re:ID

Fall 2007

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

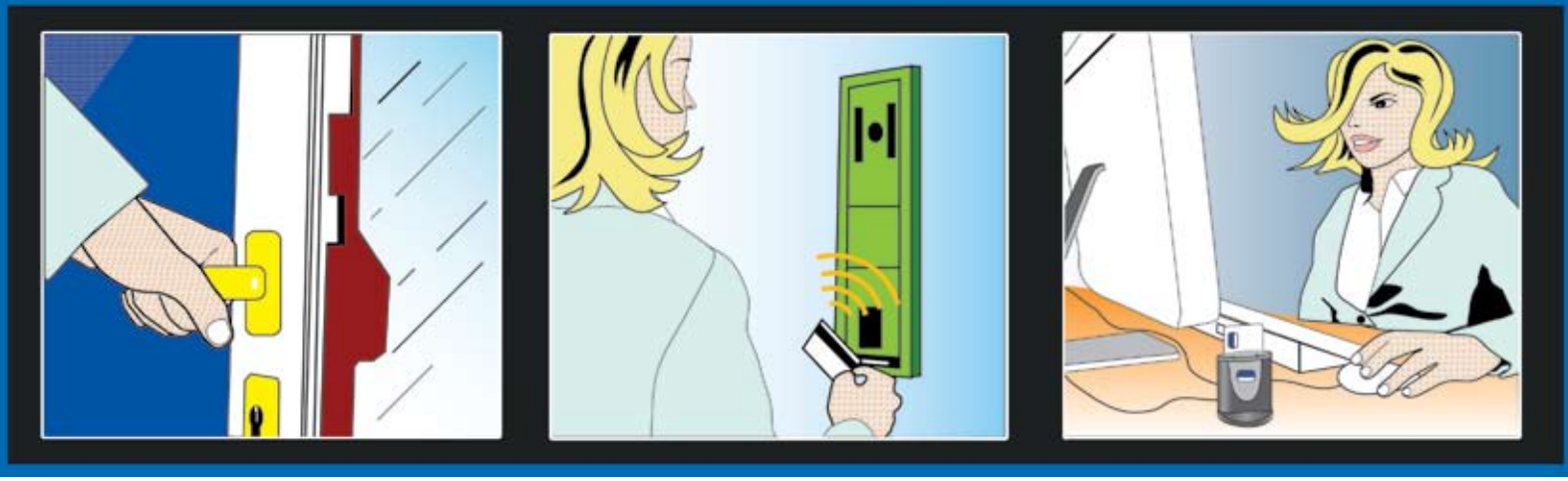
Security convergence becomes corporate mandate

NYC and Utah use branded contactless cards for transit

Matrix codes are 'not your father's barcode'

Contactless cell phone payments debut at Pennsylvania campus

Reverse image vs. direct to card ID printers



AVISIAN

" Trustworthy "

zero guess work. just **verified.**

INSTANT ON THE GO IDENTITY VERIFICATION.

VERIFY ID CARDS ANYWHERE FROM PARKING LOTS TO PORTS. ADD PHOTOGRAPHS OR FINGERPRINT CHECKS TO CARD SYSTEMS. GIVE LAW ENFORCEMENT OFFICERS A WAY TO SCREEN SUSPECTS AGAINST FINGERPRINT DATABASES WITHOUT RETURNING TO HEADQUARTERS.

DATASTRIP'S DSVII MOBILE CARD READER:
THE SOLUTION FOR WIRELESS IDENTITY CHECKS.

be trusted.

DATASTRIP

800.548.2517
www.Datastrip.com

Pick a Card...

LEGIC®
innovation in ID technology

Not Just **Any** Card

Pick the **LEGIC** contactless smart card. Already chosen by companies around the world, more than 70 million people use **LEGIC** at work and play. Learn how your employees and visitors only need one ID for multiple applications. Ask for **LEGIC** inside!

