, Inc.

If the final rule won't change minimum technology standards, another favorable option for states might be to let the citizen decide if they want to pay a few extra dollars for the additional functionality beyond the 2D bar codes. Cards in number of other countries use chip-based technologies for multiple purposes.

"The whole purpose for the Real ID was to improve the security, and the 2D barcode doesn't materially improve the security of the driver license," says Mr. Wiley. "Secondly, there's a golden opportunity to lay out some requirements for chip-based ID cards so states can add functionality."

Real ID Estimated Costs (10 years)	$ million (2006 dollars)	% Total
	undiscounted	undiscounted
Costs to States	**$14,600**	**63.20%**
Customer Service	$6,901	29.90%
Card Production	$5,760	24.90%
Data Systems & IT	$1,436	6.20%
Security & Information Awareness	$471	2.00%
Data Verification	$18	0.10%
Certification Process	$14	0.10%
Costs to Individuals	**$7,875**	**34.10%**
Opportunity Costs (268.8 million hours)	**$7,113**	30.80%
Application Preparation (161.9 million hours)	$4,283	18.50%
Obtain Birth Certificate (26.5 million hours)	$700	3.00%
Obtain Social Security Card (15.8 million hours)	$418	1.80%
DMV visits (64.7 million hours)	$1,712	7.40%
Expenditures: Obtain Birth Certificate	**$762**	3.30%
Costs to Private Sector	**$9**	**0.00%**
Costs to Federal Government	**$617**	**2.70%**
Total Costs	**$23,101**	**100.00%**

Source: Department of Homeland Security

The act sets "minimum standards" for both what goes on the card (driver license) and for the security of the card itself. Probably most states already meet some of those requirements as to what's included in the license (e.g. photo, name, address, and other personal verifying information).

"The piece that's a little stronger is the anti-counterfeiting section," she says. "What's lacking right now is an easy way for the local police officer to determine whether an ID is fake just by looking at it."

But while such security features haven't been built into Real ID, there are ways "you can embed something in a card to make it easy to determine if the card is fake," said Ms. Kephart. Such security features could include tactile (touch and feel), "bumps in the card that are hard to reproduce. There's also digital watermarking and other kinds of laser technologies that can be used," she added.

"I've talked a lot to folks who do immigration and ID enforcement and they're the ones telling me about what you can do against a counterfeiter. We can't do away with it but we can drive up the cost so high (that you effectively)

do away with them." While such thinking may be naive, doing nothing is just as dangerous.

"We need to drive up the cost of recreating a counterfeit card so the counterfeiter's cost becomes so high that he's driven out of business," she added.

Ms. Kephart said, "every state is looking to get on board as fast as possible with a digital image exchange," another way to verify if the same person holds more than one license. "Some of the states are already requiring that kind of information. A lot of states have stronger requirements than Real ID requires, but they haven't been able to cross check with other states."

With one of the requirements – proving who you say you are, such as with a birth certificate – there's no way to check if that's valid or not, "but if you can check against other databases, you'll know if someone else also has that same birth certificate," she said. That's one of the purposes of Real ID, she added, "to give states the ability to have this information in front of them so they can verify that information and use it to make good decisions."

Another issue that has surfaced regards central issuance of driver licenses. It has its pros – more security, more time to check data – and cons – primarily convenience, since applicants must wait a couple of days before they get their licenses.

She points to states like Kansas that have moved from an over-the-counter system to a central issuance system and have actually seen a decrease in applicant processing time from 14 minutes per person to seven minutes per person.

Real ID isn't going to go away. But, as she points out in her white paper, Real ID "can make a difference ... but only if fully implemented and adequately funded."

Additional resources

Ms. Kephart has created an online Identity Document Security Library, consisting of legal, technical, and policy pieces regarding identity document security. She calls the library a "one-stop-shop information portal for those seeking objective, credible information on the issue of identity document security." It is available at: 911securitysolutions.com/idsecuritylibrary.

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

re:ID

FREE SUBSCRIPTION

The following questions must be answered to complete your subscription.

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

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

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

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

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

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

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

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

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

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

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

Name _____

Job title _____

Company _____

Address _____

City _____

State/Province _____ Zip/Postal Code _____

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

Phone _____

Email _____

Signature _____ Date _____

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

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

❏ SecureIDNews ❏ ContactlessNews ❏ CR80News ❏ RFIDNews

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

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

Two-factor authentication for remote banking

Nigel Reavley
Director, Banking Unit, XIRING

Consumer confidence in online banking has grown rapidly in recent years. Once limited to their local branches, customers are now embracing new technologies for their banking needs. A recent study by Lloyds TSB showed that over two-thirds of Britons conduct the majority of their banking over the Internet, which is a three-fold increase on 2005 figures.

Despite the growing popularity of online banking, fraud within this particular channel remains a prime concern. Indeed, the current trend for migration to EMV in many countries across the world has reduced the instances of fraud within cardholder present transactions, but increased the threat amongst other channels, including the Internet. Consequently, these less-protected transaction channels now urgently require an anti-fraud solution.

As a result, two-factor authentication card readers are currently being trialled or deployed by a number of financial institutions worldwide in the fight against Internet fraud. In the UK and Belgium banks previously in pilot mode with the readers have moved to the deployment stage. The UK market is particularly advanced, where major banks are now at the stage of considering their choice of supplier. 2007 will be the year when the first few million users receive two-factor authentication card readers for their online banking transactions.

Other countries such as France, Portugal, Turkey and Italy are closely following and moving into the pilot stage. In addition, the Eastern Europe market will be ripe for deploying the technology in 2007. Without the burden of legacy systems, the adoption of anti-fraud solutions can be made quickly without the need to change infrastructures.

As recent years witnessed a rise in the popularity of online banking, we are now seeing telephone-banking and m-commerce come into their own. In the UK, for example, £23 billion worth of payments are made through the telephone, which accounts for 45% of all card-not-present payments. Due to the successful deployment of Chip and PIN however, there has been a 57% increase in UK direct telephone order fraud in the past year. Two-factor authentication technology will need to extend its reach to telephone payments in order to combat this trend.

Access to banking via videophones will further increase the reliance on authentication technology to ensure the security of face-to-face transactions via screens. Lessons learned from Internet banking should be applied to securing these emerging channels, which hold the key to making the concept of a mobile bank a reality.

Locking down Citrix

Examining the popular solution for security, mobility and compliance ....

Many of the more than 180,000 organizations using Citrix have to deal with new concerns about security, and they all share the same goal: to keep their system, and their Citrix implementation, as user friendly as possible. Smart cards, one time password (OTP) devices, and biometrics are all being used to authenticate the user in Citrix-controlled environments. The company is doing its part to keep up with these increasing security demands by implementing a new partnering process to certify third party security products as "Citrix ready®."

Though virtually a household name, many non-users are not quite sure what Citrix really does? Senior Product Marketing Manager Chris Harget explains that, "Citrix endeavors to deliver any application to any user, anywhere with the best performance, highest security, and lowest cost." By virtually any measure, the company has been successful in its mission. Citrix boasts that 98% of Fortune Global 500 companies use at least one of its products.

But the ability to access information from virtually anywhere, at any time is no longer just a necessity for large companies. It is essential even for small companies, and hundreds of thousands rely on Citrix.

Tips from Citrix for securing your network

Protect the front door with two-factor authentication. The most secure are certificate based smart cards, protecting the broadest range of files, email, application etc.

Once you're in the front door keep applications and data in the data center and not on indivdual workstations. This reduces the chance that either can be compromised.

Citrix's application firewall further increases security. Other firewalls allow everything through except certain ports, which means attacks can exploit open ports. Citrix's application firewall keeps everything out except traffic required for your known applications.

Citrix Access Gateway (SSL VPN) provides the smart access approach based on the device you are on and the network you are coming from. If you are accessing a resource from inside the firewall on a corporate device, you'll have full access. But, if you log in from home on an unmanaged device, you can be restricted from printing or saving locally ... because that's less secure.

Ryan Kline
Contributing Editor, AVISIAN Publications

The distant workforce demands immediate and secure access to the applications and information on the network from anywhere the business takes it. But this need highlights the dicotomy between security and ease of access. Traditionally, if the network is to be secure one must expect more inconvenience when connecting to it.

Citrix recognizes that securing the network is essential to maintaining a risk-free environment for employees and clients. "From securing the VPN (Virtual Private Network) connection … to securing the application … to ensuring that the data does not leave the data center … and the single sign-on … are elemental functionalities that Citrix provides to secure the network," explains Mr. Harget.

Strong authentication in the Citrix environment

Many organizations require strong authentication to be integrated with their network. In 2005, Citrix's research suggested that 35% of its customers used some form of strong authentication. The methods included, but were not limited to, one time password generators, smart cards, USB tokens, or biometrics.
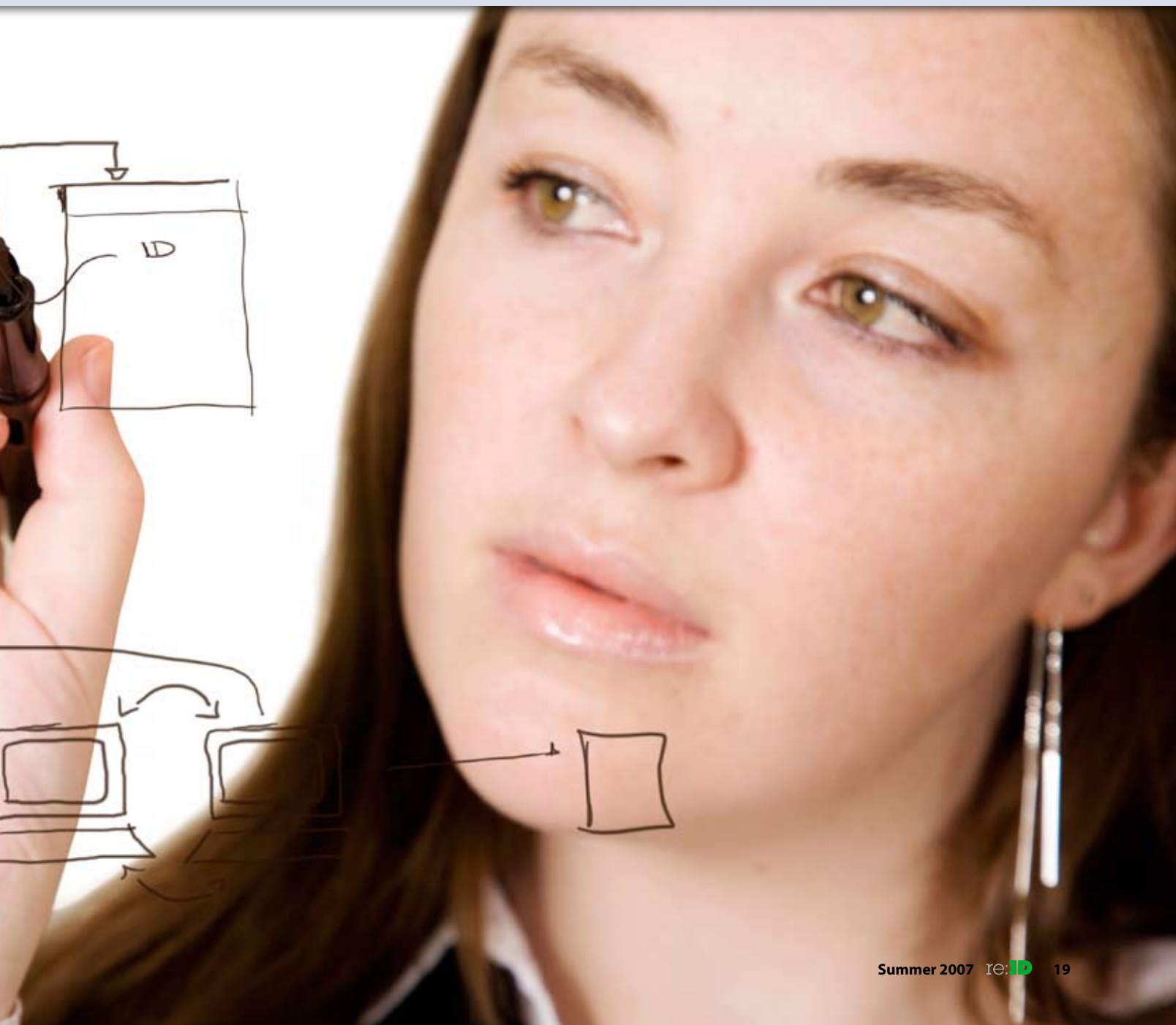
Strong authentication is most commonly used in organizations that must comply with regulations such as: medical, financial, government, manufacturing, technology, or law enforcement.

The healthcare industry complies
with HIPAA via secured Citrix solutions

The largest user of Citrix's single sign on functionality has been the healthcare industry. Single sign-on is a specialized form of software authentication that enables a user to authenticate once and gain access to multiple applications or areas of the network. Since single sign-on authenticates a user for all other applications to which he has access, passwords to secondary applications need not be shared with the user, thus minimizing risk to the organization when a user leaves.

The medical industry is required by HIPAA (Health Insurance Portability and Accountability Act) regulations to meet strong authentication for login if patients' records are kept electronically.

Ron Crall, CIO and HIPAA Compliance Officer for St. Joseph Hospital in Bangor, Maine, understands how important it is to protect the privacy of patients' information. In a case study done jointly between Citrix and St. Joseph Healthcare, he stated, "with HIPAA regulations, we can't have an employee walk away from a workstation that they've logged into and leave the screen visible. With Citrix … we have a solution for easily disconnecting users from an active session and rapidly logging them back in without having to restart applications."

Citrix reduces the log-on time from one minute to less than ten seconds, a time savings which can translate into treating several additional patients per shift. It also provides an additional security benefit, keeping application data behind the corporate firewall. There are no longer "pools of health information sitting unprotected on somebody's desktop computer," says Mr. Crall.

Security for all

Keeping critical information off or machines and behind the firewall increases security for both the healthcare industry and all industries. According to Mr Harget, "traditional firewalls allow everything through except certain ports, which means attacks can exploit open ports. Citrix's application firewall keeps everything out except traffic required for your known applications."

A smart access approach determines access levels based on the device you are on and the network you are coming from. From inside the firewall on a corporate device, you will be granted full access. But, if you log-on from an unmanaged device off-site, you will be restricted and possibly not allowed to print or save locally, because that is less secure.

Government plays, too

Government agencies across the United States are beginning to feel the effects of HSPD-12 and FIPS 201. With physical security in the forefront of many governmental agencies, Mr. Harget expects government agencies to lead, issuing one authentication device to secure both the entrance and the network. "We are seeing some customers look for a way to converge devices (the actual token or card) used for physical and logical access, but they do not want to converge the databases. Citrix Password Manager is very capable of working with card systems that can be used in this way."

While creating Password Manager, Citrix took an architectural approach that made it easy to incorporate two-factor authentication. Citrix implemented a method called "GINA chaining," which allows the network to be compatible with any hardware that conforms to the Microsoft standard. GINA, an acronym for Graphical Identification and Authentication, is the Windows component that manages the Ctrl + Alt + Delete dialog box that collects the data needed for authentication.

Many of Citrix's products require alterations to the GINA chain. "This simply means we intercept and insert ourselves into the GINA process without disrupting it," continued Mr. Harget, "such that we do not inhibit or alter other components that interact with GINA."

Ultimately, any FIPS 201 compliant identification card could work with the Citrix platform. But, Citrix, for strategic reasons, partners with select vendors that have gone through testing to become Citrix Ready in order to boost confidence in third party strong authenticators. For ultimate ease and convenience governmental agencies only need to purchase FIPS 201 approved PIV cards and middleware that are also "Citrix Ready." (Although it may be required in the future, nothing in HSPD-12 states that governmental agencies have to secure their workstations with FIPS 201 compliant log-ins.)

Currently more than 20 options for Citrix Ready two-factor authenticators exist. These products range from smart cards to one time password generators. and

Citrix has an extensive selection of two-factor authentication partners that have been certified Citrix Ready. Partners use a variety of techniques, including BioPassword and bioChec as biometric solutions; Vasco and RSA with one-time password generators; and Gemalto as a smart card solution. The complete list of Citrix Ready products can be found at Citrix's website, www.citrix.com.

27 countries
60 million citizen IDs per year
50 years of service
1 universal feeling: Trust

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

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

Real Solutions for Secure ID.
Learn more. Request your copy of the Secure ID Lifecycle whitepaper by visiting:
www.digimarc.com/ID

DIGIMARC

Innovative card form factors revolutionize look, function

New shapes, transparency, 3-D and more make the 'plain old card' just plain …

Andy Williams
Contributing Editor, AVISIAN Publications

Whether in the form of a football, a brand logo, or a keychain-ready miniaturization, different card shapes are battling the traditional 'CR80' or 'ID1' format for market share. Even watches, cell phones, and key fobs are joining in the game. But as long as ATM machines and many mag strip readers are geared for only one card shape, the common 3.370" x 2.125" rectangular form factor will continue to maintain its unimaginative grip on card users.

Still, the rapid growth in contactless technology has freed card makers from being locked into a single standard card shape that's been around since the first credit card was invented. The first modern day charge card was issued in the 1920s by oil companies to give their customers a convenient way to pay for gas. According to Wikipedia, the first credit card for general purchases besides oil was likely the Diners Club in 1950. The first bank-supported card didn't come along until the late 1950s with BankAmericard (now Visa) and Master Charge (now MasterCard) a few years later.

With contactless technology, you no longer need to worry about swiping a card's mag stripe through a reader, sometimes more than once to get a successful read. A simple tap will do, and this feature has given marketers free

rein to develop new kinds of more durable and convenient cards and fobs, both two- and three-dimensional.

Rahul Gadkari, Financial Services Marketing Manager for cardmaker Gemalto North America, said the company shipped some five million contactless cards just in the first six months of 2005, shortly after the contactless phenomenon took hold.

"We started with regular ISO (card) form factors that you see now with regular mag stripes. It's still the predominant form factor because it works in ATMs, (and) fits in wallets, Mr. Gadkari said. "It's a legacy device, and at the same time something people are comfortable with."

He believes that when Visa developed its mini credit card, things began to change in card design. The mini card was made durable enough to allow a hole to be punched through it for use on key chain. "We make a lot of mini cards today," said Mr. Gadkari.

"With pure contactless cards, we are free to use any dimensions. It makes payment easier, and there are many different form factors possible," said Hans Heusmann, Contactless Product Manager for Giesecke & Devrient (G&D), one of the world's largest card manufacturers. "That's why it's difficult to explain what's out there. It depends on customers and what they want."

While bank and card issuers are leading the way with different card form factors, Mr. Heusmann added that for the manufacturers themselves, "there's quite a bit of investment necessary to bring out a three dimensional form factor."

Gemalto also produces what Mr. Gadkari calls, "our two-dimensional card form factors covering different shapes." He adds, "Some cards are shaped like a donut, a football, soccer ball or basketball. Those are usually contactless." But designers haven't stopped there. "Beyond that we also saw some requirements from banks and issuers who wanted a three dimensional fob or token device, something people are used to getting for authentication devices. Banks said they wanted these devices to be just like a contactless payment card," said Mr. Gadkari.

Gemalto works with "some of the leading issuers" to develop different fob form factors. "We have some prototypes done and we're working with some issuers who have provided us with their marketing design," he continued. An issuer in Asia wanted a watch to be a contactless payment device. "We worked closely with MasterCard to come up with a watch which can be used as a payment device," he said.