It's **Innovative.** It's the **Future.**

LEGIC®
innovation in ID technology

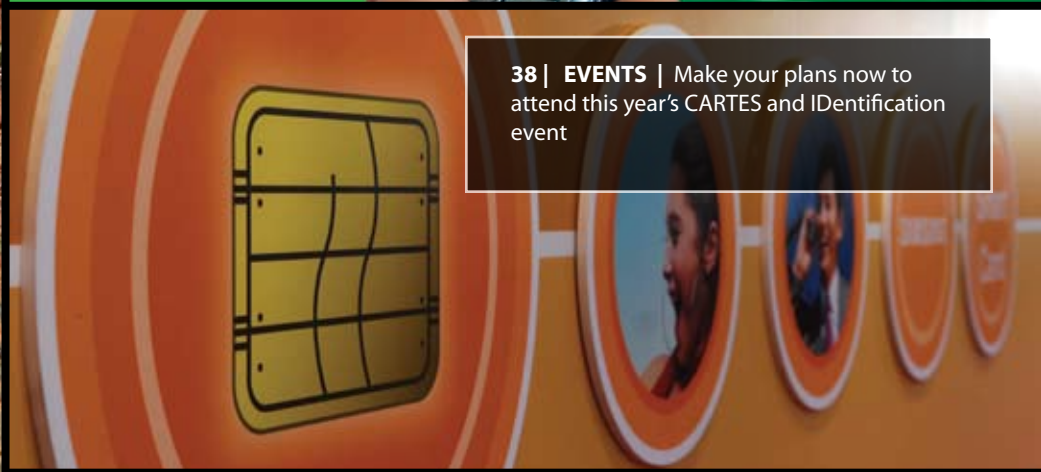
www.legic.com ph: (630) 717-5843

Fall 2007

| CONVERGENCE |

Contents

INDEX OF ADVERTISERS



One key, many doorways: Convergence has arrived

Chris Corum
Executive Editor, AVISIAN Publications

One of the best things about publishing online is that all past articles are archived via the web (our family of ID technology publications has produced more than 7,000 individual pieces of content in the past five years). So when I want to look at the historical progression of our coverage of a particular topic, it is quite easy for me – or for you – to do.

So as I began to consider this editorial on the convergence of physical and logical security, I looked at our prior coverage of the topic. We first started writing about convergence way back in 2003. In those early days, we discussed the topic almost as an oddity, noting that some forward-thinking companies were beginning to consider merging the building access and network access credential.

Soon after, the political challenges occurring within organizations over control of the credential took center stage. We explored the push and pull between those responsible for physical security within the organization and those in charge of IT.

To this point, the focus was on the credential as the point of convergence but that was changing just as the nature of the credential was changing. As you will see in this issue, ID technology is not just about the traditional 'card.' One article details how a Pennsylvania campus is issuing a contactless tag to turn the mobile phone into the credential. An interesting article on a new generation of barcodes, called matrix or QR codes, explores how an image can be an ID. And we explore some exciting ways that biometrics and new on-card display technology are changing the nature of the credential.

Moving to the third wave of our editorial coverage of the convergence revolution, the industry is recognizing that the real obstacle and opportunity is in the major systems that manage the enterprise, controling the identity and lifecycle of the employee, student or member within the organization. More than the credential, these systems have become the focal point of convergence efforts.

So here we are more than four years into our coverage of convergence. In this issue, our editorial team takes a look at the topic from the both IT perspective and the access control perspective, we talk with several companies actively working to help organizations achieve convergence, and we explore steps an organization must take to make it happen.

I hope you find some insight that can help you advance your organization's goals. Enjoy.

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

CONTRIBUTING EDITORS
Nate Ahearn, Daniel Butler, Ryan Kline, Marisa Torrieri, Andy Williams, David Wyld

ART DIRECTION TEAM
Darius Barnes, Ryan Kline

ADVERTISING SALES
Angela Tweedie, angela@AVISIAN.com
Chris Corum, chris@AVISIAN.com

SUBSCRIPTIONS
Regarding ID is free to qualified professionals in the US For those who do not qualify for a free subscription, or those living outside the US, the annual rate is US$45. Visit www.regardingID.com for subscription information. No subscription agency is authorized to solicit or take orders for subscriptions. Postmaster: Send address changes to AVISIAN Inc., 315 E. Georgia Street, Tallahassee, Florida 32301.

ABOUT REGARDING ID MAGAZINE
Regarding ID is published four times per year by AVISIAN Inc., 315 E. Georgia Street, Tallahassee, Florida 32301. Chris Corum, President and CEO. Circulation records are maintained at AVISIAN Inc., 315 E. Georgia Street, Tallahassee, Florida 32301.

Copyright 2007 by AVISIAN Inc. All material contained herein is protected by copyright laws and owned by AVISIAN Inc. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopy, recording or any information storage and retrieval system, without written permission from the publisher. The inclusion or exclusion of any does not mean that the publisher advocates or rejects its use. While considerable care is taken in the production of this and all issues, no responsibility can be accepted for any errors or omissions, unsolicited manuscripts, photographs, artwork, etc. AVISIAN Inc. is not liable for the content or representations in submitted advertisements or for transcription or reproduction errors.

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

STRENGTHEN SECURITY, PROTECT BUDGETS

INTEGRATED ID SOLUTIONS

DISCOVER WHY SECURITY PROFESSIONALS TURN TO DATACARD FOR A TOTAL SOLUTION

With ID card solutions from Datacard Group, you can enhance your security program without sacrificing your budget. That is why corporations, governments and other organizations make Datacard® the world's best-selling brand of photo ID solutions.

We offer everything you need to issue ID cards quickly and efficiently. We integrate and test every component for seamless compatibility. So, you can expect outstanding power, performance and value.

To learn more, call +1 800 356 3595, ext. 6623.
Or visit us at **www.datacard.com/ID**.

PHOTO ID SYSTEMS

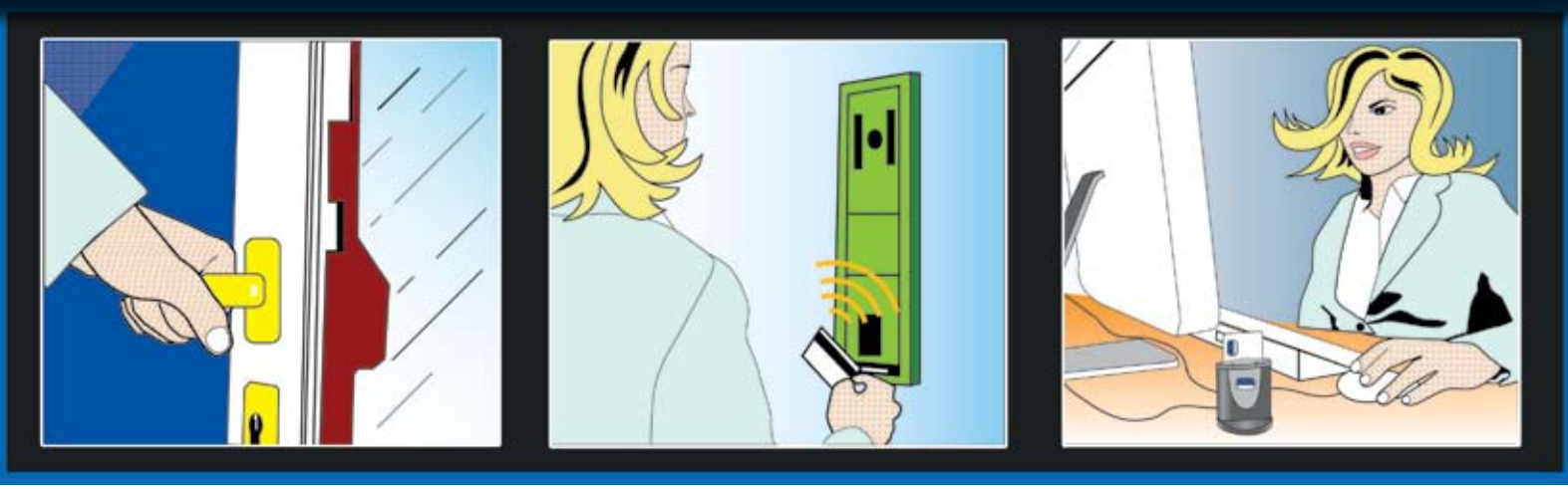
CARD PRINTERS

ID SOFTWARE AND CAPTURE SOLUTIONS

SUPPLIES

DatacardGroup
SECURE ID AND CARD PERSONALIZATION SOLUTIONS

©2005-2006 DataCard Corporation.
All rights reserved.



Convergence of logical and physical security moves from industry 'buzzword' to corporate mandate

For enterprise and government markets, networking companies are opting to converge and fine-tune access control applications

Marisa Torrieri
Contributing Editor, AVISIAN Publications

Depending on your frame of reference, the term "access" conjures thoughts of very different applications. Traditional building security or access control professionals think of physical access. The IT community thinks of logical access to computers, networks and systems. But it's actually the convergence of logical and physical access that presents the biggest opportunities and challenges to both enterprises and industry.

Convergence has been *the* buzzword in security for several years now, but it is rapidly moving from the chalkboard to the implementation list for cross-sector organizations. According to Forrester Research, spending on merging physical and logical access control in both the public and private sectors will increase to more than $7 billion in 2008.

This projected growth is driven in large part by HSPD-12 (Homeland Security Presidential Directive 12), the presidential mandate that requires all federal agencies to start issuing new identification cards based on the FIPS 201 standard.

But it is not just the federal government that is spending on convergence. Corporations, health care, higher education, and other levels of government are also keeping companies that specialize in one or more aspects of converged security busy.

The evolution of convergence

Before one can understand the emerging challenges and market opportunities for converged access control systems, one must first understand the differences between logical and physical security. Physical access control, traditionally managed by security personnel, refers to the granting and restricting of access to buildings, facilities and borders. Logical access control refers to the granting and restricting of access to electronic environments.

Logical access involves securing intellectual property, data, communications, and information processes, adds Peter Beardmore, product marketing manager for RSA Security. The authentication point may occur at the machine, network, domain or application-level, and authentication is based on the users' credentials.

Convergence is a common phrase given to the practice of combining or streamlining physical and logical credentialing and access control. The result is more secure, efficient and manageable systems that protect against identity spoofing (and can potentially identify or prevent security breaches).

With projects like HSPD-12, a centralized credentialing process in an environment of multiple credentials introduces challenges for technol-

PIVMAN

Handheld device
by DAP Technologies
www.daptech.com

Is he legit? Are you sure?

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

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

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

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

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

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

TSGP
PSGP
IBSGP
BZPP
SHSP
UASI
LETPP
MMRS
CCP
EMPG

CoreStreet ENABLED

2007 CoreStreet, Ltd. All rights reserved. CoreStreet and the CoreStreet logo are registered trademarks of CoreStreet, Ltd. The PIVMAN System and the CoreStreet Enabled logo are trademarks of CoreStreet, Ltd. All other trademarks are property of their respective owners.

174_0207

CORESTREET®

ogy managers, Mr. Beardmore says. Men and women in these roles must ensure that federal agencies' systems are interoperable with mandated technology as well as other existing systems.

"When we talk about convergence of physical and logical security, we could be speaking from a few different perspectives," says Mr. Beardmore. "It could be a single device that authenticates me to the front door [and then lets me] log onto my computer. I use a smart card with the traditionally contactless physical credential and a digital certificate that authenticates me to a variety of electronic resources inside the building."