It's obvious that, with contactless technology, form factor rules have gone out the window. "We can be very creative," said Mr. Gadkari. Be-

sides watches, "you now can have wristbands (used mainly at swimming or ski resorts) that are contactless devices, basically more like a prepaid device," he said. "They reduce time at the concession stands, speed up their concession stand payment experience, and (visitors) get more satisfaction."

With watches or wrist bands, "there's always a discussion about the value of the form factor," said Andreas Johne, G&D's EMV production manager. "You have to look at how it will be used, where you will present the key fob. Will you present the complete key ring when you make a payment? Most people are not willing to present a key ring at time of sale. A watch or wrist band isn't really convenient."

Those issuing contactless fobs, "have to undergo Visa and MasterCard approval, an expensive and lengthy process," said Mr. Johne. "That's why you don't have too many different form factors."

The other consideration, said Benoit Guez, VP of Smart Cards and International Sales for Colorado-based CPI Card Group, is *just how many key fobs one person is likely to carry around?* "I don't want five key fobs in my pocket," he said.

Marketing gimmick or legitimate innovation?

So are alternate form factors simply a marketing gimmick? Mr. Johne doesn't believe in producing form factors "just to have them." He adds, "We're willing to cooperate with our customers and to fulfill their requirements."

For example, a bank might have a form factor in the shape of its logo, or a car manufacturer with a fob shaped like a car. "Our experience is that banks are reluctant (to develop new form factors). But non-banking industries have used form factors successfully," he added.

"Imagine," said G&D's Heusmann, "that McDonald's could issue its own McDonald's Pay-Pass card on a fob in the shape of a hamburger. You're giving your customers a payment device – it could be a debit card, credit card, preloaded. There are several possibilities," all now feasible in today's card form factor world.

"You need to make (the fob) more of a marketing tool rather than a gimmick," insisted CPI's Guez. "It's not going to replace a CR80 card. In Hong Kong 15 million people are using CR80-style cards for transit. They don't need a fob."

There's another interesting problem, particularly for banks, said Mr. Heusmann. When a bank issues a regular-sized credit card, it's mailed to the customer. But if it's a fob, "banks must invest in different machinery to personalize them." When they want to send the fob to the card holder, it can't be sent through the normal channels as economicaly. "G&D has different solutions for this. For example, instant issuance. The bank clerk can personalize the fob directly in front of the customer," issuing the fob immediately.

Yet, while many of the different card shapes carry the contactless chip and antenna, they can still operate with just a mag stripe to be read at any POS system equipped with a handheld reader.

While marketing promotions such as the FIFA World Cup event (with soccer ball shaped fobs or cards) are some of the impetus behind varying form factors, for banks it's simply to try to, "differentiate themselves from others," said Mr. Gadkari. "Anyone doing contactless was looked at as having a cool device. Prior to that, the maximum differentiator banks had was in the printing on the card," such as how bright it was, perhaps a hologram, or the bank's raised logo. He continued, "They had stretched that look and feel as much as they could. That credit card is the true brand disclosure for the issuer. You want to make sure their debit or credit card is top of wallet because most carry six to seven cards, yet they usually only use one," he added.

"What contactless did was make those cards top of wallet. If consumers liked it, they would keep using it," said Mr. Gadkari. But now, since many banks have jumped on the contactless bandwagon, banks are looking at newer differentiators. "You're now talking out of wallet concept."

Creating a new type of card isn't something that's done overnight. "With fobs, since they're so closely tied to brand exposure, they have to be very specific to each bank," adds Mr. Gadkari. "Since these are technology devices, they also need to be certified. We can make any shape or form, we just want it to be robust enough to house a chip and antenna."

With more and more unusual shapes and sizes for contactless cards being created and issued, you may soon begin to ask yourself, "What **is** in my wallet?"
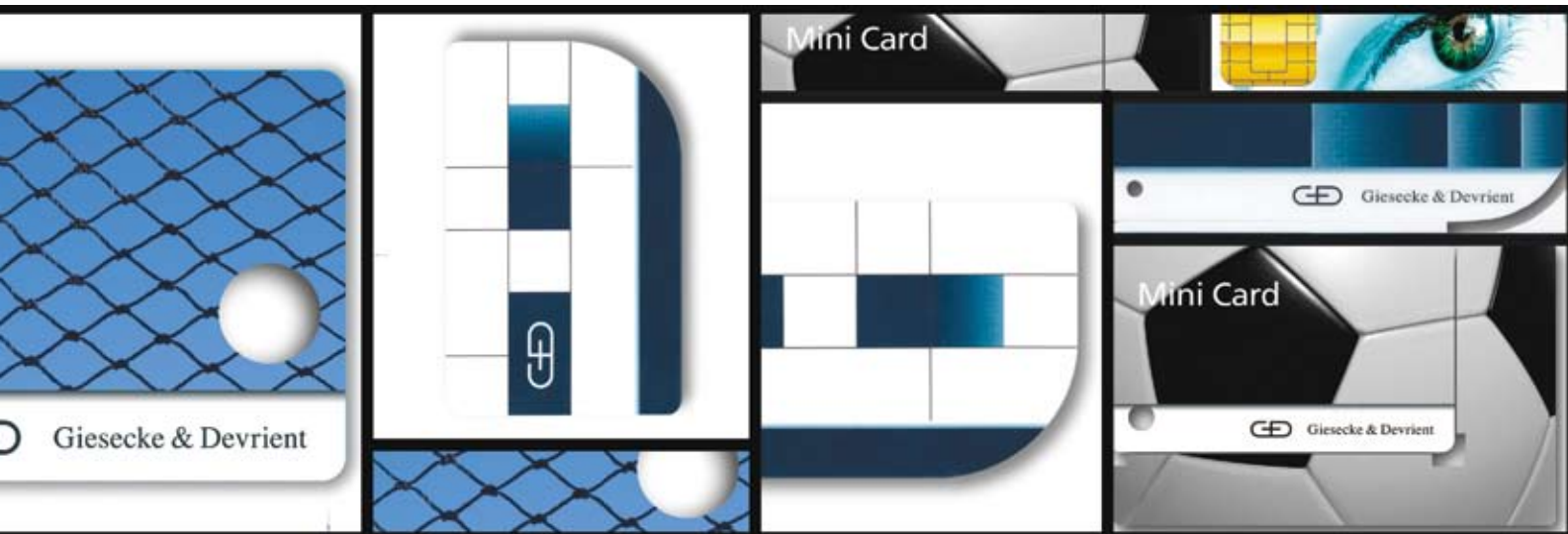
"Having HID and Fargo together as one organization can better serve the marketplace. We're coming together through the photo ID channel as well as through the access control channel, producing more complete ways (that issuers) can enhance their security."

— David Sullivan, President, Fargo Electronics

New Fargo president lays out company's direction as part of HID Global

Andy Williams
Contributing Editor, AVISIAN Publications

Fargo Electronics' merger with HID Global last year was just the beginning of what officials at both companies see as a bright future for the secure card identity systems company. Fargo Electronics' new president, David Sullivan, fresh from a stint in Europe, wants to grow the company, not only in the U.S. but internationally. The fact that HID Global turned to a person with more than a few years' experience in the international market certainly foreshadows this move.

Mr. Sullivan began with Hughes Identification Devices, a subsidiary of Hughes Aircraft in 1994. Later when the company became a subsidiary of Palomar Technological Companies in 1995, it changed its name to HID Corp. Five years later, it became a part of the ASSA ABLOY chain of companies and has since been renamed HID Global.

Fargo was founded in 1974 in Fargo North Dakota as a manufacturer of specialty printers. In February of 2000, Fargo became a publicly traded company and concentrated its product line on secure technologies for identity card issuance systems, including ID card printers, encoders and materials. The company merged with HID in August, 2006.

"I started as a regional sales manager for HID," said the 46-year-old Sullivan. "Then I went on to become North American sales manager." He eventually migrated to Europe to head up a sales team for "several ASSA ABLOY companies, one of them being Indala (a contact/contactless smart card producer). At HID Global, I was managing director for Europe, the Middle East and Africa."

"Dave has a long history of success with HID and in the industry," said HID's President/CEO Denis Hebért when he announced the promotion. "Like Fargo, our EMEA division was a well-established enterprise. Dave strategically positioned the business and accelerated the growth beyond its previous success."

One of Mr. Sullivan's main goals is implementing international expansion objectives within Fargo. His experience in the European, Middle East and African markets can accelerate this process, he said.

"We plan to take advantage of HID's global footprint in order to better serve our international customers. Fargo has done a fantastic job of building an international presence without any international offices, but now we're putting our products and people into distribution centers internationally."

Previously, Fargo relied on US-based staff to manage their international business. "We only had one employee in Europe," he said. "We have never had anyone in Asia. Now, we're hiring additional people in the UK, Hong Kong and Latin America. We also have HID offices in England, Hong Kong, India and China and by the end of the year we'll be distributing Fargo printers from those locations."

In addition to his international experience, Mr. Sullivan sees his time spent on the HID side as an asset to his current job. Access control manufacturers often include credential personalization systems in their packages, like a desktop printer that prints the cardholder's

image to the access card, he said. "By working in conjunction with HID, Fargo will be able to accelerate our opportunities with those access control manufacturers."

With the emphasis on security today, it's no longer about simply printing an ID badge from a printer. "You take a photo ID badge and integrate it with the entrance doors, the network log-on and the time and attendance program," said Mr. Sullivan. "It's much more tied into the total security program."

Why? The tragedies of September 11 not withstanding, "there are a number of reasons. It goes back to increased attention being paid to ID management and security related to identity. You see that now at the government level with Real ID, CAC (Common Access Card from the U.S. Department of Defense) and electronic passports," he added.

These are all areas in which Fargo is involved. "We print to plastic making the driver licenses (key to Real ID compliance) as well as the badges. The opportunity with increased technology in cards is that you can load multiple applications on the card, so that it includes the credentials, as well as cashless vending or other value on the card, or even biometric templates that can be stored on the card. All these applications require you to program them onto the card. It makes sense to do this at the same time that you're printing the badge."

Put another way: "By incorporating HID's (security and contactless) encoding technology inside the printer, the end user benefits from the result. He receives a complete badge."

"You can see, through some of HID's recent acquisitions, such as Synercard (ID card software solutions provider), that there are various

components coming together to provide users with integrated solutions. As one company, we can provide more complete solutions." Recently, HID Global rolled its Card Service Bureau, AccessID and Synercard into an "expertise group" called HID Identity.

Mr. Sullivan emphasized that much of Fargo's past agenda will remain, "but we'll refine it with enhancements, our ability collectively to provide more complete and robust solutions."

He concludes, "having HID and Fargo together as one organization, can better serve the marketplace. We're coming together through the photo ID channel as well as through the access control channel, producing more complete ways (that issuers) can enhance their security."

Keystroke dynamics: Biometrics at your fingertips

Ryan Kline

Contributing Editor, AVISIAN Publications

On May 24, 1844, the message, "What hath God wrought!" was sent by telegraph from Baltimore, Maryland, to our nation's Capitol in Washington, DC. A new era in long-distance communications had begun. By the 1860s, the telegraph revolution was in full swing, and telegraph operators had become a valuable resource. Each operator developed his own unique signature and could be identified simply by his tapping rhythm.

As late as World War II, the military still relied on Morse code to transmit its messages. Military intelligence identified that many individuals had their own way of keying in a message's dots and dashes, creating a rhythm that could help distinguish ally from enemy.

Telegraphs and Morse code lead to the earliest examples of keystroke dynamics, a behavioral biometric indicator which can be used to recognize an individual based on a behavioral characteristic rather than the more common physiological measures.

Science of keystroke dynamics

Modern keystroke dynamics utilizes behavioral biometrics in an effort to identify individuals by the manner and rhythm that he or she types characters on a keyboard or keypad. The keystroke rhythms of the user are measured to develop a unique biometric template of the user's typing pattern for future authentication. Raw measurements available from most every keyboard can be recorded to determine dwell time (the time a key is pressed) and flight time (the time between key down and the next key down and the time between key up and the next key up). After the recording is made, it is processed through a specialized algorithm, which determines a primary pattern for future comparison.

Speed & errors help identify the individual

In the most basic case, simple rules can be used to determine if the correct individual user is attempting to log in to a system. For example, if we know that 'Bob' types at a rate at 20 words per minute, and the subject is typing at 70 words per minute, it is almost certain that it is not Bob. This test, called a one-way test, is based simply on raw speed uncorrected for errors. It is always possible for people to type slower than normal, but it is unusual for them to suddenly type twice their normal speed.

One could also assume that the mystery user at the keyboard and Bob both type at 50 words per minute; but Bob never felt comfortable with the location of numbers on the keyboard and always has to slow down an extra half-second to enter a number. If the mystery user does not slow down for numbers, then, again, it is safe to assume the presence of an imposter.

The time to get to and depress a key (seek-time), and the time the key is held down (hold-time) may be very characteristic for each person, regardless of how fast they are typing overall. Most people have specific letters that take them longer to find or get to than their seek-time for most other letters, but the specific letters that take longer can vary dramatically from person to person. Right-handed people often have faster seek-times when using their right hand fingers when compared to their left hand fingers. Index fingers may also be characteristically faster than other fingers to a degree that is consistent for a person day-to-day regardless of his overall speed that day.

Additionally, sequences of letters may have characteristic properties for a person, which are often called rapid-fire sequences. In English, the word "the" would be considered a rapid-fire sequence, along with common endings, such as "ing." The rapid-fire sequencing will often vary enough to consistently distinguish different users.

Common "errors" may also be characteristic of a person, and there is an entire taxonomy of errors, such as common substitutions, reversals, double-strikes, adjacent letter hits, homonyms, and hold-length-errors (for a shift key held down too short or too long a time). Even without knowing what language a person is working in, by looking at the rest of the text and what letters the person goes back and replaces, these errors can often be detected. These patterns of errors can differentiate two people who tend to make different errors.

Authentication versus identification

Keystroke dynamics identifies patterns that are strictly based on statistics, and are not as reliable as other biometrics that are often used for authentication (e.g. fingerprints, retinal scans). The benefit to keystroke dynamics is that they can be captured continuously during a session triggering an alarm to another system or person if the keystrokes do not match the recorded formula. (Note: Keystroke dynamics are not always implemented for continuous monitoring and often are used only when someone is logging in to a workstation at the start of a session.)

In some cases, a person at gunpoint might be forced to access his computer by entering a password or providing his fingerprint. But once logged in, the authenticated individual could be replaced by someone else at the keyboard. Keystroke dynamics could stop this from happening because the person at gunpoint may not be able to log in to the workstation properly. Even if he could and the intruder took over, the intruder could be detected and locked out via continuous monitoring.

Keystroke dynamics could also protect doctor/patient confidentiality. If a doctor forgets to log out of an electronic medical filing system, keystroke dynamics could identify when someone other than the authenticated user was typing.

Temporal variation

One of the major hurdles that keystroke dynamics has encountered is that a person's typing varies substantially during a day and between different days. People may become tired or angry, switch computers, reposition their keyboard, or even talk on the phone or otherwise be distracted. These seemingly small shifts could affect the way that the computer interprets a user's keystroke dynamics. These variations will cause error rates to almost any system, both false positives and false negatives. A valid solution that uses keystroke dynamics must take these elements into account, and strive to decrease false positives and negatives.

Even considering these possible false results, the United States National Bureau of Standards asked SRI International to conduct a study on the use of keystroke dynamics for computer security in the early 1980s. The results of the study demonstrated that a simple security measure, such as a username and password sequence, was sufficient for virtually error-free authentication of users.

Commercial products

There are several home and commercial software products that use keystroke dynamics to authenticate a user.

BioPassword is a patented commercial system that uses keystroke dynamics to restrict access to computers. In 1984, International Bioaccess Systems Corporation acquired all the rights to the keystroke dynamics technology that had been developed by SRI International.

Deepnet Security isdeveloper of a keystroke biometric authentication system, TypeSense. It is claimed that this product employs advanced new algorithms such as auto-correlative training and adaptive learning, and achieves better results than similar products.

iMagic Software makes Trustable Passwords and Trustable Presence. Trustable Passwords is its flagship product delivering authentication via password rhythm recognition across all enterprise access points. Trustable Presence couples Trustable Passwords with RFID Proximity badges and readers.

FIPS201.com

THE PREMIERE RESOURCE FOR COMPLIANT CREDENTIALING

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

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

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

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

Contact: **Angela Tweedie**
AVISIAN Marketing Coordinator
850-391-2273
angela@avisian.com
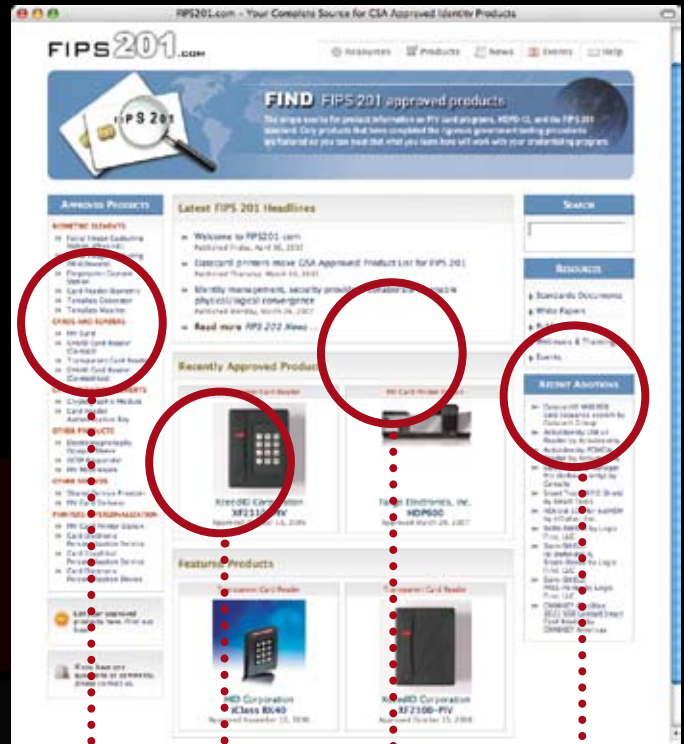
Search for Approved Products by category or search by product name or vendor

Recently approved member listings are highlighted on front page, as are random listings

Constantly updated news feed keeps visitors up-to-date on FIPS 201-related content

Resources section enables member companies to promote white papers, webinars, events.

AN **AVISIAN** ID TECHNOLOGY RESOURCE

Hurdles remain for PIV card use

Marissa Torrieri
Contributing Editor, AVISIAN Publications

Now that federal agencies are invested in the planned government-wide issuance of highly secure, interoperable smart card IDs, actually implementing the new system remains the biggest practical and technological hurdle.

"The card is only the first stage," says Randy Vanderhoof, executive director of the Smart Card Alliance. "There's a whole other phase – accessing the physical access control systems and integrating the smart card into the logical security and PKI infrastructure that many of the agencies operate."

Many of last year's hurdles revolved around learning how to implement FIPS 201, the technological specification developed by the National Institute of Standards and Technology. It is the synthesis of many different technological components: Physical access, logical access, biometrics and PKI, among others.

While the technical standards of the first mass implementation are pretty much set for the first round of PIV cards, getting the cards into use for physical access control in a timely manner poses a big challenge.

Curt Barker, chief of the computer security division at NIST, attributes this to the magnitude of the project, which involves making changes to old physical access systems and making sure the cards and systems are interoperable among agencies.

"The major hurdle right now is that there are a large number of what we call legacy cards – transition cards that are not yet interoperable with fully FIPS-compliant cards," says Mr. Barker. "A lot of card readers handled an older technology that simply passed a numeric value that was 10 digits long. One of the challenges is accelerating the migration from the transition cards like the DoD card and the endpoint card. When you have a lot of equipment that's currently in place that can't read the new cards, it takes time and money to replace."

Smart card developers are keeping other concerns on their radar screen, namely possible future revisions of FIPS 201.

Walter Hamilton, Chairman of the Board of the International Biometric Industry Association, highlighted an ongoing issue – whether to allow reading of the PIV cards' biometric fingerprint data via the contactless interface, or to continue to require the use of contact readers and PINs when accessing the biometric data The issue is an especially large source of contention for the maritime industry's Transportation Worker Identification Credential (TWIC).

"The current implementation of biometrics in FIPS 201 in general raises some issues of specific restrictions of the PIV card itself when used for biometric authentication," says Mr. Hamilton. "The issues currently relate to the physical access applications, where you need to move volumes of people. Entering a PIN seems to us to be overkill and an unnecessary inconvenience when you have strong biometric authentication."

FIPS 201 products and services from the GSA Approved Products List

SecureIDNews

Card Printer Station

XTEC Incorporated	AUTHENTX Card Printer Station
SETECS, Inc.	SETECS OneCARD Card Printing Station
Gemalto	SafesITe Card Manager Pro (Software only)
Digital ID Solutions	XID590i Re-Transfer Printer & Laminator
Datacard Group	Datacard® MX6000 card issuance system
Secure Network Sys.	SNS Credential Issuance
Ultra Electronics	Magicard Tango+L with Omnikey encoder
Datacard Group	Datacard® CP80 Card Printer
Fargo Electronics Inc.	HDP600
Fargo Electronics Inc.	HDP600-LC
Datacard Group	Datacard® SP75 Card Printer

CHUID Reader (Contact)

DataStrip	DSVII

CHUID Reader (Contactless)

Sagem Morpho, Inc.	MA120 W

Cryptographic Module

nCipher, Inc.	nShield 500 for netHSM
nCipher, Inc.	nShield 2000 for netHSM
nCipher, Inc.	nShield PCI 500 TPS, F2
nCipher, Inc.	nShield PCI 2000 TPS, F2
SafeNet, Inc	Luna K3 Cryptographic Engine
Thales e-Security	SafeSign Crypto Module (SGSS v3.3 engine)
SafeNet, Inc	Luna PCI Cryptographic Module
SafeNet, Inc	Luna K3 Cryptographic Engine
Thales e-Security	SGSS v3.2
nCipher, Inc.	nShield PCI 4000 TPS, F2
nCipher, Inc.	nShield PCI 2000 TPS, F3
XTEC Incorporated	Oberthur PIV EP V1 on ID-ONE Cosmo 64k
SafeNet, Inc	Luna K3 Cryptographic Engine
nCipher, Inc.	nShield PCI 500 TPS, F3
SafeNet, Inc	Luna K3 Cryptographic Engine
nCipher, Inc.	nShield PCI 4000 TPS, F3

Electromagnetically Opaque Sleeve

Secure Network Sys.	SNS IdShield Zippered Wallet
XTEC Incorporated	XSHIELD Badge Holder
Identity Stronghold	Secure Badgeholder for ID cards
Secure Network Sys.	SNS IdShield Womens Zippered Wallet
Orient Instr. Comp.	Skim Block Horizontal Badge Holder
Secure Network Sys.	SNS IdShield Tri-Fold Wallet
Smart Tools	Smart Tools RFID Shield
Logic First, LLC	Skim-SHIELD ID-Defender II, Smart-Sleeve
Orient Instr. Comp.	Skim Block Card Insert - Printable
Logic First, LLC	SKIM-SHIELD
Identity Stronghold	Secure Sleeve for ID and Payment Cards
Logic First, LLC	CAC-CAGE Enforcer
Identity Stronghold	Secure Badgeholder for ID cards
Logic First, LLC	CAC-CAGE Defender
Secure Network Sys.	SNS IdShield Bi-Fold Wallet
Orient Instr. Comp.	Skim Block Sleeve
Orient Instr. Comp.	Skim Block Card Insert -Thin
Logic First, LLC	Skim-SHIELD PASS-Porter
Secure Network Sys.	SNS IdShield Credit and Bus. Card Wallet
Exponent, Inc	Electromagnetically Opaque Sleeve

Graphical Personalization

Gemalto	SafesITe Card Manager Pro Service

Electronic Personalization (Product)

Thales e-Security	SafeSign Management Server for PIV
SETECS, Inc.	SETECS OneCARD CMS
VeriSign, Inc.	VeriSign CMS for PIV
RSA Security, Inc.	RSA Card Manager
Intercede Ltd	MyID PIV
Actividentity	Card Management System
XTEC Incorporated	AUTHENTX XANODE26SR Core Ent. Appl.

Electronic Personalization (Service)

Gemalto	SafesITe Card Manager Pro Service

Facial Image Capturing (Middleware)

XTEC Incorporated	AUTHENTX Image Capture Middleware
Aware, Inc	PreFace/PIVPack SDKs

Facial Image Capturing Camera

XTEC Incorporated	AuthentX XA520 Facial Image Capture Sol.
BearingPoint, Inc.	BearingPoint Facial Capture Kit 2.0
Secure Network Sys.	SNS CRITSEC® Image Capture
Aware, Inc	PreFace SDK with Canon A640
Liska Biometry, Inc	DCS8000SF
Liska Biometry, Inc	DCS8000S
Aware, Inc	PreFace SDK with Canon A620
Lockheed Martin	Camera
BearingPoint, Inc.	BearingPoint Facial Capture Kit 1.0
Identix, Inc.	TPE-HWOX-DCPIC
Liska Biometry, Inc	DCS8000SFR

Fingerprint Capture Station

Identix, Inc.	TPE-3500SD-PIV
Identix, Inc.	TPE-4x4XDFS-PIV
Identix, Inc.	TPE-3000XD-PIV
Identix, Inc.	TPE-4x4XD-PIV
Identix, Inc.	TPE-3100XDFS-PV
Cross Match	LScan Guardian
Identix, Inc.	TPE-4100XDFS-PV
Identix, Inc.	TPE-3100XT-PIV
Aware, Inc	PIVSuite SDK, Epson 10000XL (card scan)
Identix, Inc.	TPE-4100XT-PIV
Aware, Inc	PIVSuite SDK with Epson 4490 (card scan)
Aware, Inc	PIVSuite SDK with I3 digID LE flats
Identix, Inc.	TPE-3000XT-PIV
Aware, Inc	PIVSuite SDK with Cross Match Guardian
Aware, Inc	PIVSuite SDK with Cross Match ID700
Aware, Inc	PIVSuite SDK with Identix TP-4100
Aware, Inc	PIVSuite SDK with Identix 4x4
Cross Match	ID 700
Identix, Inc.	TPE-4100XD-PIV
Identix, Inc.	TPE-3500XDC-PIV
Identix, Inc.	TPE-3100SD-PIV
Cross Match	ID 500M
Identix, Inc.	TPE-3100XD-PIV
Identix, Inc.	TPE-4100XA-PIV
Aware, Inc	PIVSuite SDK with Epson 4990 (card scan)
Identix, Inc.	TPE-3000XDFS-PV
Identix, Inc.	TPE-3000SD-PIV
Aware, Inc	PIVSuite SDK with I3 digID LE plain/roll
Identix, Inc.	TPE-4x4XT-PIV
Cross Match	ID 500

OCSP Responder

Tumbleweed	Tumbleweed Valicert Validation Authority
CoreStreet, Ltd.	CoreStreet Responder Appliance 2400
SETECS Inc	SETECS OnePKI OCSP Responder
CoreStreet, Ltd.	CoreStreet Path Builder System
CoreStreet, Ltd.	CoreStreet Validation Authority

PIV Card

Gemalto	SafesITe FIPS 201 w/ HID Prox Card
SETECS Inc	SETECS OneCARD PIV Card
Gemalto	SafesITe FIPS 201 Card
Oberthur Card Sys.	PIV End Point Dual Interface Smart Card

PIV Middleware

Sagem Morpho, Inc.	Sagem Morpho PIV Client API
Actividentity	ActivClient v6.0
RSA Security, Inc.	RSA Authentication Client
SETECS, Inc.	SETECS OneCARD PIV Middleware
ImageWare Systems	IWS PIV Middleware
SafeNet, Inc	SafeNet PIV API
Gemalto	SafesITe FIPS 201 Client API

Single Fingerprint Capture Device

Cogent Systems, Inc.	CSD301 Single Finger Capture Device
Precise Biometrics, Inc.	Precise Biometrics 250 MC
SecuGen Corporation	Hamster IV Optical Fingerprint Reader
Sagem Morpho, Inc.	MSO 350 PIV
DataStrip	DSVII
Cross Match	Verifier 310
UPEK Inc	TCS1
Identix, Inc	DFR-2100-USB2G

Template Generator

Precise Biometrics, Inc.	Precise BioMatch 378 Template Gene
Identix, Inc.	BE6-SDK-PIV, BioEngine SDK
Sagem Morpho, Inc.	MorphoKit
Aware, Inc	Aware XM SDK
Bioscrypt, Inc.	Bioscrypt ANSI/INCITS 378 Generator
Cross Match	Cross Match Template Generator License
SecuGen Corporation	SecuGen 378 Template Generator v3.5
XTEC Incorporated	XTEC PIV/INCITS 378 Generator
Cogent Systems, Inc.	BioSDK 4.1/COGENT BSP

Template Matcher

STARTEK Engineering	STARTEK ANSI/INCIT 378 Template Matcher
Cross Match.	Cross Match 378 Extract & Match
Sagem Morpho, Inc.	MorphoKit
Aware, Inc	Aware XM SDK
Bioscrypt, Inc.	Bioscrypt ANSI/INCITS 378 Matcher
SecuGen Corporation	SecuGen 378 Template Matcher v3.5
XTEC Incorporated	XTEC PIV/INCITS 378 Matcher
Cogent Systems, Inc.	BioSDK 4.1/COGENT BSP
Identix, Inc.	BE6-SDK-PIV, BioEngine SDK

Transparent Reader

Tyco Fire & Security	SWH Multi-Tech Mullion
Tyco Fire & Security	SWH Multi-Technology Reader with Keypad
Precise Biometrics, Inc.	Precise Biometrics 200 MC
Tyco Fire & Security	SWH Multi-Technology Reader
Honeywell	OT35HONA
Honeywell	OT30HONA
Gemalto	SafesITe USB SC Reader (GemPC USB-SW)
OMNIKEY Americas	CardMan 4321 ExpressCard SC Reader
Honeywell	OT36HONA OmniAssure
Honeywell	OT31HONA OmniAssure
Precise Biometrics Inc.	Precise Biometrics 250 MC

Sagem Morpho, Inc.	MSO 350 PIV
Integrated Engineering	Desktop/SmartLOGON Pro OEM Board
Integrated Engineering	800-1086 SmartID OEM Board
OMNIKEY Americas	OMNIKEY CardMan 3021 USB Reader
SCM Microsystems	SCR3340 ExpressCard 54 SC Reader
SCM Microsystems	SCR333 Drive Bay USB SC Reader
Actividentity	Actividentity PCMCIA Reader
Actividentity	ActivIdentity USB v3 Reader
SCM Microsystems	SCR531 Serial/USB S/C R/W
SCM Microsystems	SCR131 Serial Port S/C Reader
SCM Microsystems	SCR3311 USB Smart Card Reader
SCM Microsystems	SCR3310 USB Smart Card Reader
OMNIKEY Americas	CardMan 5321
Farpointe Data, Inc	Delta5.4, Vandal Res. Contactless Reader
SCM Microsystems	SCR243 PCMCIA S/C Reader
Farpointe Data, Inc	Delta5, Single Gang Contactless Reader
Farpointe Data, Inc	Delta1, OEM Contactless Reader
Farpointe Data, Inc	Delta3.4, Vandal Res. Contactless Reader
Farpointe Data, Inc	Delta3, Mullion Contactless Reader
XceedID Corporation	XF2110-PIV
XceedID Corporation	XF2100-PIV
XceedID Corporation	XF1100-PIV
SCM Microsystems	SCR331 USB Smart Card reader
OMNIKEY Americas	CardMan 3821 USB Pin Pad Display Reader
Hirsch Electronics	Card Reader-IE SmartProxPIN-Mullion
OMNIKEY Americas	CardMan 3621 Contact Pin Pad Reader
Hirsch Electronics	Card Reader-IE SmartProx-Mullion
Hirsch Electronics	Card Reader-IE SmartPIN-Mullion
Hirsch Electronics	Card Reader-IE Smart-Mullion
SCM Microsystems	SCR338 Smart Card Keyboard
Farpointe Data, Inc	Delta5.3, Euro Style Contactless Reader
Ingersoll Rand	SCHLAGE SXF2110-PIV
Farpointe Data, Inc	Delta6.4, Sgl Gang Contactless w/ Keypad
OMNIKEY Americas	CardMan 3121
Ingersoll Rand	SCHLAGE SXF1100-PIV
Ingersoll Rand	SCHLAGE SXF2100-PIV
Integrated Engineering	SmartTRANS 125Khz/ Smart Reader w/ PIN
Lenel	IE800-8110-0606
Lenel	IE800-8100-0606
Integrated Engineering	SmartTRANS 125Khz/ Smart Reader
Lenel	Lenel OpenCard PIV Reader XF2110-PIV
Lenel	Lenel OpenCard PIV Reader XF2100-PIV
Lenel	Lenel OpenCard PIV Reader XF1100-PIV
Lenel	LNL-3121
SCM Microsystems	PAT1322 Physical Access Reader
SCM Microsystems	PAT1312 Physical Access Reader
Integrated Engineering	800-1063 Desktop/SmartLOGON Pro
Secure Network Syst.	SNS CRITSEC® CPKR100
Secure Network Sys.	SNS CRITSEC® CPR100
Integrated Engineering	800-8080 SmartID Reader
Secure Network Sys.	SNS CRITSEC® SCE100
Secure Network Sys.	SNS CRITSEC® CKR100
SCM Microsystems	SDI010 Contact/Contactless Reader
Secure Network Sys.	SNS CRITSEC® CR100
Integrated Engineering	800-8085 SmartID Reader w/ PIN
HID Corporation	iCLASS OEM150
OMNIKEY Americas	CardMan 4040 PCMCIA Contact Reader
HID Corporation	iCLASS RP40
HID Corporation	iCLASS RK40
Lenel	IdentityDefender IE800-1063-4023
HID Corporation	iCLASS R40
HID Corporation	iCLASS R30
Lenel	OnGuard IE800-8080-4023
HID Corporation	iCLASS R10
Lenel	OnGuard IE800-8085-4023

SecureIDNews

GSA selects EDS consortium for massive PIV rollout via Shared Service Provider program

Highly sought contract will result in issuance of 400,000 IDs at 40+ agencies

Marissa Torrieri
Contributing Editor, AVISIAN Publications

Vendors who make FIPS 201-compliant products have spent the first quarter of 2007 aggressively courting federal agencies while waiting to see who will get a piece of the anticipated $100 million contract as part of the General Services Agency's Shared Services Provider program.

For months, stakeholders in all corners eagerly anticipated the GSA's announcement of the award for its SSP program. As we prepared to go to press with this issue of re:ID, the award was finally announced. The consortium of companies led by EDS was selected for the five-year. $66 million deal.

As a bit of background, the PIV cards are the key to Homeland Security Presidential Directive (HSPD) 12, which President Bush signed into law in August 2004. HSPD-12 calls for all federal employees to be issued cards based on a technological specification developed by the National Institute of Standards Technology (NIST), known as FIPS 201.

GSA's Shared Services Provider program, which began last August, gives agencies a one-stop-shop for implementing standards-compliant solutions. The SSP program sets up a long-term partnership between the GSA's chosen contractors and federal agencies to help them with card issuance and management of the program.

Under the SSP competitive contract, agencies in the same geographic locations would be able to share required HSPD-12 implementation services and take advantage of GSA's oversight and related management services.

The original $104.6 million contract was first awarded to McLain, Virginia.-based BearingPoint, which helped nearly 40 agencies produce their first cards for the October 27, 2006 deadline. Participating agencies included the departments of Agriculture, Housing and Urban Development, Archives and Records Administration, and Commerce. But the contract ended in December – a BearingPoint spokesman says it "expired" so the government could open up the program to multiple bidders.

As the myriad of players in the game busily fine-tuned their technology, each hoped to be selected to help agencies through the next phase of the PIV project. That next phase involves getting background checks up and running, activating card enrollment centers, and putting final methods of production and distribution into place.

And the winner is ...

The announcement of the award to EDS was made in late April of this year. Other members of the consortium include:
- Northrop Grumman Corp.,
- ActivIdentity Corp.,
- Data Systems Analysts Inc.,
- Identification Technology Group,
- L-1 Identity Solutions,
- Oberthur Card Systems, and
- Tibco Software Inc.

EDS brings a strong background in major government ID issuance to the table. The company was a key player in the Department of Defense Common Access Card (CAC), a standard ID issued to all military personnel, and was responsible for much of the CAC issuance.

But not all agencies will go for the shared service approach

Many agencies with unique needs or other drivers will certainly implement their own solutions outside of the GSA's Shared Services Provider program, says Randy Vanderhoof, executive director of the Smart Card Alliance. But, he points out, "the majority of agencies are planning to use the Shared Service Providers. It's easier for agencies to go through the GSA because they don't need to build internal infrastructure, they just need to link their internal cardholder database to the Shared Services provider that will produce the cards."

Companies that were not a part of the contract will still have plenty of opportunities for work with FIPS 201. Though not a part of the GSA award, smart card chip manufacturer Gemalto's Neville Pattinson, vice president of governmental affairs and standards, says the company is intensely promoting its product line – SafesITe Government Solution, which consists of a comprehensive set of cards and services, all of which are listed on the GSA FIPS 201 Approved Product List.

"We see, over the next couple of years, agencies getting their infrastructure in place," says Mr. Pattinson.

Mr. Vanderhoof agreess, "there's plenty of business out there for other vendors."

REGISTER TODAY FOR OUR BEST RATES!

CardTechSecurTech 2007

17th Annual Conference & Exhibition
May 15-17, 2007
The Moscone Center West • San Francisco, CA

CONFERENCE AGENDA

CTST'S WORKSHOPS DELIVER BATTLE-TESTED SOLUTIONS TO REAL-WORLD PROBLEMS
Each full-day workshop will introduce you to major challenges, outline potential solutions, and provide real world case studies in a key market sector.

TUESDAY, MAY 15, 2007

Introducing: A New Intensive Workshop at CardTechSecurTech
Speaker: Allen Weinberg, *Partner*, GLENBROOK PARTNERS

CT01 - Overview: Advanced Card Payments and EMV
Moderator: Alison Colquhoun, *VP*, EXPERIAN

CT02 - Applying GlobalPlatform Technology in ID & Mobile
Moderator: Kevin Gillick, *Executive Director*, GLOBALPLATFORM

CT03 - Merchant-Driven Alternative Payment Systems
Moderator: David Evans, *Founder*, MARKET PLATFORM DYNAMICS

ST04 - Overview of ID Security
Moderator: Bryan Ichikawa, *Identification Solutions Architect*, UNISYS

ST05 - Emerging ID Security Technology
Moderator: Conor White, *CTO*, DAON

WEDNESDAY, MAY 16, 2007

CT11 - Contactless Payment Technologies
Moderator: Henry Dreifus, *CEO*, DREIFUS ASSOCIATES, LTD.