Much of RSA's customer base uses SecurID one-time password tokens to access virtual private networks or remote applications such as web-based e-mail. Some of its banking customers such as E*Trade use tokens for authenticating customers into web banking and trading.

Card management systems facilitate enrollment of the user, request credentials, issue the smart device (e.g. a smart card or other chip-enabled token), and then manage those credentials through their lifecycle, Mr. Beardmore says.

Growing market sophistication suggests convergence has become more than just talk

Another provider of solutions for converged systems, ActivIdentity, says its corporate customers are exploring ways to upgrade to more sophisticated converged physical and logical access systems.

"There are now identity management systems like ones from Sun and Oracle that are looking at managing the whole process of provisioning a new employee, whether it's physical access or the different applications they need to have access to," says Ed MacBeth, vice president of marketing and business development for ActivIdentity.

As convergence matures beyond the early, basic concepts of a single access point, token, or credential the more robust challenges emerge. How do we provision the credential in a coherent, streamlined process? How do we update privileges and manage the lifecycle of the applications on that credential? How do we revoke certain privileges or an entire credential?

These issues point to the real challenges surrounding convergence – the "care and feeding" of the host of enterprise-wide systems that exist within an organization.

ActivIdentity is currently on board to provide the logical access component to EDS as part of the General Services Administration's Shared-Service Provider Program for the FIPS 201 initiative.

Now that FIPS 201 is coming, "these access cards are no longer proprietary cards," says Mr. MacBeth. "Rather than being provided by the physical security provider or reseller, those cards will be issued by either government agencies that are running their own system or by the GSA managed service (office) that EDS is running. So now, having a card that is based on a single, smart card chip design that can be used for physical and logical access means there is going to be a change in the readers that are on the doors everywhere. They'll be switched out to read the ISO 14443 (contactless) interface."

In other words, this change to standardized contactless technology for physical security takes the ID card out of the control of the traditional security manager and supplier, opening the floodgates for converged systems.

"What tends to happen when we engage in new opportunities," says Mr. Beardmore, "is we're asked to take a look at an incumbent system to assess interoperability. In some cases, proprietary applications are in place and this may or may not be feasible. But even when it's not, it illustrates that a comprehensive credentialing and credential management strategy is needed."

Moving from concept to reality brings growing pains

As convergence becomes more than just a buzzword in government agencies, institutions, and corporations around the globe, its real challenges are coming to light.

Industries and organizations are making progress on the initial battle over who controls, owns, or issues the credential. While this debate between physical security and IT departments is not finished, many organizations have come to a truce recognizing that both groups can get what they need from a properly managed program.

Now the hard work begins … developing the cross-departmental data sharing, update, access and authentication that must occur constantly and in real time for true convergence to be achieved.

Progress continues as leading vendors and issuing organizations prove that convergence is more than a buzzword, it is real.

ASIS
Booth 2649
Booth 1697

How do you fit a global security network into the palm of your hands?

[Hint: it takes the right partners and technology.]

Deploy everywhere. OnGuard enables security solutions of any size, any complexity, in 18 languages.

Global reach. Lenel's premier value-added resellers provide extensive coverage and support to over 15,000 system installations in 93 countries.

Experience the freedom of open standards. Lenel's standards-compliant platform ensures integration with best of breed hardware and software for your operations. Today, and tomorrow.

Rest assured, OnGuard never sleeps. Lenel solutions deliver five nines reliability (99.999%), allowing you to focus on your business rather than your security system.

Check out the complete OnGuard® 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

LENEL
A UTC Fire & Security Company

©2007 Lenel Systems International, Inc.

New fingerprint reader brings biometrics to consumer desktops

The Eikon from UPEK makes biometric authentication within reach of the masses via availability on Amazon.com and other high profile channels

Ryan Kline
Contributing Editor, AVISIAN Publications

The new Eikon biometric fingerprint reader from UPEK has a sleek look and is within reach of individual as well as corporate users. At just $39.99 at Amazon.com, it seems a cost effective option to secure a computer with this simple USB add-on device. I gave it a try to see if it really was easy to install and convenient to use …

It was hard to imagine that such a small, thin layer of silicon could reliably read a swiped finger, but I had to start by getting it installed to find out. Brian DeGonia, software product marketing manager for UPEK, explained that area sensors (the larger silicon or infrared sensors often seen in movies) are extremely easy to use, but come at a high cost. "When inserting it into a small unit, such as the Eikon," he said, "it is much more cost effective to use a small strip of silicon and have the user move a finger over the reader, capturing the fingerprint."

The Eikon comes with an installation CD and claims to be an easy install. I found that to be true for PC installation, though support for Macintosh is currently not available. But Mac friends, Mr. DeGonia told us, "we are working on Macintosh compatible software right now. It is in the works."

An installation wizard guides you through the steps necessary to enroll and use the biometric reader with the PC. First, you enter your Windows password, and then scan your fingerprint in order to associate the two.

Once the device has been registered, logging in to Windows is a breeze. All you have to do is swipe your finger and Windows automatically detects the login from the reader. Biometric login is as easy as that.

The system allows for multiple users to be registered on one computer. When multiple users are registered, the computer automatically logs in the user presenting his fingerprint. The Eikon can also be used for fast user switching when someone else is logged in.