CT12 - POS and Payment Processing Technology
Moderator: Paul Grill, *Partner*, FIRST ANNAPOLIS CONSULTING INC.

CT13 - NFC and Mobile Payment Technologies
Moderator: Chris Corum, *Founding Partner, Executive Editor*, AVISIAN PUBLISHING

ST14 - Biometric Security and REAL ID
Moderator: Raj Nanavati, *Partner*, INTERNATIONAL BIOMETRIC GROUP

ST15 - Advanced ID Management and Cybersecurity
Moderator: Randy Vanderhoof, *Executive Director*, SMART CARD ALLIANCE

THURSDAY, MAY 17, 2007

CT21 - Contactless Payment Strategies and Markets
Moderator: Sunil Dewan, *Director, Product Management*, FIRST DATA CORPORATION

CT22 - Prepaid Technologies, Strategies and Markets
Moderator: Anil Aggarwal, *CEO*, PREPAID MEDIA

ST23 - Healthcare Card Technologies and Strategies
Moderator: Zack Martin, *Editor*, *HEALTH DATA MANAGEMENT*, SOURCEMEDIA

ST24 - Data and Physical Security Convergence
Moderator: Ray Bernard, *Principal Consultant*, RAY BERNARD CONSULTING SERVICE

ST25 - Authentication and Secure Payment Technology
Moderator: Richard Crone, *Founder*, CRONE CONSULTING

SourceMedia
CONFERENCES & EXHIBITIONS

www.ctst.com
800-442-CTST   212-803-8777

Near field communications is the talk of the ID world, but what will it take to turn the talk to action?

Andy Williams
Contributing Editor, AVISIAN Publications

Every time you turn around you see an NFC pilot program cropping up somewhere in the world. What you haven't seen are many full-scale commercial rollouts. In fact, those could be counted on one hand. Sure, near field communication technology is still relatively new – but in a world where new innovations quickly become yesterday's news, could NFC be starting to show its age?

Developed by NXP Semiconductors and Sony, NFC is a standards-based, short-range wireless connectivity technology that enables simple two-way interactions among electronic devices.

While some industry watchers are suggesting that NFC is slow out of the gate, one research firm has gone so far as to speculate this year

is "critical for NFC technology." New York-based ABI Research predicts that five years from now 20% of mobile handsets – nearly 300 million –will have NFC capability. But that's down sharply from the 25% by 2010 the firm had earlier projected.

Early "enthusiasm for NFC adoption in handsets – fueled by its functionality and flexibility – has been tempered by the complexity of the ecosystem," the company said in a statement released to promote this latest report.

ABI claims that NFC will not become widely available in handsets until wireless operators are confident that they will see a clear return on their investments, calling mobile operators the "gatekeepers of NFC's entry into new handsets."

The *Original* Multi-Technology Readers

125 kHz
PROX

13.56 MHz
SMART

**FIPS 201
PIV II**
US GSA APL

The Most Versatile, Secure Readers in the Industry

XceedID ®
Xceeding The Ordinary

To learn more please visit: www.xceedid.com

Others remain upbeat, still bullish on the progress

NXP, one of NFC's developers, would beg to differ both in the number of handset makers who are getting more involved and in the requisite infrastructure.

"There's too much on the plate, but that's fortunate," said Dave Holmes, NXP business development manager for NFC. "There is so much activity going on with handset integration. There's been a monumental shift in the level of interest and the work being done. What we're focused on is the execution stage, making it happen."

Mr. Holmes said a few "are really pushing, innovating and most likely will be the first out of the gate with NFC handsets. Others are sitting back and waiting to see. The good news is that some of the leaders are some of the biggest names in the business. You've seen some of the trial activity, Cingular in Atlanta, and the New York City transit trial." Many handset makers are beginning to get involved. "It's kind of a who's who of handset makers and carriers," said Mr. Holmes. Added to the mix are Visa in Atlanta and MasterCard in New York, he points out.

He said the first commercial rollout in Hanau, Germany, for transit, "proves that (NFC) works and users really liked it and wanted it. What I think will be the next big thing to make it explode are payment applications in the U.S. and transportation applications in Asia."

Most of the trial activity so far has been with low-end or mid-tier phones. "That's designed to test it with mainstream users. It's not something that requires a professional user," said Mr. Holmes.

He added, "from my perspective, we don't need to go much further. Now that it's chugging away, we've settled into our core competency, hardware and software."

New specs refine tag formats, define peer to peer communication, and more

The NFC Forum was created in 2004 and has grown to more than 110 members, including leading mobile communications, semiconductor and consumer electronics companies. The forum's mission is to advance NFC use by developing specifications, ensuring interoperability among devices and services, and educating the market.

Martin Buehrlen, NFC program manager for NXP and secretary of the NFC Forum, said that while the organization has already created some up-front specs designed to encourage NFC implementation, its work is far from done.

"We're finalizing a few more technical specifications regarding support for the tag formats (the tags go on smart posters and coupons to be read by NFC-enabled devices). There was an announcement a year or so ago saying that there's a list of tags which are readily available in the market and that NFC Forum supports these tag formats," said Mr. Buehrlen. "These are easy and cost-effective with existing solutions so manufacturers don't have to make new transponders with NFC," he added. Bottom line is that "the NFC Forum decided to be compliant with existing tag formats." These specs are already in the voting process and should be ready soon.

"Other specifications being worked on are focusing on the peer to peer communication between NFC devices and mode switching, utilizing an internal switch so the device can operate in several modes -– card emulation mode, card reader mode, peer to peer mode," he added. "They're on the schedule (for adoption) this year. We also need to provide the test specs for all the other specifications available in order to establish the compliance program. When you have specs you also need to have a way to test devices in order to make sure they're compliant."

The forum doesn't want the consumer to have to think twice before he whips out his cell phone to make a payment or place it near a smart tag to download some information.

With payments, he said, "in many cases we're already covered with existing specifications. In some areas this is outside the NFC Forum. What's covered is the RF (radio frequency) level and the protocols" such as ISO. "When it comes to higher level protocols and how software works with credit cards, those (protocols) are available from Visa and MasterCard and others."

Where the NFC Forum is involved, he added, is with the communication from the NFC chip to the smart chip in the mobile phone. "This is being worked on now but it's not something that's waiting for implementation because Visa already has a system with NFC in New York and it's running based on existing technologies, no new specifications," said Mr. Buehrlen.

In search of ROI

In answer to ABI Research's comment about a business case for NFC, Mr. Buehrlen says, "there are a lot of business models which are possible with NFC but it does require a certain investment by the companies

who want to benefit. If you want to do payment with NFC you need to have an investment in payment terminals. If you want to have a revenue stream (a mobile operator, for example) with respect to downloadable content, then the infrastructure for the consumer to pick up this location-based content needs to be established. The same goes for advertising. When you use NFC in combination with smart posters and product info, you need to build up a certain infrastructure. This is a very normal situation in new technologies."

He said it would help "if more companies would decide to go for a bigger rollout and a faster rollout then what we have seen so far."

He cites, as an example, Japan, that has shown that such business models pay off. "More companies are jumping on the train with public transport tickets. There are a lot of payment schemes and loyalty schemes and voucher applications. There are several public transport operators using the mobile phone for not only transit, but for numerous loyalty schemes. Small stores, not chains, but individual restaurants, can have their own loyalty schemes based on this. It's proof that you can make money with this kind of technology."

Shortage of handsets and models continues,
but help is on the way

"The variety of different mobile phones with NFC support at this time are not sufficient (when compared to) what consumers are used to getting when they go into a store to select a phone," says Mr. Buehrlen, "but this is really increasing and improving."

He cites the forum's increasing membership as an example. "A lot of cell phone manufacturers are members, including a lot of the big ones. Research in Motion (RIM), Blackberry inventor, has come aboard. "The very encouraging part is that so many companies which are in the business of mobile devices are members."

One of the founding members of the NFC Forum and one of the leaders in producing NFC-compatible phones is Nokia, which, earlier this year, released its latest phone, the 6131, at the Consumer Electronics Show. Attendees got a chance to view its use, including swapping business cards by tapping two NFC phones together, buying coffee, and more.

Calling the 6131 an extremely positive development for NFC, NXP's Mr. Holmes states, "from my point of view, at least from the U.S. development stage, it gives carriers an option with a nice looking, high end, full featured phone."

He adds, "major carriers can request a phone and have it pretty quickly. It opens doors to some of these smaller carriers to have an NFC phone option."

Gerhard Romen, head of marketing development for Nokia in Finland, said the 6131 is a mass volume device. "Going from pilot to deployment will only happen step by step. We see a three to five year development period. We'll start in high density areas and evolve from there."

Nokia views the phone as a mini computer

Mr. Romen said he was in a meeting recently with about 100 people. "I asked everyone if they had a mobile phone and for how long. Most started between 1994 and 1998. The prime application was voice but there has been a huge evolution with texting, SMS, Web browsers, then the introduction of Java on mobile phones. From Nokia's point of view, the phone is now a mini computer with a full-blown operating system with a keyboard. There are more than two billion users globally who now have Internet connections … they can use eBay. All of a sudden you have much more than a phone."

He added: "From our heritage at Nokia, we focused on a simple user interface. That's what brought us into NFC. Back in 2001 we studied user behavior. We felt this touch and point was a powerful thing, not intrusive, something you could do (and) if we combined the phone capabilities with that touch paradigm … that would be powerful. We looked at other technologies, including bar codes, and ended up with NFC."

Mr. Romen is obviously excited about the potential applications for NFC. "Visa and MasterCard are working with Nokia to make the phone a fully functional credit card. Just tap, and you've paid," he says. But it "offers more than just your credit card. You can confirm the payment before it happens, or you can check your balance first before you make payment."

In the U.S., he points out, the contactless infrastructure is already there. "We're just complementing or replacing it. Then you add things like posters or a contact point on your washing machine where you could view the manual on how to operate it, again the touch paradigm, or open hotel doors with your phone. You're already pre-booked, you have your key on your phone and you can go straight to your room. Airlines could also do that with check-in."

He uses an analogy to explain NFC's future. "Think about the key you use for your car … you know you have to insert it under your steering wheel and turn it. Have you ever wondered how many things start happening when you turn the key? The engine and all its moving parts, start up. If you have GPS, it starts. All that is simplicity. You turn it on and it is all available. That's similar to what we're trying to do with NFC."

European consortium created to foster NFC interoperability

StoLPaN group includes heavy hitters in tech, finance, and education

Andy Williams

Contributing Editor, AVISIAN Publications

Europe is looking to get a head start on creating an NFC ecosystem, thanks to the recently announced creation of a new consortium with the unlikely acronym, StoLPaN. It stands for Store Logistics and Payment with NFC and includes a pan-European consortium of companies, universities and user groups seeking to develop an open architecture for the development, deployment and use of NFC-enabled applications in mobile handsets. It is co-funded by the European Commission and the Information Society Technologies (IST) program.

The three-year project is expected to define the business rules and technical specifications required for the successful commercial deployment of third party applications into NFC-enabled mobile devices. These standards will then be submitted to the relevant trade bodies for adoption by the payment, mobile, transit and ticketing industries to create a standardized NFC ecosystem. The project is expected to establish a smart retail environment including support devices and business processes to demonstrate the new solutions.

"We started drafting this project two years ago," said Francisco Prato, NXP Semiconductors' business development manager for NFC. "The European Union (EU) gave us the funds (because it) liked the proposal." Any project the EU funds must be based in Europe and usually lasts three to five years, he added. StoLPaN, while initially given a three-year life span, could be expanded another two years. There are currently 16 companies involved in the consortium.

"We want to create an ecosystem for the end user to use NFC," said Mr. Prato. One of the biggest concerns is interoperability. It's the same thing that initially occurred when credit cards were issued. They each needed their own reader. "Nokia will not interoperate with Motorola phones, and so on, so one of our objectives is to look at interoperability issues. We'll be looking at different projects around the world, focusing on the European market and make recommendations on how the different systems can work together."

"We'll define the framework, a set of rules that if the company follows will guarantee a degree of interoperability," added Mr. Prato. "If you develop applications for Motorola phones and follow the rules you'll be insured interoperability. The same applies for the ecosystem," which he defines as "the applications and all the things you need to know to run the applications."

He said StoLPaN is looking at payment, ticketing, loyalty and the fact that payment requirements in Europe are different than in the U.S.

But StoLPaN will not write standards. "We'll issue recommendations," says Mr. Prato. "People think we're a regulatory body … that we're going to write standards. That's not the case. What we're doing is looking at the market to see what going on, to define the framework for interoperability for the industry. Companies should look at it as a tool and not as a competitor."

Implementing test cases to understand the NFC ecosystem

Right now, he said, StoLPaN, a member of the NFC Forum, is still studying the market. "We're collecting information on existing systems. The next step will be looking at these systems, how these applications are being deployed in the field and the interoperatiblity of the phones involved. The next stage is once we issue some recommendations, we'll implement one or two test cases, small tryouts."

In order to accurately address the interoperability issues currently affecting the technology, various use cases are to be defined within the StoLPaN framework and tested throughout Europe. These use cases will contribute to the identification of a common set of business rules, which will define the roles and responsibilities of every player in the NFC ecosystem.

Based on these findings, the consortium will then look into the specifications for technical requirements and the security aspects of NFC-enabled applications. They will also explore the connection to existing contactless platforms, attempting to ease the burden on individual providers. At the same time the project team will demonstrate how the business rules and technical requirements can be implemented in existing contactless infrastructures, Mr. Prato said.

While transit ticketing with NFC is big in Europe, StoLPaN also wants to track deployment of NFC in the retail environment. "In this case, you can use the phone not only to track items in a supermarket but to pay for these items."

In this "store of the future," a shopper would place items in the cart, tracking (and paying for) them with the phone. "You simply exit the market through a gate, which will read that everything you've placed in the cart has been scanned," Mr. Prato added.

The consortium members involved are Motorola, NXP, Auto-ID Lab St. Gallen, Banca Popolare di Vicenza, Bull, Baker&McKenzie, Consorzio Triveneto S. P. A., Consult Hyperion, Deloitte, Fornax, Libri, Safepay Systems, Sun Microsystems, T-Systems, as well as the Budapest University of Technology and Economics and Budapest Tech John von Neumann Faculty of Informatics.

On Your Desk

On Your Desktop

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

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

AVISIAN

The technical basics of Near Field Communications

Understanding why NFC is more than contactless, Bluetooth, or RFID ...

Certainly among the hottest of topics in the ID world today is Near Field Communication (NFC), an exciting and relatively new technology. While it has become a household term in most identification-centric circles, a significant gap in understanding of its technical operations and capabilities remains. Ask a number of people to define NFC, and you are likely to get responses like: 'It's a way to make payments with your mobile phone' … 'It's contactless but it can go in a other devices' … 'Its like Bluetooth but it is in a card." While each of these descriptions are accurate to a degree, they fail to capture the true understanding of what sets NFC apart from other technologies.

NFC's industry association, the NFC Forum, defines the technology as "a standards-based, short-range (a few centimeters) wireless connectivity technology that enables simple and safe two-way interactions among electronic devices, allowing consumers to perform contactless transactions, access digital content and connect electronic devices with a single touch."

Put another way, it is a standard that enables contactless, bi-directional communication between devices. These devices can be NFC-equipped mobile phones, computers, consumer electronics, cards, tags, signs, posters, washing machines … virtually anything that can be tagged.

NFC standards are the result of work conducted by Ecma International, a global industry association dedicated to the standardization of technology and consumer electronics. The NFC effort was initiated within Ecma by the creators of the technology, Sony and Philips (now NXP). The standard created by Ecma was titled ECMA-340 and it was subsequently submitted to the International Organization for Standardization (ISO) for consideration. ISO adopted it as ISO/IEC 18092 in October 2003.

ISO/IEC 18092 details the modulation, coding, data transfer speeds, anti-collision, data exchange, and other technical operations that enable standardized operation across NFC devices.

NFC is closely related and complementary to other contactless technologies with which it shares the 13.56 MHz frequency band. Specifically, the popular ISO 14443 standard is a key building block for much of the Near Field operations. NFC is compatible with the ISO 14443 Type A and B standards, NXP's Mifare, and Sony's FeliCa technologies.

Initiators and targets

NFC splits the components of a communication session into initiators and targets. The initiator is the device that begins and manages the communication and exchange of data. The target responds to requests from the initiator. This is where one of the key qualities of NFC comes to light: devices can act as either an initiator or a target.

In traditional RF systems, a device is either an initiator (called a reader or interrogator) or a target (called a card, token, or transponder).

Establishing protocols for devices to act in either role enables bi-directional establishment of communication and enables devices to function as what is commonly referred to as 'either the card or the reader.'

How does NFC compare to other wireless/RF technologies?

Near Field Communication (NFC) is a standards-based, short-range (a few centimeters) wireless connectivity technology that enables simple and safe two-way interactions among electronic devices, allowing consumers to perform contactless transactions, access digital content and connect electronic devices with a single touch.

Bluetooth wireless technology was designed to replace cables between cell phones, laptops, and other computing and communication devices within a 10-meter range.

Wi-Fi technology was designed and optimized for Local Area Networks (LAN); it provides an extension or replacement of wired networks for dozens of computing devices within a +100-meter range.

ZigBee wireless technology is a standard enabling control and monitoring capabilities for industrial and residential applications within a +100-meter range.

IrDA is a short range (< 1 meter), line-of-sight communication standard for exchange of data over infrared light. IrDA interfaces are frequently used in computers and mobile phones.

RFID (Radio Frequency Identification) is an automatic identification method, relying on storing and remotely retrieving data using devices called RFID tags. An RFID tag is a small object that can be attached to or incorporated into a product. RFID tags contain silicon chips to enable them to receive and respond to queries from an RFID reader/writer.

Contactless smart cards incorporate a chip (microprocessor) that communicates with a card reader through RFID technology. Examples of contactless smart card communications are ISO/IEC 14443 and FeliCa, which allow communications at distances up to 10 cm.

Source: NFC Forum, Frequently Asked Questions, 2007

The single industry voice for smart cards ...

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

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

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

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

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

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

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

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

Advanced ID Management and Cybersecurity
A Smart Card Alliance Educational Institute Event

NETWORKING

At the CTST Conference • Wednesday, May 16, 2007 • 9 am - 4:30 pm

9-10:30 am	Smart Cards and ID Management Infrastructure
10:45-12 pm	Managing Identities Across the Enterprise
1:45-3 pm	Card Management and Identity Management Solutions
3:15-4:30 pm	Use Cases for Enterprise and Mobile Authentication

Come learn from the industry's most influential payment card leaders!

WORLDWIDE OUTREACH

UNRIVALED EDUCATION

TASK FORCES & REPORTS

CONFERENCES

A sampling of NFC pilots from around the world

With trials occurring at a fevered pace, NFC is being tested for real world use

USA: Cellular South and Kyocera Wireless conduct NFC payment trial of "Wireless Wallet" with consumers in Memphis, TN and Jackson, MS. End date: August 2007.

The Netherlands: Roda Stadium trials NFC phones for football ticketing and payment with KPN, Philips, Bell ID, SmartPoint. Dates: Aug 2005-May 2006

Taiwan: MasterCard, Taipei Fubon Bank, Taiwan Mobile, and Vivotech deploy NFC pilot in Taiwan for payment and couponing via smart posters. Start date: February 2007.

USA: Citi, MasterCard, Cingular, and Nokia conduct NFC payment trial using phones with PayPass in New York City. Start date: January 2007.

Germany: Nokia, Philips, Rhein-Main Verkehrsverbund trial NFC ticketing for public transport in Hanau/Frankfurt. Start date: April 2005

USA: Visa tests delivery of coupons and rewards to NFC-equipped phones with 500 of its employees in California. Start date: November 2006.

France: City of Caen trials NFC for payment, parking, tourist / transit information via smart posters. Participants include Philips, France Telecom, Orange, Samsung, Groupe LaSer and Vinci Park (retailers). Dates: Oct 2005-May 2006

France: Grenoble trial sees participants pay fares for public transport. Start date: March 2007.

USA: Mastercard, Verizon Wireless, and Motorola conducted a trial of NFC phones and PayPass technology in Dallas. Start date: November 2004.

China: China Mobile, Philips, Nokia, and Xiamen e-Tong Card trial NFC payments with 100 participants in the city of Xiamen. Start date: July 2006.

United Kingdom: Manchester City Football Club trials NFC for stadium ticketing and payment. Start: August 2006.

France: Strasbourg trial demonstrates contactless EMV transactions via mobile phones with Groupe Crédit Mutuel, CIC, NRJ Mobile, MasterCard PayPass, and Inside Contactless. Start date: November 2006.

Austria: University of Applied Sciences of Upper Austria conducted a trial of 100 students and staff using NFC phones for payment at vending machines, peer to peer transfer, and access. Start date: November 2006.

Malaysia: Visa, Maybank, Maxis and Nokia trial Visa Wave payments with 200 participants. Dates: April 2006 - Aug 2006

USA: Philips Arena in Atlanta pilots NFC for payment and poster download with Atlanta Spirit, Chase, Cingular, Nokia, Philips, Visa USA and ViVOtech. Dates: Dec 2005-June 2006

Korea: SKTelecom and Philips trial NFC with 400 SKT employees in Seoul. Applications include access control, smart posters, ringtone download, payment. Start date: June 2006.

The Netherlands: In Amsterdam, JCB trials NFC payments with 100 participants. Start date: September 2006

France: The Paris Metro, Inside Contactless, and Bouygues Telecom enable pilot participants to use an NFC phone to pay fares as a complement to the contactless Navigo card. Start date: April 2006.

The significance of this dual-role capability is best explained with an example. Imagine a restaurant scenario where a diner and waiter are settling the check. The diner holds out his contactless card and the waiter simply touches it with his NFC-equipped device (e.g. PDA, point of sale add-on, mobile phone) that is functioning as a 'reader.' The waiter captures the payment info and the customer verifies it on the device and adds a gratuity. The waiter walks back to the main counter and touches the device to the central point of sale (POS) reader. The waiter's device then switches to 'card' mode as the central POS reads the payment information for processing.

The same device, the waiter's handheld, has functioned as both a contactless reader and a contactless token to complete the transaction. This is one of the elegant features of NFC that open doors for functionality never before possible.

As the NFC Forum describes it, "an NFC-enabled device can operate in reader/writer and peer-to-peer mode, and may operate in card emulation mode."

Passive and active NFC modes

Another important feature of NFC is that it defines two distinct modes of communication. In the active mode, both devices are responsible for creating the RF field to carry data. In the passive mode, only the initiating device creates the RF field. This enables battery-powered devices, such as mobile phones, to avoid power consumption at the RF level during periods of inactivity.

The benefit of ease of use

According to Ecma, the short-range nature of NFC is optimal for its application. Because NFC devices must be no more than 20 centimeters apart for operation (most agree actual distance is smaller in operation), the "touch" metaphor applies. This means that devices must, in essence, touch each other to establish communication. Ecma notes the following benefits:

• "Devices can rely on the protocol to be inherently secured since the devices must be placed very close to each other. It is easy to control whether the two devices communicate by simply placing them next to each other or keeping them apart."
• "The procedure of establishing the protocol is inherently familiar to people: you want something to communicate – touch it. This allows for the establishment of the network connection between the devices to be completely automated and happen in a transparent manner."

Initial applications

NFC developer Innovision cites peer-to-peer, payment and ticketing, and service initiation as the three initial applications that will drive NFC's growth. It describes these applications as follows:

In peer-to-peer applications, NFC can set up a separate wireless connection via Bluetooth or WiFi. Typical peer-to-peer applications are printing photos straight from a digital camera, establishing an Internet or network connection, transferring files between devices, or sharing electronic business cards.

Initially, NFC-enabled devices are likely to be used for low-fraud, limited-value payment situations, such as quick-serve restaurants, kiosks, vending machines and parking meters.

Service initiation applications use NFC to transfer a small amount of information to the NFC device (e.g. text, a web address (URL), phone number). Smart posters direct the device to a web site for info, to book tickets, or access video or audio files without the need to key anything into the phone to open the browser or input the URL.

Boston's new contactless CharlieCard makes commuting easier for a million daily riders

Andy Williams
Contributing Editor, AVISIAN Publications

A transit card named after a character in a folk song has to carry with it a coolness factor. And, since the Kingston Trio made the song famous way back in 1959, why not have the group on hand when the card is first announced? And so it was when the CharlieCard, a contactless transit card for the Massachusetts Bay Transportation Authority, made its first appearance late last year, its name the result of a survey taken by the Boston Globe.

The CharlieCard is named after the title character in the 1948 folk music song, "Charlie on the MTA," written to protest a fare increase in the form of an extra five cent exit fare. Charlie didn't have the nickel it took to get off the MTA so, as the song goes, "...he was fated to ride forever 'neath the streets of Boston..."

It wasn't the only name suggested in the newspaper survey. Others included the "Fare Cod" derived from the way Bostonians pronounce "card," the "TGo Card" with the "T" the symbol for MBTA, and the "Bean Card," since Boston is also known as "Bean Town," as in Boston baked beans.

"But we didn't want to isolate it to Boston," said Scott Henderson, Massachusetts Bay Transportation Authority's systems project manager. "We service all of Massachusetts."

"We contacted the Kingston Trio, (and) they came out and performed it when we kicked off the name in November 2004," said Mr. Henderson. According to news reports, Massachusetts Governor Mitt Romney also participated in that sing-along.

Founded in 1896, MBTA's transit system is the country's oldest and fifth largest mass transit system as measured by ridership. The MBTA serves 175 communities, providing transit alternatives to a population of almost 4.7 million people over an area of 3,200 square miles. The authority serves 1.1 million passengers per day. To provide these services, the authority maintains 204 bus routes serviced by 1,200 buses, four rapid transit lines of heavy and light rail, one bus rapid transit line, four trackless trolley lines, 11 commuter rail lines, five ferry routes, and a paratransit service.

Host of reasons lead to the technology upgrade

By the mid-90s, MBTA knew it had to upgrade its antiquated fare collection system. "With our turnstiles, most of the manufacturers were out of business. It was hard to get parts. Fare evasion was also a major issue. And we wanted a better customer service presence," said Mr. Henderson.

Describing the speed at which the CharlieCard rollout occurred, Mr. Henderson states, "we shocked ourselves and the industry. We went from a token system with collectors to a stored value, ticket-based system, converting over 75 subway stations and more than 2,000 fare boxes." While installing a new infrastructure took a little longer, the cards themselves were produced and distributed in under three months.

Pre-encoding cards at the factory expedites issuance

A key to the quick release of the cards was that they were pre-encoded by MBTA's card supplier, Gemalto. The company issued some 2.4 million cards in the first three months, said Manny Menard, business development manager for Gemalto North America. "We were awarded the contract last July," and by December, distribution began, said Mr. Menard.

It intends to issue another 1.1 million over the life of the contract. Gemalto also has other transport projects around the world, including the Netherlands, Paris, London, Sao Paulo and Santiago.

Mr. Henderson admitted that MBTA was originally skeptical "about having someone else encode our card. We were looking at issuing the cards slowly, but with our new fare increase, we needed to get something out right away."

"Gemalto's role is to provide cards that are fully encoded and ready to go," said Mr. Menard. Well, almost. "Cards right out of the box will work with the (MBTA) equipment, but they have no value," he said.

Additional benefits arise from the new program

One major advantage to the new card is that "we were able to move our collectors out of the booths,º and they became customer service representatives, helping customers work the machines," noted Mr. Henderson.

If a card is lost or stolen, MBTA can also "hot list" a card, which locks it out of the system.

MBTA offers a corporate program that companies can utilize for their employees. "We have 2,000 corporations that have signed up," said Mr. Henderson. Previously, MBTA had to send out passes to the companies each month. Now, one card takes care of everything. "We've saved $20,000 a month just on the shipping bill. Plus there were all those man-hours to package the passes each month." MBTA has distributed 100,000 CharlieCards to these corporate customers. "Once we do commuter rail, that will grow," he said.

What's next for the CharlieCard?

"We need to do commuter rail. We'll probably be doing that this summer," said Mr. Henderson. Because there are more than 130 commuter rail stops throughout the state, building up the infrastructure could be time-consuming. "We're looking at different options (including) handheld validation as a possibility aboard the trains," he added.

A web site is currently under development as well, which will allow CharlieCard holders to add value, check schedules, etc. If value is added, the next time the card is used, it will be updated. "We're looking at doing this sometime this year," Mr. Henderson said. "Once we have the website up and running, you'll also be able to opt in, so if your card drops below $5, we'll automatically load it up for another $20."

So far, customer feedback has been "very positive." Boston is, after all, "very tourist oriented," added Mr. Henderson.

So if, while riding the MTA, you happen to run across Charlie, slip him his namesake card and 'get him off that train.' Both he – and the Kingston Trio – will appreciate it.

Mr. Menard believes Gemalto was selected "because of the services we could perform, such as doing the actual encoding here in the U.S." The CharlieCards are produced in Gemalto's Montgomeryville, Pennsylvania, facility, and as Mr. Menard points out, "transit agencies do make 'buy American' as part of their contract."

He said some transit agencies "take it upon themselves to do the encoding process, but having us do it saves them money. (MBTA) didn't have to buy encoding equipment. One piece costs between $500,000 and $800,000, plus you have to train the staff. We can do high volume because we have the equipment to do it."

He added, "if an agency chooses to do its own encoding, it is probably not as secure as we are. We're Visa- and MasterCard-certified. MBTA had to rapidly deploy 2.4 million cards. There was no way they could handle that internally. The agency has done a fantastic job getting the largest number of cards (distributed) in a short period of time. They focused their efforts on distribution and allowed us to perform the other pieces of the puzzle."

Limited distribution of the CharlieCard began in mid-2006 to senior citizens, disabled riders, and reduced and free-fare customers, but the full-scale rollout didn't begin until December 2006. In January 2007, MBTA started "flooding the market" with the CharlieCard, and to encourage its use, riders incurred a surcharge if

they used cash to buy their tickets. Using the CharlieCard, says Mr. Henderson, "they could save 30 cents per ticket on the subway and 25 cents on the bus."

The contactless card can contain up to $100 stored value to purchase tickets. But the card can also track MBTA's massive menu of other riding options. "We have 50 different types of monthly passes we sell, including time-based passes," said Mr. Henderson. "A number of those are available on the CharlieCard. It's designed to have two purses for the time base product and one for cash." The card is also designed for expansion. "We took 50% of the real estate on the card. That leaves 50% available for future use." That could include parking "sooner or later" and merchant use. "If Dunkin' Donuts wanted to team up with us and use the card, they could."

The card uses a 1K MIFARE chip from NXP. "We've delivered 100 million cards in transport, and a good portion of that has been MI-FARE," said Mr. Menard.

German-based Scheidt & Bachmann, a provider of management systems for mass transit and car parking, oversees the MBTA project from its U.S. office in Burlington, Mass. The contactless readers are supplied by On Track Innovations, Fort Lee, New Jersey.

CardTech SecurTech showcases
great lineup for May 15-17 event

Near field communication is still, technically, in its infancy, but it's gaining a good head of steam as illustrated by this year's edition of the CardTech SecurTech event. The show is being held May 15-17 at the Moscone Center in San Francisco. Bill Rutledge, CTST program director, projects a 15% increase in attendance over 2006 figures for the SourceMedia Conferences and Exhibitions event.

Why go? "There's a lot going on in security and on the payment side," said Mr. Rutledge. "For people in the payments industry, there's a lot to be aware of. On the security side, the big effort now is on protecting data and managing identity."

Focusing on these issues and more will be 15 workshops as well as the CardTech Americas Executive Summit that will feature an hour-long Q and A with key officials from Gemalto, Giesecke & Devrient, Oberthur, and Sagem Orga, added Mr. Rutledge. "Attendees will be able to ask whatever they want." In addition, a well-known security expert, former FBI Director Louis Freeh, who is credited with transforming the FBI from a national law enforcement agency to a global security institution, will be a keynote speaker.

A few years ago the show, now in its 17th year, was dominated by security, particularly after 9/11 and the subsequent issuance of HSPD-12 and FIPS 201 standards. Then, contactless made its big splash but stepped aside while everyone rushed to get on the ID security bandwagon.

Then along came near field communication, a co-developed technology of NXP and Sony, to reawaken interest in contactless applications. It has caused an "increasing focus on contactless," said Mr. Rutledge.

CardTech

This year, the CardTech portion of CTST will be "focusing on NFC and other mobile payment technologies," he added. A full day will be devoted to NFC. That will include a look at some of the trials currently underway, including the Dallas, Texas consumer trial initiated by MasterCard and a Bank of America "internal test" with its employees, where they were issued NFC-enabled phones, said Mr. Rutledge.

"A lot of vendors are talking about this new technology," he added. These vendors include not just credit card issuers or chip makers, but wireless carriers as well. And there's more to mobile payment projects than just NFC. There's one "payment scheme that will allow you to call up, enter a number and transfer money via a phone line," said Mr. Rutledge. "A lot of smaller companies are experimenting with that."

Along with NFC market projections from Ginger Schmeltzer, manager of Edgar Dunn and Co., and market opportunities in telecom-based payments by NXP's Manuel Albers, the NFC/Mobile Payment Technologies session will also include a look at Visa's pilot mobile payments programs and an "Update on NFC Reference Design" by INSIDE Contactless and a look at SIM-based NFC services from Gemalto.

There are also what Mr. Rutledge calls "merchant driven alternative payment systems, like PayPal that allows merchants to go beyond major credit card vendors to offer payment systems that don't have anything to do with MasterCard or American Express. That's started to take off in a lot of areas. Whether its online or over the phone, alternatives to different payment systems will be some key topics," he said.

May Kay Bowman, Senior Manager, Global Payments for Amazon.com, will discuss "The Retailer Rebellion," while a Verizon representative will talk about the "Move to Mobile." Under the heading, "Battle of the Systems," a panel discussion will include representatives from First Data Commercial Services, Gratis Card, Tempo and Yodlee.

With these alternative payment systems also comes different card form factors, he added.

A section titled "Battle of the Form Factors" will include panelists from Cardinal Venture Capital, iCache, and Aliaswire.

The CardTech portion will also feature an update on EMV migration, particularly in Canada. Catherine Johnston, President and CEO for ACT Canada, will head a panel discussion featuring representatives from the Bank of Montreal, Interac (the country's national automated banking machine and POS debit sale network), MasterCard Worldwide and the Visa Canada Association.

There will also be an EMV case study, "Deploying a Full Grade EMV Card and Acceptance Network," a look at "Contactless EMV: Finding its Place in the U.S. Market," and "The Role of EMV in Fraud Mitigation."

Another daylong session will cover contactless payment strategies and will look at those of Visa and MasterCard, Wells Fargo's contactless card rollout, American Express' contactless card, and "Consumer Perceptions versus Realities."

SecurTech

The other half of CTST, security, won't be outdone. "We've always talked about security at the card level. We have a new workshop called 'Advanced ID Management and Cybersecurity,' where we'll be talking about network security, management of digital IDs, public key encryption," said Mr. Rutledge. This Smart Card Alliance-produced session will include representatives from Gemalto, Microsoft, Actividentity, Verisign, Lockheed Martin, GSA, Intercede, the Department of Defense and CoreStreet.

Some of the topics include: ID management on desktops and servers, managing the identity on the credential, shared services for ID man-

agement, the DoD's Common Access Card and mobile credential management for first responders.

"We'll be talking about the system holistically, taking it to a new level in terms of network ID, managing security life cycles, etc.," said Mr. Rutledge. "This will be a very intense workshop."

There will also be half-day sessions, back-to-back, covering biometrics security and the Real ID Act. Sponsored by the International Biometric Group, the biometrics portion will include what the federal government is doing with biometrics, consumer acceptance of biometric technology, and an update on biometric testing and technology. The Real ID portion will cover what some of the states are currently doing to comply with the act, a panel discussion on "obstacles and opportunities" to Real ID Act implementation, and some of the "benefits and challenges" to the Real ID Act. A panel discussion will feature representatives from the American Association of Motor Vehicle Administrators, California's DMV, Department of Homeland Security and Digimarc.

Two other daylong sessions in the SecurTech track will cover Healthcare Card Technologies and Strategies and Data and Physical Security Convergence.

The former will feature speakers from Accenture, IBM Research, Healthmeans, G&D, Siemens and Gemalto and will include a look at healthcare cards market projections, open technology standards, best practices in healthcare card implementation, and case studies on the Taiwan health care card, the Texas Medicaid Access Card and the French health care card.

The data/physical security convergence session will include speakers from the City of Vancouver, Symantec, Intel, the Boeing Company, Identity Alliance and Unisys and will feature global security management, interoperability standards for security convergence, case studies in convergence engineering, ID token technologies for converged security, and more.

A daylong session on Authentication and Secure Payment Technology for executives will include speakers from Crone Consulting, Javelin Strategy and Research, Volubis, mSystems, Magtek, eFunds Xiring, and IBM Canada.

curTech 2007

First cross-campus interoperable card program a success for Boston's Colleges of Fenway

Andy Williams
Contributing Editor, AVISIAN Publications

Six colleges, located around Boston's famous Fenway Park, have something in common besides their affinity for the Boston Red Sox. Their student campus cards can be used interchangeably among the six schools. It took a consortium to make that happen, as well as a card company with the technology and expertise to meet the consortium's unique needs.

"It's one of the coolest and most dynamic projects I've ever worked on; it's innovative on many different levels," commented Taran Lent, Vice president of Product Development and Management for CardSmith, the company that installed the card system for the Colleges of Fenway.

The Colleges of Fenway, a consortium of six colleges established 10 years ago, "was created for just this type of opportunity," said the consortium's executive director, Claire Ramsbottom. Its members are Em-

manuel College, Massachusetts College of Art, Massachusetts College of Pharmacy and Health Sciences, Simmons College, Wentworth Institute of Technology, and Wheelock College. Five are private; only Massachusetts College of Art is public, she added.

"These are very distinct institutions. Emmanuel College is a Catholic institution founded in the early 1900s," she added. "Simmons has an all women's undergraduate college. Wentworth focuses on technology. They're all very different institutions with long standing heritages."

"When the presidents (who serve as the organization's governing board) created the consortium, they wanted to enhance opportunities for students, staff and faculty," said Ms. Ramsbottom. One of the first opportunities they put in place was the ability for students to cross register for courses between the colleges, with no additional tuition charged.