Learning to slide

If you can master the "biometric slide," then this strong authentication device can help keep your workstation secure. My challenge from the beginning was to get a good, readable swipe of my finger. I learned that it has to be a slow and controlled motion … not too fast and not too far to the right or left. It may take a bit of practice, but I was soon getting reliable reads on first attempts. For some users it may take several attempts to log in, but if security is what you are looking for, this is a great affordable compromise.

Managing passwords

Do you need help remembering all those different passwords for websites that seem to always evade you when you need them most? The Eikon can help here too. "Our main position is to reach out to people and solve the password problem that haunts so many of us," said Mr. DeGonia. "We also wanted to make the same security available at home that many people have at their work."

The Password Bank allows users to program the Eikon to be used in conjunction with password-protected websites. Registering websites is fairly straightforward. From the web browser, you swipe your finger when you are at an account login screen. This launches the Biomenu applet that walks you through the

simple process of entering user information that is then tied to your fingerprint. When you return to the login page on the site in the future, a swipe of your finger will automatically log you in.

The Protector Suite QL with the Eikon reader has many other add-ons or options as well. Users can encrypt file folders that can only be unlocked with their fingerprint as well as associate a finger to an application so that, for instance, when you swipe your pinky finger, it could automatically launch your favorite game.

Security still prevails

Mr. DeGonia said that the Eikon captures "between 20 and 30 points, the FBI only requires 8 common points to confirm a fingerprint match."

"The Eikon does all of its processing in the reader, so the fingerprint image and the algorithm never use the computer for processing," said Mr. DeGonia. This limits vulnerabilities where attacks could occur within the external PC or networked environments.

The reader can be co-branded, which according to Mr. DeGonia is one of their main marketing platforms, and there already are "quite a few partners that create applications such as single sign-on and hard disk encryption software."

While the Eikon may have slashed prices, it did not slash security. With over 20 points being sampled per each slide of a finger, the biometric authentication is strong. The only drawback is that it may take a bit of practice to get reliable reads ... and that "biometric slide." ID

InCard puts the OTP on the card itself

Andy Williams
Contributing Editor, AVISIAN Publications

Innovative Card Technologies (ICT) calls its InCard product "a smarter card." It can do everything a payment, access or ID card can do, while providing the authentication and one-time password functionality usually reserved for tokens. But it didn't start out that way. Originally, the company was making credit cards with an on-board magnifying lens.

Today, the InCard is a one-time password generation card that's ideal for today's two-factor authentication world. The brainchild of Alan Finkelstein, president, founder and director of ICT, the password-generating card won't hit the market until later this year.

"Normally when you go to your online banking account, you put in your name and static PIN (or password) which could be your dog's name, all which could be easily compromised," he explained. That process is ripe for online theft and is why the Federal Financial Institutions Examination Council (FFIEC) suggested that all financial institutions implement two-factor authentication.

With the ICT card, dubbed the "InCard," a person would still log on to his online bank, enter his static password, but then he would enter the one-time pass code generated by the card.

The number generated by an InCard is good for just one transaction. "This satisfies dual factor," he said. So even if someone stole the person's ATM card and his ICT DisplayCard, the thief would still be locked out because he would need the person's login name and static password.

The InCard has a small button that's flush with the surface of the card. Push it, and a number is generated in a small display on the card.

A back end server identifies the pass code as coming from that particular card. "There's a counter in the chip, and it knows it's been pressed, for example, 6,400 times. If it's really me, the number should be that number," he said. "Depending on how many digits (in the resulting code), 6 to the 10th power, or 8 to the 10th power, you could have a hundred million possibilities" every time the code is generated, he added.

Beginning with a magnifying lens …

As Mr. Finkelstein explained it, he started experimenting with cards in 1993. His original idea was to place a magnifying lens in credit or ATM cards. His intention was that people (such as those who need reading glasses) could more easily examine a restaurant bill with the same card.

"I first had an agreement with one credit card company, then I walked into Chase Bank" to sell it on his LensCard idea. It was, as he later described it, "the luckiest day of my life."

That was when he met John A. Ward, III, who was then CEO of Chase BankCard Services.

"John believed in us enough and while it took us many more years, in 1998 Chase started issuing cards with a magnifying lens."

While Mr. Ward didn't pair up with Mr. Finkelstein right away, "John and I developed not only a professional but a personal relationship," added Mr. Finkelstein.

Mr. Ward later went on to several other jobs, including chairman and CEO of Doral Financial Corporation and Chairman and CEO of the American Express Bank, President of Travelers Cheque Group, before he joined ICT as its chairman in October 2005. About a year later, he also assumed the role of Chief Executive Officer.

Meanwhile, his LensCard now included a light. It was at that point that Mr. Finkelstein said he "made the difficult decision to stop marketing the LensCard and to figure how to put power into a card." The LensCard is still available, however.

"We first put a battery with a straight circuit to an LED light, but we didn't know where the killer application was," he said. "We developed a chip that could produce sound that could play Jingle Bells or happy birthday." But it wasn't until he saw a key fob that could be used either

for generating passwords or as a payment vehicle that he thought he had found the application for which he was searching.