Other opportunities include an intramural program for the six institutions. "It would be difficult to for each campus to sustain an intramural program on their own. Together, we have over 2,000 students who participate in that program. We also have an orchestra, and we've launched a dance program, things that colleges want to do. By coming together we can build the critical mass to do it more effectively," she said.

Origins of the Fenway Card program

Instead of each of the six schools with student populations ranging from 700 to 2,800 handling the purchasing, staffing and operation of their own campus card programs, the consortium brought in CardSmith to implement a global program connecting all six campuses.

"The beauty of our arrangement with CardSmith is that it allowed our smaller colleges to do things they normally couldn't have done."

She noted that a shared card system started as a discussion among the schools' IT directors and some of the chief financial officers. "We had built a fiber optic network which connected the campuses. That allowed us to significantly increase the bandwidth. When we were building that network, we had a lot of discussions about other opportunities. Technology seemed the key and a card system was one of the items put on the table. At that time, two of the colleges had invested in proprietary systems. One realized it needed a significant upgrade and that was when we looked at having one card program for all six institutions managed by a joint card office."

She said the consortium wanted the students to have something portable so that "they could eat in the dining hall at another campus or use the soda machine, etc., on any other campus."

Outside consultants quickly showed the consortium that the cost of "putting in our own proprietary system was daunting," said Ms. Ramsbottom.

"Our centralized processing center eliminates the need for deploying a local IT infrastructure," said Mr. Lent. "That's what takes up so much time. All we need is an active data jack and we'll take care of everything else."

"We asked our consultants to check out CardSmith, which was launching another Boston-based program at Berklee College of Music. Berklee had a very positive experience which merited further investigation," continued Ms. Ramsbottom.

Berklee is not a member of the consortium, but its experience gave CardSmith the inside track to obtain the Fenway contract.

"We started in late Fall 2005 to check out CardSmith." By early 2006, the decision was made to go with the company. "We had it up and running that Fall," said Ms. Ramsbottom.

"CardSmith offered us an alternative to get it done quickly while mitigating our financial investment," she added.

To get the six schools "to cooperate is really impressive," said Mr. Lent. "It required a solid commitment and leadership from the presidents and their key administrators."

"The first true multi-school interoperable program"

CardSmith, based in Doylestown, Pennsylvania, "is relatively new. We were the underdogs for that project. The Colleges of Fenway's consultants, who looked at all the different players, came to the realization that the only way it could be done was to use our centralized technology and managed service approach. We delivered more in two to three months of implementation than a lot of schools have done in one to two years. But the schools also deserve a ton of credit for the leadership and commitment to making the project succeed," said Mr. Lent.

He described the program as a first for the industry – "a true multi-school interoperable program, the first time six schools simultaneously developed and launched an integrated campus card community. The six campuses are so close to one another that a common program enables cardholders to more easily utilize each other's resources. The schools and the consortium said, 'Let's cooperate and provide a service experience greater than we can working alone'," he added.

Mr. Lent describes CardSmith as "an outsourced management service provider. We're the first and only company to provide centralized processing technologies coupled with

complete outsourced management services enabling clients to outsource some or all of their card operations."

To enable that business, CardSmith had to develop a centralized campus card transaction processing center. "That's one thing that's unique. We think of ourselves as a very different kind of company. As ongoing service managers we are also daily users of our own technology. This is very different from a company that sells and licenses software and leaves the rest for clients to figure out on their own. For example, we provide a toll-free help desk providing live customer care to students, parents and merchants so we are very intimate with the nuances and challenges of running a high quality card operation."

To show the student acceptance of the Fenway Card, Ms. Ramsbottom noted that Wentworth's enrollment in the Fenway Card surpassed what it previously had on its own card.

Each school issues its own cards, maintains its unique identity and can even customize aspects of the program to their individual campus. "We created a common brand, the Fenway Card. While each has a look and feel specific to each school, every card also has the Fenway Card branding and logo," Mr. Lent added.

As Ms. Ramsbottom further explained: all students are required to have the Fenway Card since it does serve as the official campus ID, but they're not required to put cash on the card. In the card's bottom right hand corner beneath the student's photo, is the Fenway Card logo. "Everything to the left is up to the campus to populate. Each card has the name of the campus on it. However, when you go into any place that accepts the card, the Fenway Card logo is the common denominator. We agreed also on the coding (for the magnetic stripe)."

The financial applications are driven by the magnetic stripe. Security and access applications are powered by either the magnetic stripe and/or proximity technology, said Mr. Lent.

"One trend we see is that more and more schools, particularly in metro areas, are partnering with specialized security companies for building and door access solutions. We coordinate and integrate with leading security firms to make sure that the card is compatible with both platforms," he said.

CardSmith also recommends that clients follow the national and international card number and encoding standards defined by ISO to ensure current and future compatibility with open-ended systems and avoid the pitfalls of using non-standard programs that lock them in with proprietary providers.

At Colleges of the Fenway, the flexible spending account is called Fenway Cash. "Every cardholder has that account available on their card. You put money in that account, and it's similar to cash," said Mr. Lent. "But most cards also have additional accounts linked to the cards. There might be a mandatory meal plan, a print account or financial aid. Most cardholders have four or five different accounts."

CardSmith also has a feature which it has nicknamed "beg-o-matic," with which a student can email his or her parents a request (with a compelling argument) for more money. The student's email contains a hyperlink which will take the parent directly to the Fenway Cash web site, where the parent is able to instantly add money, said Mr. Lent.

However, students own and control their account. "They can optionally set it up so mom and dad can access the account and define what privileges are allowed. For example, the student may allow the parent to add money but not view the student's balance or history. It's a privacy feature," he added. "If they don't want parents to see where they're spending the money, they have that option. It's their decision; we put them in the driver's seat."

Off-campus purchasing

Before the Fenway Card, none of the institutions offered off campus use of their cards, but that has changed. According to Mr. Lent, "we have recruited about 50 merchants in the Boston community to date."

Schools invest significant time and money supporting and marketing the program to maximize student participation, said Mr. Lent. "Accepting merchants do pay a commission on the transactions, and we share those commissions with the schools 50-50."

He said that when the Berklee College of Music card was launched, "we recruited 20 or so merchants. Because of how CardSmith's central platform works, Fenway Card users are able to use the card at merchants in the Berklee neighborhood; and Berklee cardholders can use their card at Fenway merchants in the Fenway area."

CardSmith has no proprietary readers or software at point of sale. "We use industry leading devices and deploy one terminal for the merchant. They only need one to accept all seven schools' cards," added Mr. Lent.

In Ms. Ramsbottom's opinion, the whole operation has been a smooth transition. "They've (CardSmith) signed up the local businesses, we've canvassed where we wanted readers, they've installed the readers. They helped produce the marketing materials for mailings to students. They helped develop a web site where students could add value."

By the end of January 2007, "we had over $1 million that students had put on the cards," she said. Currently, 52 off-campus merchants accept the Fenway Card. Revenue (commissions) earned from the off-campus programs is shared between the consortium and CardSmith, said Ms. Ramsbottom. Reports are provided by CardSmith. "We know how much money students have spent at a particular machine on which campus and where the student came from," she said.

Eventually, she believes the colleges will add new applications. Some of their members already use the card to monitor door access. She points out, "we've agreed on the common formatting. As campuses want to add functions, they can move ahead and do it."

The biggest challenge in the implementation, she added, was communications between all the players that were involved. "We might have a committee which represents a functional area, but does that infer that what the committee decides gets back to the right people (among the six colleges)? Some had card offices who understood; but others didn't, so it was a learning process for them."

And deciding where the card can be used off campus also has proved interesting. "We surveyed the students across the colleges, reviewed the list with the vice presidents for student affairs and an on-going operational team. They agreed that we didn't want anyone accepting this for cigarettes or at a local bar," she said, "but recently the question has been raised about local tanning businesses. There have been some concerns raised that we will be promoting something that has health risks.

So she summarizes, as they have done throughout the Fenway Card project, "we bring the six colleges together and work to come to a consensus."

The CardSmith philosophy

Mr. Lent describes CardSmith as "a team of people who have been in the campus card space for 10 years. I believed that full-featured campus card programs were cost prohibitive and inaccessible to many schools. We looked at the market that wasn't being served and wanted to start making getting in the campus card business cheaper and easier. The Internet helped a lot because 10 or 15 years ago, the technology didn't exist. We studied bank card service models and got a lot of our ideas from that industry. Every bank doesn't own and operate its own credit card processing platform. They outsource to a small number of third party processors that have enormous economies of scale. Why not use a similar approach to benefit the education market?" he asked.

"One of the things we do is that we have a lot of redundancy, like two data centers capable of doing the same thing. If one goes down, the other jumps in. Think about some of these big schools that have a huge operation. Their campus cards power the commerce on campus and is mission-critical to the campus. How many of these schools have a second back-up system in the event of a disaster?" asked Mr. Lent.

He feels that with the Colleges of Fenway project, the consortium "has created a community that's bigger than each school on its own. The leadership demonstrated by each school should be a model to which other colleges can look. We all learned that you can do a lot more by collaborating and cooperating rather than working in your own vacuum. I'm happy that CardSmith could be a part of making it happen."

Campuses to have iCLASS contactless option for the multi-application card program from SmartCentric

Andy Williams
Contributing Editor, AVISIAN Publications

A time tested business adage suggests that one key to success is to give customers a choice. That is one of the driving principles behind Ireland-based SmartCentric's latest move, adding support for the iCLASS contactless smart card to its campus card system through one of the best known contactless solutions providers, HID Global.

SmartCentric recently announced the addition of iCLASS to SmartCentric's SmartCity platform with expected availability later this year.

SmartCentric Technologies International focuses on secure payments and transactions and multi-application smart card systems. Its flagship product, SmartCity, was developed in the early 1990s and is a multi-application smart card based system with multiple uses, including stored value, loyalty, gift cards, logical access, physical access, biometrics, car parking and ticketing.

SmartCity has been used in more than 90 sites worldwide with five million cards issued to colleges (about 10 in the U.S.), government offices, military establishments, banks, cities, towns, shopping areas, and stadiums.

"One of the prime reasons we chose iCLASS is that it has a good reputation and good brand recognition," said SmartCentric CEO Kieran Timmins.

"That means we can offer yet another choice within SmartCity. One of our founding philosophies is to give customers a choice. Previously we only had contact cards, but last year we added contactless support with NXP's DESFire. Now we are expanding with iCLASS," said Mr. Timmins.

"The incorporation of iCLASS into SmartCity will provide our customers with a real choice of advanced RFID card platforms and new opportunities for expanded use of SmartCity's family of smart card solutions," he added.

SmartCity, an HID iCLASS Development Partner, has been working with HID Global to ensure that the iCLASS implementation supports a campus' needs for a multi-application smart card.

"It's hard to say when schools will switch over to contactless technologies but most will over time," said Mr. Timmins. "While contactless hasn't taken off in U.S. campus markets as yet, most schools are talking about contactless."

He added: "To date, most schools' exposure to any type of contactless technologies have been with the prox card used solely for physical access. iCLASS provides a natural migration from prox to a fully functional multi-application smart card while protecting any investment in prox readers."

He said SmartCity will be migrating its technology to enable a full suite of SmartCity applications, such as parking, logical and physical access, vending, pay for print, meal plans, web revalue, ticketing and off-campus use, where needed.

"Essentially our proposition is to move everything you can get on a contact chip today to contactless technology over a period of time with iCLASS," said Mr. Timmins. He predicts the price range for iCLASS will be comparable to that of other contactless cards.

To convert schools to an iCLASS environment will require some software upgrades. "They'll also have to buy new readers for vending, laundry, etc.," he said.

One way to convert a school is to go with what he calls the "big bang approach and card everyone, that is, issue everyone with a brand new card," he said.

Another way to migrate to the new contactless card would be to issue the new cards just to all incoming freshmen. In four years, the migration would be mostly complete.

For schools currently using SmartCity, "we can also provide them a hybrid reader that will support both contact and contactless cards allowing schools to gradually replace hardware over the period of the migration. With the hybrid readers, we're trying to give the colleges options, to work within their budgetary constraints so they don't have to card everyone."

Mr. Timmins could not say how many schools might convert to iCLASS. "We're talking to a couple of schools who have SmartCity now."

He sees iCLASS support as simply another menu item from which colleges can choose. "We can support a variety of readers depending on the applications. Our strategy going forward is about supporting every application. If they (colleges) want DESFire, we'll get it for them," he added. "We also can work with companies like ViVOtech and On Track Innovations and their existing readers. From my point of view, we're simply reacting to customer requirements in the U.S."

CR80News

Students monitor laundry progress online via new monitoring solutions and their campus card

Messages are sent to email or cell phone when wash and dry cycles are complete

Ryan Kline
Contributing Editor, AVISIAN Publications

The campus card has helped to alleviate the frantic search for quarters that characterizes the student laundry experience. Card-based payment solves that problem, but what will solve the problem the ever so busy college student faces now – waiting … and waiting for open washers and dryers?

Students use the Internet for almost everything … but laundry? Yes, the online revolution has reached the laundry room. At least four companies are offering solutions to monitor the laundry facilities and allow students to view machine availability in real-time. At least one other company, CBORD, is beta testing a new laundry monitoring solution.

CR80News investigated these laundry solutions to find out the benefits for students and institutions and to identify differences between the various offerings. We talked to:

- Dick Casey, Director of Route Sales for Wash Alert, a subsidiary of Speed Queen Alliance Laundry Solutions
- Wendy Jenkins, VP of Marketing for e-Suds, a subsidiary of USA Technologies
- Robert Looney, VP of Sales Development and Bob Tuttle, VP of Technology for Laundry View, a subsidiary of Mac-Gray Corporation Corporate Laundry

How do these systems function?

At the core of each of these systems is a web-based visual representation of a campus' laundry rooms. Students access the preferred room online to monitor machine availability and determine the right time to lug dirty clothes to the room. But the convenience doesn't end there. "Students can check machine availability as well as select a notification option of their wash or dry cycle completion," says Mr. Casey. "An e-mail can be sent to their computer or their e-mail-enabled cell phone. For instance, if a student figures it will take them 5 minutes to return to the laundry room, they can select to be notified 5 minutes before the end of cycle (or) be notified when three washers are available."

Wendy Jenkins, explains that, "with e-Suds (students) only need to register their email address where they would like to be notified once. When they swipe their student ID at the e-Suds controller, the system will identify who the student is and alert them when their cycles are complete."

"Simply point and click on any machine to request a notification when the machine next starts or ends a cycle," adds Mr. Looney. Students can request to be notified by instant message, e-mail or by a text message to their mobile phone."

The various web options include either 2D or 3D representations of the laundry room with in-use machines colored differently than open machines. "(With Laundry View) cycle time and existing notification information appears in a pop-up window when the student rolls the mouse over each machine," comments Mr. Looney.

An easy implementation that pays off big in convenience

"Today's college students are far more technology savvy than even those a decade ago," says Mr. Casey. "They also are extremely busy. Wash Alert takes a basic chore all students need to do and offers a high-tech way of maximizing their time."

The students love the convenience and the level of effort on the part of the campus is minimal.

According to Mr. Looney, "we have converted over a thousand laundry rooms to the system at over 100 schools in the last three years. The process is very simple. If the necessary network connections are in place, a room can be converted and on-line in a matter of hours."

The systems also make money

Maximizing machine usage and helping to spread the 'load' across normally-underutilized time periods increases revenues from campus laundries. Additionally, more efficient utilization can reduce the need for additional machines or rooms.

But laundry monitoring systems can provide another benefit that translates into increased revenues – they can inform maintenance staff when a machine is broken or offline. This can result in more rapid repair and thus better uptime for the facilities.

Mr. Looney explains, "each machine's status is monitored at all times so that the server can detect problems as they occur. Machine problems are then reported to the service organization for action."

"e-Suds sends diagnostic reports, including machine fault codes, to an operator's dispatch area," says Ms. Jenkins. And Wash Alert's Mr. Casey continues, "error codes such as fill or drain errors or break-in alarms can be sent to personnel of the university's choosing such as a maintenance supervisor, security officer or receptionist."

Reserving machines online?

An obvious next question involves the student's ability to reserve a machine online and hold it until he can get to the laundry room. While it seems like a great convenience, all of the company representatives noted that this feature was not allowed in their system. Reasons included the added downtime it would cause and the inevitable arguments that would occur on site.

Questions & answers

In the following question and answer section, we posed a series of specific issues to each of the three respondents. Their answers help provide a glimpse into the similarities and differences between the products.

What laundry machines and dryers does the system support?

Dick Casey, Wash Alert: Wash Alert works exclusively on Speed Queen washers and dryers.

Wendy Jenkins, e-Suds: Maytag and Speed Queen, for e-Suds 2.0 but e-Suds Lite is compatible with any brand of washers and dryers.

Robert Looney, Laundry View: All commonly used commercial laundry equipment may be monitored by the LaundryView system.

What hardware is required on each machine to implement your solution?

Dick Casey, Wash Alert: The machine needs for our Wash Alert System are quite simple. Wash Alert requires Speed Queen washers and dryers equipped with the NetMaster control and a network card.

Wendy Jenkins, e-Suds: We have two versions: e-Suds 2.0 and e-Suds Lite. e-Suds 2.0 is a transaction processing (payment) system with monitoring. This system connects to the individual washer and dryer. It is compatible with Maytag and Speed Queen. e-Suds Lite is a monitoring system that connects to a third party payment system and is compatible with any brand of washer and dryer.

Robert Looney, Laundry View: A Smart Laundry Machine Interface board is used for each machine to monitor machine activity and status, door status and to track all payments, whether by card or coin. They passively monitor machine activity and are daisy-chained to the LRM using a standard RS485 serial connection.

Is the data hosted on the school's server or on a central server maintained by the company?

Dick Casey, Wash Alert: Laundry room information is hosted on the school's server. This gives the university ultimate flexibility in its display. In addition, because the interface is hosted by the school and not off-site, schools have no on-going fees for such a service.

Wendy Jenkins, e-Suds: On our servers maintained by our company.

Robert Looney, Laundry View: The LaundryView web site provides the laundry room status information. It is hosted off-campus on a dedicated Mac-Gray server in a managed, 7x24 data center for maximum reliability. The school needs only to provide an outbound connection to the Internet for each LRM so that it can provide regular updates to the server using standard HTTP messages. The system is designed such that inbound connections are not required. Students may then use any standard browser to view the laundry room status.

What type of reporting is available for the campus?

Dick Casey, Wash Alert: A wealth of audit data is collected through the NetMaster software. Reports can detail usage history by machine, group, time-of-day, and special vend options as well as service door openings and coin vault openings.

Wendy Jenkins, e-Suds: e-Suds reports both cash and card usage. Password protected access is given to school administrators and/or laundry operators enabling them to get usage reports by campus, by hall, by room and by student.

Robert Looney, Laundry View: The system provides usage reports for both the students and for school administrators. Students can see a weekly snapshot of the activity in each room by day and hour so they can plan the best time to use the facility. The data is refreshed every day and is based on the most recent two weeks usage. Administrators can log in to a special administrative web site to view information about machine usage over any period that they specify.

Many universities and colleges now have card systems that are used to pay for their laundry services. Is your system compatible with any of the major campus card programs?

Dick Casey, Wash Alert: Wash Alert will work with all campus card systems.

Wendy Jenkins, e-Suds: Blackboard and CBORD. For Blackboard we are fully integrated and able to debit funds from a student's Blackboard account. With CBORD we function along side their system. We provide the monitoring and they provide the transaction.

Robert Looney, Laundry View: All of them. LaundryView is installed to monitor Blackboard (current LR3000 product as well as earlier Unix and Windows equipment), CBORD (current IP versions of the Odyssey controller as well as earlier versions and Diebold CS Gold LR3000 and LR1000 controllers), General Meters, NuVision, and CardSmith systems. Laundryview may also be installed with various off-line magnetic card systems including ITC, Debitek, ESD (e-Danyl), Danyl as well as smart card systems from ESD, Debitek and Greenwald/Intellicard.

Card system vendors refine off campus offerings

Students enjoy added flexibility, and institutions benefit from new revenues by extending the ID card's purchasing power to the merchant community

In the drive for more bucks–and don't kid yourself, nearly every college and university needs more money, particularly in today's tax revolt environment–one overlooked revenue stream could be as near as the pizza joint next door to the college.

Off campus card usage is becoming more common among campuses, particularly since campus card companies have overcome one of the major obstacles: the institution's perceived loss of on-campus revenue. The fear of 'robbing Peter to pay Paul' kept many colleges from pursuing off-campus programs … But that fear seems to have largely subsided.

All those interviewed agreed on one thing: Allowing students to use their cards off-campus enhances the student experience.

"One of the things we did last spring and last summer was to interview a variety of presidents, provosts, and vice presidents, and followed that up with a survey trying to find out what are the key issues among universities," said Tom Bell, vice president, industry relations, for Blackboard, which produces the off-campus card program BbOne, part of the Blackboard Commerce Suite.

"The number one issue was the student experience and how to improve it," Mr. Bell said. "Number two was accountability to your customer, the student, staff, private entities who may be evaluating your campus (such as accrediting agencies)."

And number three? You guessed it. "Colleges are looking for new sources of revenue. That's something we run into all the time," said Mr. Bell.

Obviously numbers one and three are closely related when it comes to off-campus card use.

"The number one thing from my road show when I visited 27 schools, was that students wanted off-campus use," said Shawn McCarthy, managing director, Off Campus Advantage, now a subsidiary of campus card provider CBORD. "It's out there enough so they're all hearing about it and they see the value of it. They don't want to carry a lot of extra things (in their wallets), they love the way it works on campus with vending, laundry, so they want everything on one card," he added.

Jeff Zander, vice president of General Meters, which manufactures and supports the campus card program known as the University OneCard System, said it only makes sense for merchants to "capitalize on this captive market, students from nearby campuses who are increasingly asking to use their University OneCard at off campus at restaurants, movie theaters, pharmacies, taxi services, hair salons and more. Students are going off campus, they can spend the money wherever they want and campuses are recognizing this fact. They're also aware there's money to be made here," said Mr. Zander.

"Students are getting more savvy with payment products; it's something they expect," said Pedro Marzo, Blackboard's BbOne director, "and they're pushing the university to do it."

Does on-campus revenue drop?

Mr. Marzo says in the past, the discussion about off-campus use was different. "We had to first and foremost sell the concept because they were initially skeptical." The biggest fear, of course was would it pillage on-campus sales, particularly at dining facilities and bookstores.

Losing on campus revenue "was valid at one point," said Mr. Zander. "But they're adults and they're going off campus so why not make some money off them? If they put money on that card, they're going to want to use that card wherever they can." It's the old 'if you can't beat them, join them' mentality, he adds.

"That loss of on-campus revenue argument is going away more and more, because on-campus spending is going up," said Mr. McCarthy. "It ups the amount of money deposited into those discretionary accounts and parents love it (that they're able to) place a defined amount of money into a discretionary account."

Mr. Marzo agrees. "We've been following this data and we've found that when a university goes off campus, they actually see an increase in on-campus spending because there's more money in the system," he said. "Most of them do not see a (negative) impact in on campus sales. On average, on campus spending increases 25% because there's more money in the system. If students have money on the card, they'll still spend it on campus because it's more convenient."

Percentage-wise, Mr. Marzo estimates that for every dollar a parent deposits in his child's account, less than a third goes for off campus purchases.

He said many universities have two purses on their campus cards, one for dining and another "called flexible funds. Most of the time, only flexible funds can be used off campus but they also can be used on-campus" while the dining purse is limited to on-campus use only.

Added Mr. Bell: "As the parent of a college student, I love the idea of depositing money to my student's account rather than sending them a check for $200. I then have some idea of how it's going to be spent."

"Parents feel better about making deposits into a closed loop declining account," said Mr. Marzo. "We've seen schools that compete in the same market, the one with the off campus program is seen as more favorable in the eyes of students and parents," said Mr. Marzo.

Making the move off campus

Colleges who tried to manage off campus programs in many cases found themselves "a victim of their own success," said Mr. McCarthy. Colleges would end up with 75 to 100 merchants but it became a nightmare to settle with each merchant. They quickly realized they didn't want to be in this business, he added.

Niles Dally, vice president, sales and marketing, for NuVision Networks' One Card System, remembers the first time one of its schools installed an off campus program. "It was 15 years ago, a small school, which had this idea to put a card reader in a local pizza place. The cardholder would call up the pizza joint and read off the ID number off his card, it would clear his account and the pizza was delivered. Everything worked fine at first but in the first week, the thing crashed. Actually, the concept crashed. It was taking four to five hours to get a pizza because they were so busy." But the college and the merchant made money, lots of it, he said, since the school was keeping a 20% commission.

Things have quieted down since then, or gotten more organized and sophisticated. Now, Mr. Dally estimates off campus usage has grown some 200%.

CBORD and its Off Campus Advantage subsidiary offer central processing

CBORD recently purchased a company specializing in off-campus use, Off Campus Advantage (OCA), which had been serving many of CBORD's customers that had formerly been users of Diebold's Gold offering (CBORD acquired Diebold's Card Systems Division in 2005).

"What we found interesting was they (OCA) had a central processing technology solution which is what we were developing," said Mr. McCarthy. So, instead of continuing with development of the central processing part, CBORD went a step better and bought the company, which is now a CBORD subsidiary.

> *"When you think of off campus you think of fast food, but it goes beyond that. The most popular category we've seen is grocery stores."*
>
> *— Pedro Marzo*
> *Blackboard's BbOne director*

CR80News

"Up to this point, all the campuses needed to connect through a dial-up (if they had off-campus functionality)," said Mr. McCarthy. "Now that's alleviated with the OCA technology which connects all the campuses with a secure connection."

Mr. McCarthy sees CBORD and OCA as the "bridge" between merchants and the college.

"There's been a tremendous reaction from schools because the schools want this in a hurry," he said. There's no cost to the campus, it provides them a revenue stream and "we'll take care of everything. They just have to monitor the reporting features," he added. "If they wanted to recruit their own merchants, we're open to that, but it's a soup and nuts operation."

"We would sell them specific readers that they could take off campus. But when they started getting out there and realized what it took, they realized they needed a better solution," said Mr. McCarthy.

CBORD is in the process of creating a national merchant network that its colleges to tap into wherever they are.

General Meters offers campuses the ability to self-manage or out-source the program

In General Meters' case, the university can also buy the reader and operate the off-campus program on their own. "Some campuses buy our readers direct and solicit merchants themselves and they make all the money," said Mr. Zander. "And then we have some campuses tell us they don't want to get involved at all. We sell it to the merchant directly."

"In most cases the merchants don't purchase the readers, they rent them from the campus or from us," adds Mr. Zander. "One university gave a reader to the merchant and every time the university card was swiped through, the college took 25 cents, whether it was a dollar sale or a one hundred dollar sale." That college, he said, turned a tidy profit. "There are a lot of ways a campus can make money."

"There are many different ways the program can work, but it's up to the campus to tell General Meters what they prefer. Unless the campus card office gives us their blessing, we don't do it without their approval," he added.

He said that when colleges let General Meters do everything, "we gamble. If the merchant leases it, we bundle a lease agreement so it covers our expenses … and we split the profits with the campus and/or the merchant." He said General Meters has created an entire division dedicated to off campus merchant programs (in cases where the campus doesn't have the time, personnel and/or resources to pursue such a program but wants help in developing one). This program is known as 1Card Advantage. In this example GMC will handle everything right down to connecting the terminal in the merchant location then sharing profits with the campus and/or merchant based on the variety of agreement options offered by GMC.

He said more campuses are realizing the potentials of buying these terminals and managing them themselves. "But we still have a lot of clients who want us to do it all."

General Meters' merchants can be paid daily, weekly or monthly, said Mr. Zander. The General Meters system can generate a dollar amount (of sales) and a check is sent to the merchant. "Or we can do an electronic transfer where General Meters can transfer the value to the merchant's online account. The most efficient way is for the campus to cut the check and we confirm the balance."

The card readers are manufactured by General Meters and are easy to install at just about any merchant location, he said. "We make a variety of readers that talk over a variety of phone lines. At the very minimum if you only have a phone line to conduct Visa and MasterCard charges, you can attach our reader to the same phone line," said Mr. Zander.

NuVision offers web-based off campus purchases

NuVision rents colleges its card readers, "or we can ship directly to the merchant," said Mr. Dally. "In most instances, a card can't go through a national clearing system because they still don't have ISO numbers. So another device is necessary."

Another option for NuVision's college customers is, "our web portal, a campus center. It has a shopper built into it and allows a cardholder to log on to the campus center and actually place an order for items at a merchant location. That's usually done with merchants delivering a product, like pizza, or picking up an order (e.g. an off campus bookstore). It's not designed for those locations where a cardholder needs to present his card," said Mr. Dally.

NuVision's software is built into the card reader. "Just put a card reader on a merchant's table top, and plug it in. It attaches to a phone line, has a modem built in as well as our web portal," Mr. Dally added.

Blackboard views merchant settlement as key to program success

With Blackboard's BbOne offering, Mr. Marzo notes, "merchants can get reimbursed daily. We extract transaction details from our POS devices and debit the funds from the university account and deposit 100% of the funds back to the merchant. We've modeled the service after credit card best practices."

Monthly, he explained, Blackboard accounts for the money in the various merchant transactions and debit the merchant for his fees, which includes fixed rates, the percentages which vary by merchant and by each university. For example, gas stations, with lower margins, would pay a much lower fee than say a restaurant, said Mr. Marzo. Those collections are shared with the universities.

As to the money that can be made, and the reasons for implementing an off-campus program, that depends on the number of students the university has, and how much discretionary deposits can be spent, said Blackboard's Bell. "I know of some colleges that pay for their ID operation with their off campus revenue. Sources from off campus can help you fund other projects, such as vending. For other universities, off-campus is simply cost-neutral. I know of campuses that want to extend their off campus capabilities so they don't have to open a dining facility. Or they can close their dining facility at night, but with off campus, students still have access to food."

Getting merchants to buy in … and keeping others out

The philosophy behind recruiting merchants is simple. Get students as customers now and they may stay with you for a long while after they graduate. "We all know there's a soda war that's going on," explained Mr. Dally. "Whatever soda you drink then you'll probably drink for the rest of your life. The same holds for McDonald's, Burger King, etc. For them to give 10 percent away for the ability to have the student use his debit account at their restaurant" is a good deal for them.

"What's nice in a campus community is that it's fairly easy to define merchants that have a good value for the students, such as food, pharmacies and health and beauty," said Mr. McCarthy of CBORD. "We work with colleges to define what merchants they want. Colleges say parents have entrusted us to build a trusted merchant community to meet the students' needs."

"For merchants, they tap into a pool of funds they wouldn't normally have access to," added Blackboard's Mr. Marzo. "When we approach merchants, we lead with the access channels they're going to have available to them, like emails, posters and flyers that (go out to students). Some schools consider going off campus because the merchants are knocking at the door. It's a push and pull situation," he added.

In Blackboard's case, the company solicits the merchants. "Every merchant we approach is pre-approved by the institution," said Mr. Marzo.

"We think of it like working with an architect in designing a house. You wouldn't design a room without consulting the client. We wouldn't, for example, add an off campus bookstore because there's an on-campus bookstore."

But for those institutions without an on-campus bookstore, giving their students access to bookstores off campus would be an ideal arrangement, he added.

All campus card companies talked to for this story agree that certain merchants are off limits such as liquor stores, tobacco, firearms, and distributors of obscene material. "Some Catholic schools are very sensitive to having pharmacies on the program because they sell family planning products," added Mr. Marzo.

"When they think of off campus you think of fast food, but it goes beyond that. The most popular category we've seen is grocery stores," said Mr. Marzo. "We've seen a trend in universities wanting to add health foods to complement their on campus food offerings."

"The applications most common are restaurants first, then pharmacies. They're making huge money. One is making $40,000 a week in sales," said Mr. Zander.

Off campus use can also run the gamut from golf courses to housing complexes. "We have one university in the Midwest that owns a golf course and it's part of the off campus program. And one in New England owns several off campus housing complexes. They're thinking of allowing students the ability to pay their rent with their university IDs," said Mr. Marzo.

"And we're barely scratching the surface," he said. One university has just cleared a partnership with the local major league baseball team to allow students to pay for their tickets with their campus cards.

A growing trend

"The percentage of off campus use is growing," said Mr. Zander. "Right now, for every 10 campuses, only about three or four have off-campus programs. I expect that number to double in the next three years to between six to eight."

Added Mr. Dally: "We implemented this because the students wanted it and colleges could make money. It's a synergistic effect. The money is motivation for some and for others it's providing a service to students. Mom and dad win because they don't have to send money to the kid because there's control over it. The kid wins because he learns to budget. The merchant wins because they get more business. Colleges win because they get more money and thus have more to spend on student services."

"Students are incredibly interested in a variety of services," adds Mr. Bell. "Dining services are now serving sushi. I never thought we'd get there but (choices) have expanded, and off campus has also expanded to allow students to eat where it's most convenient for them."

CR80News

RFIDNews

Is RFID in the operating room a "spongeworthy" idea?

David Wyld
Contributing Editor, AVISIAN Publications

In late 2002, a Canadian woman set off an airport metal detector. When she was "wanded," the metal detector consistently sounded when placed near her abdomen. She had undergone surgery four months earlier and had suffered from unexplained abdominal pain ever since. Several days after the airport incident, an x-ray of her abdomen revealed the presence of a 12-inch long, 2-inch wide surgical retractor.

According to the most recent comprehensive study on the incidence of such surgical errors, 2,710 foreign objects were left in American patients in the year 2000. This translates into an incidence of .008% of all surgeries in the U.S., meaning that one has approximately a 1 in 10,000 chance of having something unintentionally left inside of them after surgery.

Recent research on the subject, published in the New England Journal of Medicine, indicates that two-thirds of all retained objects are surgical sponges. The risk of foreign object retention has been found to be greatest in instances of emergency surgeries and in patients with high body mass indexes. Though the actual instances are fortunately rare (far less common than the "urban legends" of surgeons leaving their wristwatches in patients' bellies or the infamous "Junior Mint" episode of Seinfeld where a candy landed inside a surgical patient), medical literature is replete with cases of sponges and other items being left inside patients during surgery. Retained sponges and surgical instruments have remained undetected for surprisingly long periods of time, though not necessarily without causing symptoms.

The retained sponge problem

The medical term for a "retained sponge" is gossypiboma (derived from the Latin gossypium, for "cotton" and the Swahili boma, for place of concealment). Gossypiboma is regarded as an all-encompassing term in the medical literature, as it now includes all types of foreign articles that can be inadvertently left in a patient's body during surgery, including not just sponges, but also:

- surgical instruments
- needles
- knife blades
- safety pins
- electrosurgical adapters.

Sponges are thus the main focus of concern, due to their omnipresent use in even the simplest of surgical procedures, including laproscopic work. Sponges are used to soak-up blood but also to enable surgeons to get a better grip on instruments, tissue, and even organs. They are also of paramount concern because when left in the body, a simple, porous sponge can cause both immediate and/or long-term health effects, ranging from minor inflammatory effects to fistulas, adhesions, and even sepsis. The sponges can calcify and be mistaken later in X-ray and MRI scans as possible tumors, leading to costly and unnecessary treatments, not to mention stress on unsuspecting patients and their families.

In 2007, the standard medical protocol is for multiple members of the surgical team to perform multiple manual counts of sponges and medical instruments before, during and after surgery, hoping that the numbers match at all times. Obviously, in the frenetic environment of the operating room, such a manual-based process is vulnerable to human error. In fact, research from the U.S. Agency for Healthcare Research and Quality has shown that when sponges have been left behind, the manual count in the operating room has been shown to be falsely correct in more than three quarters of non-vaginal surgeries. If the manual counts do not sync, nurses must try to solve the mystery by taking on the messy task of sorting through blood-soaked sponges and gauze.

If the count is still deemed unreliable, surgical patients are then routinely subjected to X-rays to attempt to double-check that all sponges have indeed been removed – a step that adds

cost and time to the surgical process and is not 100% accurate. For example, a sponge remaining behind a bone will not show-up on an X-ray. Even so, in high-risk or long-duration surgeries, patients are now routinely X-rayed to detect sponges. Dr. Jeffery Port, Chairman of RF Surgical and a thoracic surgeon at Weill-Cornell Medical Center in New York City commented that: "Although nurses do a good job keeping track of sponges, gauze and instruments in the operating room, there are several patients who retain objects in their body. The fear that we're going to leave something behind also creates chaos when manually counting equipment after the operation."

In a 2003 commentary for the Agency for Healthcare Research and Quality by Dr. Verna C. Gibbs, MD, in the University of California, San Francisco's Department of Surgery, commented that: "The critical question is not, 'Was the count correct?' It is, 'Is there a sponge or instrument in the patient?' Unfortunately, we have yet to identify the best way to answer this question."

The RFID solution for the operating room

Current research has indicated that RFID may give a valuable solution to the problem. There are several companies vying to create "smart sponge" systems for the operating room. These include RF Surgical Systems of Bellevue, Washington, and ClearCount of Pittsburgh, Pennsylvania. RF Surgical Systems' RF-Detect system was the brainchild of Dr. Jeffery Port and William Blair, an electrical engineer, who first envisioned the concept a decade ago. ClearCount was founded by Gautam Gandhi and Steve Fleck, who came up with the idea for RFID-tagged surgical sponges while students at Carnegie-Mellon University. Both companies are vying for what promises to be one of the most lucrative in-hospital markets for RFID, as sponges are both plentiful and disposable in today's operating rooms. RF Surgical's RF-Detect sponge detection system received FDA regulatory approval for patient use in November 2006, and approval for ClearCount's SmartSponge system is anticipated in 2007. Both systems embed surgical sponges with small RFID tags, programmed with a unique serial number that allows the reader to report any sponges that may be present in the body cavity.

A recent test validating the capabilities of RFID-equipped sponges was published last year in the prestigious medical journal, the Archives of Surgery. The study was conducted by the Stanford University School of Medicine and funded by grants from the National Institutes of Health and the Small Business Innovation Research Program. The subjects in this study were eight patients undergoing abdominal or pelvic surgery. Just before closing the incision, the surgeon placed an RFID-tagged sponge (containing a 20mm diameter RFID tag) in the body cavity. Then, the sides of the incision were pulled together to temporarily "close" the wound.

A second surgeon was then called in, who had not witnessed the first surgeon insert the RFID sponges. He then used a wand-style RFID reader and passed it over the incision site in order to attempt to locate the RFID sponges. In all eight cases, the RFID sponges were accurately located in less than 3 seconds, with no false positive or negative readings found in using 28 tagged sponges. Dr. Alex Macario, the lead researcher of the Stanford study, believes that such RFID-based tracking systems will become commonplace, observing that: "We need a system that is really fail-safe, where, regardless of how people use counting-system technology, the patient doesn't leave the operating room with a retained foreign body."