The chip for the ICT DisplayCard was "developed from scratch. There was no chip that would do what needed to be done. That was a major issue. The first barrier we had to overcome was power consumption. Even when they're asleep, they need power to run. We tried to figure out how to miniaturize that and put it in a card form factor and that's how it came about," he said.

"Alan was the first person to put functionality into a piece of plastic," added Mr. Ward.

"Whether it was luck or the planets were in alignment, when the two-factor authentication suggestions came out from FFIEC, it made it easier to enter the market," said Mr. Finkelstein.

One drawback, if it could be called that, is the card's cost … $12, as compared to the 35 cents or so that it costs to produce a standard credit/debit card. "Where this card would be used the most is with online banking, in certain segments of the market involving sizeable accounts, or with online securities trading," commented Mr. Ward.

"If you break the cost down to a dollar a month, it doesn't sound too expensive," said Mr. Ward. "I will not use a business center in a hotel or WiFi in an airport when I do online banking. For me, I'd be more than willing to pay $1 a month to have that extra level of security." And who knows? Maybe the bank would even absorb the cost of the card, added Mr. Finkelstein.

Manufacturing the InCard

The card itself isn't patented. "Our protection comes with the display, the chip and the process. It's not a general claim with any card generating a one-time pass code. We have a license with a company that has a patented lamination process. The way cards are built today require a lot of heat and a lot of pressure and we also have protection on the chip inside."

Thanks to a relationship with Switzerland-based card manufacturer, NagraID, a high volume production of the ICT DisplayCard is feasible. "They are our strategic partner. We provide the module and they build the card."

"The process is cookie cutter and hopefully we can produce in much larger volumes when we have to," said Mr. Finkelstein, who expects to sell a million cards over the next 12 months. "We're pretty confident we are going to take away a part of the market share from key fobs."

He said there are currently about 45 million key fobs in circulation and the number is growing dramatically. He believes one of the major advantages the InCard has over key fobs is that "people tend to leave their bulky key fobs in their office or at home, and they don't have it when they need to use it." He views the ICT DisplayCard as "a companion card to an ATM or credit card," although it can also serve as the credit/debit card itself.

Major issuers and industry leaders have joined the bandwagon

"Major banks in Europe, Latin America, the US and Asia are all in tests (with the InCard)," he said. Our test in Latin America even has an EMV chip in it." ActivIdentity, a provider of digital identity assurance solutions, has agreed to sell the card and one of the better known web security companies, VeriSign, has signed on as well.

ActivIdentity's reseller agreement with ICT will get the cards into the e-banking, e-commerce and data access authentication markets. The company plans to offer the card with its 4TRESS Authentication server to facilitate a cross-platform security solution for financial institutions. The result is a customer authentication solution that works for all types of customer transactions (payment, debit, login and transfers) at any point of access (online, ATM, phone).

VeriSign will help companies fortify their online commerce applications with VeriSign Identity Protection (VIP) coupled with the InCard. By integrating the card with VIP, the two companies will add a portable new token form factor to VeriSign's authentication network.

In addition, Inteligensa Group, a Latin American manufacturer of card-based solutions for financial applications, announced earlier this year that it will become a reseller of the ICT DisplayCard, offering it to its 150-200 client financial institutions for one-time pass code authentication. Inteligensa has regional branches in Brazil, Mexico, Colombia and Venezuela, and sells 180 million cards annually, or 35% of all bank cards in Latin America.

While the company appears ready to take off with its new card technology, it remains relatively small with 26 employees. "(Our) proof of process lab in Florida is where we first come up with the concept and built the prototypes (for new card varieties)," Mr. Finkelstein said. "We have a roadmap going out three years. This will be the first of many applications to come."