Practical considerations

There are a multitude of practical considerations when introducing new procedures and new equipment in the surgical theater. First, there is an issue of space, as introducing new equipment into the already cramped, frenetic environs of the surgical theater is an issue, regardless of how small the form factor of the readers may be. Also, there may need to be some ergonomic and operational changes made in the operating room, as RFID readers may detect not only the targeted sponges in the patient, but any stored for use around the patient. The nature of surgery also presents unique considerations, but tags have already been developed that can withstand the temperatures required for sterilization.

Can RFID tag every item in the surgical theater? ClearCount's Gandhi reports that more work needs to be done in tagging steel surgical tools, due to the metal and form factors involved.

There is also the cost issue. Harrison Chow, a clinical instructor and perioperative management fellow in Stanford University Medical Center's Department of Anesthesia, recently conducted an independent economic analysis on the cost/benefit of RFID-tagging of surgical sponges. He concluded that this technology "appear(s) to be economically attractive from society's perspective, as long as this new technology approximately cuts in half the time nurses spend counting sponges."

The final "elephant in the room" may be the liability issues involved for the manufacturers of all such RFID-devices for the surgical theater, as they could readily be the subject of malpractice claims if their devices fail to correctly detect the presence of surgical sponges or other foreign bodies.

Conclusion

The hospital environment may be one of the true hotbeds for RFID activity in the coming years. In fact, analysts have projected that the market for RFID and related technologies will grow to over $8.8 billion by 2010. This is in spite of the fact that health care administrators in the U.S. are notoriously slow to adopt new technologies. RFID presents compelling benefits across several areas, beyond the operating room, including:

- Patient tracking
- Locating and tracking use of medical devices and support equipment
- Storage and care of blood products and specimens
- Management of hazardous waste
- Tracking of garments.

However, the use of RFID in the prevention of surgical errors presents perhaps the most important benefit to both patients and hospitals. It improves health outcomes, but it can also provide ROI to the hospital by reducing certain types of extreme surgical errors. These errors can not only cost the patients their lives or their quality of life, but they can also cost the hospital in untold bad publicity and millions from lawsuits.

About the author

David C. Wyld is the Robert Maurin Professor of Management and Director of the Strategic e-Commerce/e-Government Initiative at Southeastern Louisiana University.

The principles of RFID: Hardware basics

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

The most basic radio frequency identification solution is made up of three main hardware components. These components are the RFID tag, the RFID reader, and the antenna. This is, of course, an over simplification of what it takes to apply today's RFID technology to a real world problem, but these are the fundamental building blocks. Understanding the fundamentals of RFID is the key that allows practitioners to be successful in their application of the technology. Even though this article does not discuss the software required to interpret and make use of the RFID data, its role in a complete RFID solution is vital.

The components of the basic RFID tag are an integrated circuit (IC), an antenna, and the substrate that holds it all together. The IC is responsible for controlling the tag; much like a CPU controls a desktop computer. The IC controls what is broadcast from the tag, processes commands received from the reader via the antenna, and manages any peripherals such as temperature and pressure sensors. The antenna plays multiple roles in most RFID tags. It is responsible for receiving and transmitting data from and to the reader, and, in the case of passive type RFID tags, they collect the energy required to power the tag. Passive tags power themselves off of the energy they collect from high gain antennas that are connected to the RFID reader; therefore, they must be in close proximity to the RFID reader's antenna in order to collect enough energy to function.

RFID tags with onboard batteries are known as active tags. Unlike passive tags, they transmit their data even when they are not in close proximity to an RFID reader. In most cases, active tags can be read at a longer distance than passive tags. There is a hybrid tag known as the semi-active tag. It has an onboard battery just like the active tag, but it will only transmit when it is in close proximity to the reader.

RFID tags may transmit many different pieces of data, but the most fundamental piece of data is the tag's unique identifier. The unique identifier is, in most cases, associated with a real world asset that is to be tracked. The unique identifier is used as the key that identifies information about an asset in a database in most applications. Tags may also transmit state information or telemetry such as temperature or humidity if they have the sensors to collect this type of information. Most passive tags do not have peripheral functionality due to the power limitations of not having an onboard battery.

The RFID reader is sometimes referred to as the interrogator. The reader receives all of the data that the tags are transmitting. The data is then passed on to software that makes use of the data. The tags that are in close enough proximity to a reader are referred to as the reader's "tag population." As a reader's tag population grows, the density of tags around the reader also grows, and the reader may require more time to read all of the tags in its vicinity. This is due to the fact that if all the tags transmit at the same time, the reader will not be able to separate their data into discrete transmissions, so it is important that the tags do not transmit all at once.

Passive tag readers select subsets of the population to query over time until beacons from all of the tags in the population have been received. Most active tag readers do not control the sampling of the tag population like passive readers do. Active tags beacon at a pseudo-random interval to avoid transmission collision with other tags. Anti-collision algorithms such as the ALOHA algorithm determine when the tag will beacon. The ALOHA algorithm assigns transmission time slots to each tag. The name ALOHA is not an acronym, but was given its name because it was developed at the University of Hawaii. The ALOHA algorithm is a common anti-collision algorithm that is used by many RF applications, not only RFID. Over time, the randomization of the tag transmissions will ensure that the transmissions from all the tags are eventually received. There exists a threshold where the tag density is so great that it cannot be guaranteed that all the tags will be sampled in a timely manner. The tag density maximum is different for each RFID tag and reader manufacturer. Some manufacturers even allow the anti-collision algorithm to be changed based on the needs of the solution.

The importance of the antenna that is connected to the reader cannot be underestimated. In a passive RFID solution, the antenna must be sensitive enough to receive the RFID tag transmissions, and it must also be powerful enough to power the tags. Passive tag reader antennas may be deployed in many different configurations depending on the application. A portal configuration is the most common type. Portals place an antenna on each side of the tag's path (i.e., at a loading dock door or on an assembly line). Sometimes, a portal configuration may also affix antennas on the top and bottom of the pathway to completely surround the tag's path, thus increasing the chances of reading the tag as it passes through the portal.

Antennas used in active tag applications must solve a different set of problems. Many times, active tags are used in a real-time location system (RTLS). An RTLS is used to track tagged assets as they move through a building, yard, or supply chain. Active reader antennas are usually installed in the middle of the desired coverage area. For example, an antenna could be placed in the ceiling in the middle of a room. This antenna could then read all of the tags in the room. Because of the increased transmission power of most active RFID tags, when compared to passive tags, the antenna may also read tags outside of the room. Transmissions from tags in adjacent rooms, hallways, or in a room immediately above the antenna in a multistory building may be inadvertently received by the antenna. This is known as "bleeding coverage." Most require that the coverage be well defined to a single room or to a zone within a room. To resolve this issue, the correct antenna must be selected that meets the needs of the RF environment. Antennas must provide smooth and consistent input to the RFID reader in order for it to efficiently decode the tags' transmissions. Bad input will yield bad results, especially in RTLS's.

In the words of Scotty from Star Trek, "You can't bend the laws of physics, Captain!" Even though RFID practitioners are bound by the laws of physics, they can make smart decisions about what components they choose and how they are deployed.

RFIDNews

Antiquated item pricing laws counteract potential RFID savings in many states

Old school price tag requirements create redundant expense for retailers and higher prices for consumers

David Wyld

Contributing Editor, AVISIAN Publications

This morning, you can take a time travel adventure without leaving your desk. We can go "back to the future," to the grocery store of our Baby Boomer youth. There, you can pick-up a can of beans with a price sticker that reads sixty-nine cents. Then you can take that can to the checkout line, and a real, live clerk will ring up the price manually on her register.

Believe it or not, for many this scenario is not a dream in the year 2007. Rather, it is a very real nightmare for retailers. In a significant part of the United States, grocery stores – and many other categories of retail stores – must still place individual price tags on almost every item they sell. This is because of state and local laws, commonly referred to as "item pricing laws" (IPLs). These regulations were largely enacted as consumer protection measures in the 1970s and 1980s to protect against overcharging due to checkout scanning errors.

Yet, these laws are still in vogue. As late as 2005, New York City's Mayor Michael Bloomberg signed a law stiffening its municipal item pricing regulations. IPLs have been supported by not just consumer advocates, but by retail and grocery workers' unions, who see the laws as protecting outmoded jobs. Currently, item pricing laws are in place in ten U.S. states:

- Arizona
- California
- Connecticut
- Illinois
- Massachusetts
- Michigan
- New Hampshire
- New York
- North Dakota
- Rhode Island.

Additionally, item pricing laws exist in several large metropolitan areas in otherwise non-IPL states, including Chicago and Philadelphia. In Michigan, the state's IPL covers almost every item priced 30-cents or more for sale in any retail outlet. In other states, IPL laws are restricted to food stores only. In Connecticut, retailers are exempted from that state's IPL if they install electronic shelf labeling systems (at a cost well in excess of $100,000 per store).

The laws are designed to give the consumer recourse in the case of scanner error, being able to point to the physical price tag on the item as the incontrovertible "truth" in pricing. Yet, while most of us have encountered scanner errors personally, the truth of the matter is that they are increasingly rare – and often in our favor.

The U.S. Federal Trade Commission (FTC) has conducted the most comprehensive research on scanner accuracy to date. In its "Price Check II" study, the agency's researchers checked prices of more than 100,000 items at more than 1,000 stores. They found that one out of every 30 items was incorrectly priced, with undercharges occurring just as frequently as overcharges. In fact, the grocery industry outperformed the general retail industry, where errors occurred on approximately one out of every 25 items scanned. As point-of-sale (POS) systems have improved, however, scanning errors are not just becoming less frequent, they are also far less than a casual observer might expect – typically less than 1% of the retail price.

A hidden tax on consumers

Item pricing laws have been aptly categorized by researchers as a "hidden tax" on consumers, because retailers in item-pricing states pass the compliance costs on to customers. In truth, this is because there is a fractional cost of labor added to every product sold in the store in an IPL state. Indeed, retailers' costs are high – both in terms of compliance efforts and fines for non-compliance. The average grocery store sells more than 5 million items each year, and in larger retail venues, that may double or even triple. With the need to apply price labels to the vast majority of these items, economic analysis has estimated that IPLs add between six and eleven percent to the overall labor costs of grocery chains operating in these locales.

Christopher Flynn, the president of the Massachusetts Food Association, recently stated that his organization estimates that it costs an average grocery store between $150,000 to $300,000 annually to comply with that state's IPL. The regulations also restrict the ability of retailers to change prices, due to the fact that price changes necessitate additional physical labor. Indeed, analysis has shown that stores in IPL states change their prices far less frequently and place fewer items on sale than their counterparts in the rest of the country. Thus, rather than saving consumers money from the specter of inaccurate scanning, IPLs may restrict their ability to participate in sales and promotions, exacting another cost on consumers and retailers in these select states.

The impact of item pricing laws has been proven in scholarly research on the subject. In fact, a major study on the effect of item pricing laws was just published in the *Journal of Law and Economics*. In this project, the researchers compared over 3,000 prices in the tri-state region around New York City, tracking prices on like items in:

- New York (an item pricing state)
- New Jersey (a non-item pricing state)
- Connecticut (an electronic shelf labeling state).

The researchers found that prices in markets where item pricing was required were between 20 to 25 cents higher than prices on like items in states where item pricing was not required. In Connecticut, prices were found to be far less than in New York's item pricing environment. However, due to the costs involved in acquiring and maintaining the electronic shelf labeling systems, prices in this market were – on average – ten cents higher than those found in non-item pricing markets. The lead author of the study, Dr. Paul Rubin, a professor of economics and law at Emory University in Atlanta, recently pronounced in the *Wall Street Journal* that, "the laws are a bad deal for consumers."

As we rapidly approach the point where RFID labeling of individual items for retail sale will become both economically and technically feasible, item-pricing laws are an unfortunate reality that leading-edge retailers and the RFID industry – indeed the entire auto-ID community – need to be particularly aware of. Plain and simple – without repeal of these laws, there can simply be no ROI for RFID. Indeed, we will then have quadruple redundancy – shelf-level pricing (required in all states), item-level pricing, bar code labeling, and RFID tagging of items. Still, retailers and the RFID industry must be mindful that rather than seeing these laws as being even more outmoded with the introduction of RFID tagging of products, there will be a significant segment of the population that will see the simple, old-fashioned, ink-on-paper-on glue price tag as being even more essential with the new technology. Sadly, if consumers don't trust optical scanning, they are unlikely to 'take any more stock' in radio waves.

Thus, it will be incumbent for those in the retail and RFID industry to engage in consumer outreach and educational efforts to calm the fears of consumers and educate the general populace on the benefits that will come from the RFID-enabled "store of the future." To make that store an economic reality, however, it will take legislative-level outreach and lobbying efforts to make certain that laws promoting 19th-century product labeling will not hinder the adoption of the technology of the 21st century in any state or locale.

RFID makes every drop count at smart bars and restaurants

David Wyld
Contributing Editor, AVISIAN Publications

According to hospitality industry experts, every year in the United States, over $7 billion is lost due to "liquor shrinkage." What is "liquor shrinkage?" It happens when bartenders give out free drinks, overpour intentionally making drinks too strong, or make mistakes as they mix cocktails. It also happens when bottles of liquor disappear from bar storage areas due to theft. It all adds up to a major alcohol problem.

In fact, industry analysts project that liquor shrinkage across the hospitality industry affects between 20 and 30 percent of alcohol stock. For banquet and reception operations, losses may range even higher. Thus, solving the liquor shrinkage problem can be vitally important to restaurant and bar managers, as they can not only control costs, they can recover lost revenue from otherwise unpaid drinks.

Liquor shrinkage is creating a unique opportunity for RFID in restaurants and bars around the world. RFID can not only provide improved control over operations and inventory, but provide new levels of customer satisfaction in beverage service.

How "smart bars" work

Today, there are two primary competitors that are vying for share in this marketplace. San Francisco, California based Capton, Inc. and Scottsdale, Arizona based Nuvo Technologies, Inc. are marketing systems that use RFID-equipped pour spouts that are fitted on liquor bottles in bars and restaurants. With readers positioned in the bar environment and software that compiles the data and produces analytical reports, the "auto-ID" bar gives restaurant and hospitality managers new heretofore unprecedented visibility on this critical part of their operations. Each company's system (Capton's Beverage Tracker and Nuvo's BarVision) can be installed for $10-20,000 per location, and the early results show significant (and quick) ROI – measured in months, not years – and vastly improved operational control.

How will these systems work in practice? Today, when using either system, each bottle of liquor in the bar inventory must be fitted with a reusable smart pour spout containing a battery-powered RFID tag. Currently, this is a task that must be performed by the employees of the restaurant or bar after their liquor stock is delivered to them. However, one could certainly see that when there is an industry standard, such smart pour spouts could be attached by liquor distillers and producers, or even distributors or service specialists. Both companies' smart pour spouts can be washed and used for thousands of cycles. The battery power source for Nuvo Technologies BarVision smart spout has an expected lifespan of three years, while Capton's Beverage Tracker is

RFIDNews

projected to have a lifespan of up to a decade. And with the smart pour spout at the air-filled top of the bottle and the use of active tags, there are no real readability concerns with the systems, which operate in the 418 MHz range.

Physics is key to the operation of both systems. In a free pour environment, in order to mix a drink, the bartender must tip the bottle in order to pour from it. The tipping of the bottle "turns on" the smart pour spout when each drink is mixed, and in essence, it enables the system to measure the volume of liquor poured before the employee tips the bottle back up, which ends the process of making that drink. The smart spout then instantly transmits the information on the pour to the RFID reader positioned above the bar (or in the case of a larger facility, the nearest reader). The information on each pour is then transmitted from the receiver to the bar or restaurant's computer system, which is integrated with the vendor's proprietary software that compiles bar and bartender-specific data.

In the case of Capton's Beverage Tracker, there is a flow measure device built-into the smart pour spout, which measures the amount of alcohol poured. It thus records the volume, type of liquor, and the date/time of the pour. Nuvo Technologies uses a different technique, whereby the spout simply transmits the total time of the pour and the angle of the tipping of the bottle. This data is then matched to the type of alcohol in that particular bottle in its BarVision Global software for PCs, which then matches the serial number of the RFID tag to calculate the volume of alcohol poured in each instance to the restaurant's or bar's database (containing information on the date, price, quality, etc. of all tagged bottles).

According to Christopher Morrison, President of Nuvo Technologies and Chief System Architect of the BarVision system, such smart pour systems will provide hospitality managers with – for the first time – "automatic, real-time liquor usage information." The bar management software can provide not only journal-like reports that detail sales chronologically or by bartender/shift, but detailed analytical reports on:

- Overall liquor costs/inventory
- Bartender performance analytics
- The number of pours from a given bottle, liquor brand, or price category
- Overpours and other exceptions
- Serving/purchasing trends
- Promotional impacts
- Liquor stock utilization and out-of-stock/reorder alerts.

Both Capton and Nuvo have made their software compatible with PDAs so that managers can access the information in real-time on the bar floor or anywhere in the world via web interface. Both firms' reporting and analytical capabilities are robust, providing new metrics for bar and restaurant management.

How can such reports be utilized to improve hospitality management? Take the example of the Marriott Atlanta Perimeter in Atlanta, Georgia, which is an early user of the Capton system. The hotel's Assistant General Manager, Peter Byers, spotlighted that one of the chief non-financial benefits of such systems is to better assure drink consistency. Byers commented that in today's competitive environment, "the importance of mixology standards and bartender adherence to drink preparation in the ever growing list of specialty cocktails is high." Using the reporting capabilities of such systems, hospitality managers can detect not just overpours, but wrong pours, where mixed drinks were being made incorrectly. If patterns emerge over time, management can pinpoint both bartenders that perhaps need more mixology training and also gauge the effectiveness of their training and development programs for bar staff.

RFID is rapidly spreading in the hospitality industry

What is the market potential for such "smart bar" systems? There are literally millions of bars, clubs, and restaurants globally that have what is referred to in the hospitality industry as a "free pour environment" – in which a human bartender, rather than a machine, mixes drinks. While the smart bar systems are certainly feasible for use in individual restaurants and food service chains, the interest in the technology will reach much further. Casinos, stadiums, large hotels and even cruise ships are proving to be prime venues for such systems. Installations have already been performed at several large venues, including the mammoth Treasure Island Hotel & Casino in Las Vegas and the newly built Island View Casino in Gulfport, Mississippi. Systems have also been installed at large hotels, including:

- Hyatt Regency McCormick Place (Chicago, Illinois)
- Sandestin Golf & Beach Resort (Sandestin, Florida)
- The Barclay Intercontinental (New York City, New York)
- Marriott Atlanta Perimeter (Atlanta, Georgia).

Even though U.S. firms are developing the technology, it will have a world-wide impact. Nuvo Technologies recently announced that it is partnering with Infosense Technologies to market the BarVision system in India, which has already installed the system at several Bangalore restaurants, including 1912 and Olives.

Thus, as more and more bars and restaurants around the world turn to RFID-equipped smart pour spouts, the smart bar is more than just a smart investment to improve inventory control and manage the actions of bartenders and other service personnel. It is more than simply employing RFID in a cost-effective, innovative manner to deter "liquor shrinkage." Rather, it is a great opportunity for the hospitality business to experiment with new ways of managing with the better visibility and analytics that auto-ID technology can provide.

Brain.

iCLASS
by
HID

Trust.