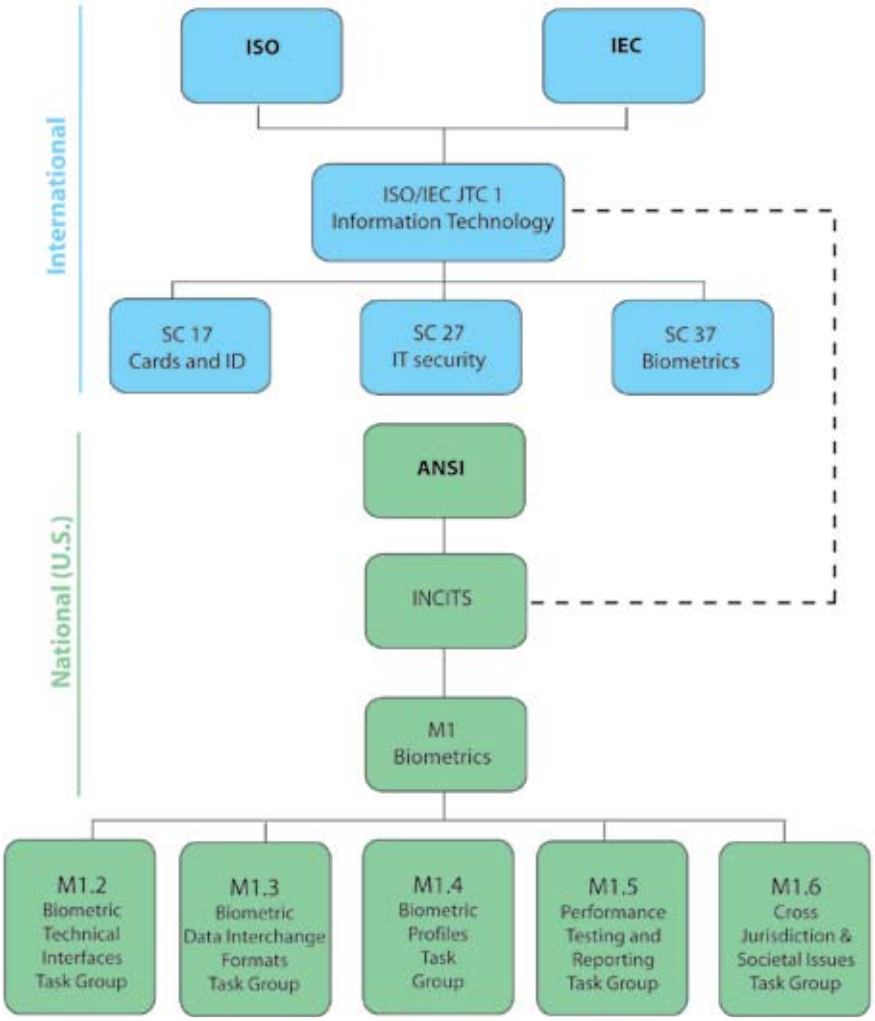
The maturation of biometric standards

Russ Ryan
Vice President, National Biometric Security Project

Numerous national and civilian security applications will see improvement in functionality because of newly published biometric standards. Biometrically-enabled passports will be made more robust because of new standards that define a general specification for physical characteristics, layout and security. A new FBI Electronic Fingerprint Transmission Specification standard helps ensure the reliability and quality of fingerprints submitted to the FBI. A new biometrics standard for financial services defines the security framework for using biometrics for authentication of individuals in financial services transactions. Additionally, a new testing methodology standard provides specific details on methods and techniques for conducting scenario or technology tests.

As biometrics become an evermore critical component of next generation identity assurance and risk management systems deployed in the protection of the civil infrastructure and personal identity, the continued development of comprehensive biometric standards is vital to ensure interoperability, scalability, usability, reliability and security.

Figure 1. Biometric Standards Bodies



Before we look at the structure of biometric standards let us quickly review the key standards bodies. Figure 1 illustrates many of the national and international standards bodies that contribute to standards development. For the purposes of this article we will focus on a few key organizations.

The International Organization for Standardization (ISO) is the world's largest developer of standards. It is composed of representatives from the national standards bodies of approximately 150 countries with a central secretariat based in Geneva, Switzerland.

The International Electrotechnical Commission (IEC) was one of the first standards bodies to be established, founded in 1906. Its mandate is to prepare and publish international standards for all electrical, electronic and related technologies. In the information technology arena, which includes biometrics, most of this work is done in conjunction with ISO through the Joint Technical Committee (JTC) 1.

ISO/IEC Joint Technical Committee 1 (JTC 1) is a cooperative effort between ISO and IEC. This committee covers all standardization within the arena of information technology. It has multiple subcommittees (SCs), several of which cover biometrics. SC 17 is responsible for cards and personal identification and thus is particularly focused on the application of biometrics to smart cards and travel documents. SC 27 is responsible for IT security techniques and thus is focused on security issues and implication around biometrics. SC 37, however, holds the main responsibility for biometric standards.

ISO/IEC JTC 1 - Subcommittee 37 "Biometrics" (SC 37) is the subcommittee of JTC 1 that has the primary responsibility for developing international biometric standards. Its scope of work is defined as "standardization of generic biometric technologies pertaining to human beings to support interoperability and data interchange among applications and systems. Generic human biometric standards include: common file frameworks; biometric

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 US 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: ❑ US (FREE) ❑ *Other (US$45) _____

Phone _____

Email _____

Signature _____ Date _____

* Non-US 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

application programming interfaces; biometric data interchange formats; related biometric profiles; application of evaluation criteria to biometric technologies; methodologies for performance testing and reporting and cross jurisdictional and societal aspects." SC 37 is the international counterpart of the INCITS M1 body in the US.

International Committee for Information Technology Standards (INCITS) is the primary US standardization body in the field of information and communications technologies. This includes information storage, processing, transfer, display, management, organization and retrieval. INCITS has a number of Technical Committees (TCs) that lead standards development efforts in various areas. In fact, there are more than 30 TCs within INCITS, including several that touch on biometric standards. The TC that focuses most prominently on the development of biometric standards is known as M1.

INCITS Technical Committee M1 Biometrics (M1) works to ensure a high priority, focused and comprehensive approach to the rapid development and approval of formal national and international generic biometric standards. M1 is the US Technical Advisory Group (TAG) to its counterpart in the international arena, SC 37.

The structure of biometric standards

It is helpful to think of biometric standards as a series of layers, like those of an onion. Starting at the center, the first four layers cover those standards of direct relevance to biometric system developers and companies. The next layer deals with the interfaces, which link the biometric components to the rest of the system. The outer two layers define how we deal with biometrics in terms of privacy, legal issues and even the language we use to describe it. Finally, there are the thin shells that separate and surround each layer. These represent the conformance standards, which describe exactly how adherence to each of the other standards can be measured. *(See Figure 2, p.20)*

Data interchange formats

The inner core of the onion comprises the biometric data interchange formats. These define the basic format of biometric images or templates and tell the technology manufacturers how to format data from their systems or interpret data coming into their systems.

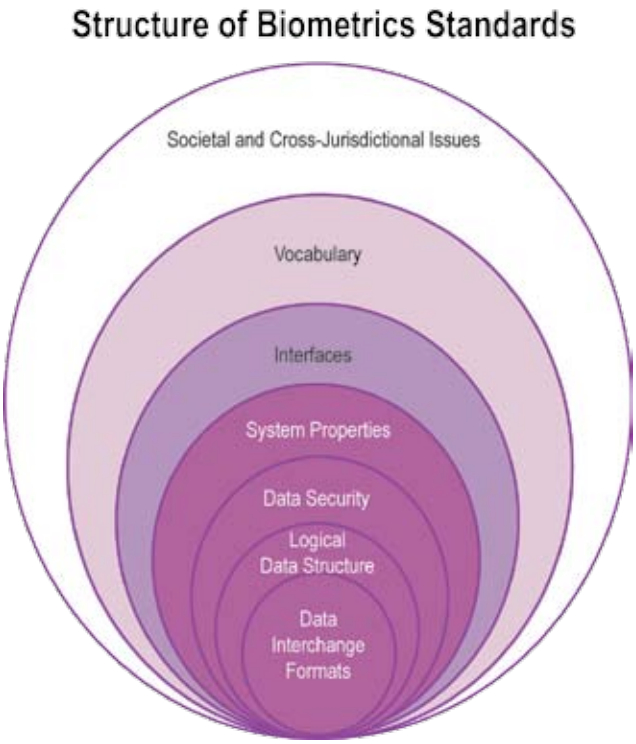
Logical data structure

The next layer is the logical data structure or exchange format framework that is used to wrap the biometric data so that systems receiving a file know how to interpret the different data fields that may be associated with the biometric data. These might include demographic information or a digital signature to verify that the data packet has not been tampered with.

Data security

Once the core biometric data in a standardized form has been wrapped in a standardized file format, it may be necessary to protect the data.

Figure 2



This may involve the use of digital signatures and other encryption techniques.

System properties

The next layer involves the properties of the biometric system. One of these is the performance of the biometric system, which is fundamental to deployment decisions. If the biometric system cannot enroll a sufficient percentage of the target population or if its ability to correctly match biometric samples from the same person without falsely matching samples from different people is insufficient, then the system is unsuitable for deployment. Over the last year, significant progress has been made in advancing biometric performance testing standards, both in the US and internationally. Several additional standards will be ready to publish in the near future.

One of the key purposes of biometric standards is to allow interoperability among components and systems involving biometrics. Performance-based interoperability testing is thus important because it allows a determination not only of the fact that two systems can work together but of how well they work together, a critical factor in system design and procurement decisions.

Interfaces

Biometric interfaces form the next layer. These are the interfaces between the core biometric systems, represented by the inner four layers of the onion, and the outside world. As interface standards continue to develop, it will be important to ensure that there is proper coordination between the biometrics experts and experts in other areas of information technology, ensuring that the technical interfaces being developed adequately reflect modern system design principles and requirements.

Vocabulary

The final two layers of the onion represent the outside world and how we deal with biometrics as a general subject. A harmonized biometric vocabulary allows different groups to avoid miscommunication when discussing biometrics. General industry practice has accepted particular usages of certain terms, so that even if they are not agreed upon in a standard, there is a de facto agreement outside the standards process.

Societal and cross-jurisdictional issues

Societal and cross-jurisdictional issues involve the impact of biometrics on privacy, health, safety and other similar areas. Within each country or region there are different legislative issues and public perceptions that may influence how biometrics are used. The key goal here is to try to develop a standardized way of measuring or managing these issues and, if possible, a set of minimum guidelines that can achieve sufficient consensus to be internationally standardized. The international standards in this area will be particularly important for the deployment of large-scale cross-border systems.

Conformance testing

Finally, surrounding and pervading the entire onion is the issue of conformance testing standards. Most standards in any of the other areas do not provide a formal method for certifying that a particular technology or product conforms to the standard. The vast majority of standards, however, do benefit from a detailed conformance testing standard, an area which will require a great deal of work over the next two years, since the work on developing conformance testing methodology standards is still at an early stage.

Conclusions

The standardization process has reached a reasonable level of maturity in the US. A few years ago there were ten published biometric standards. Today there are more than 50 with another 50 in development spanning all the major subject areas. With the development of conformance testing standards what was once a major gap in the standards portfolio is now starting to close. There are either published or emerging biometric standards that address almost every major fundamental aspect of biometrics.

Over time, more technologies are being addressed. New data formats for speaker recognition in M1 and DNA in SC 37 are currently in development. Conformance testing will be critical for the many large-scale international deployments of biometrics where the data created in one country must conform to the SC 37 standards to enable the data to be read and used by another country.

Spreadsheets of all currently published standards and many more emerging biometric standards are included in the National Biometric Security Project's latest review of biometric standards activity, "Summary of Published and Emerging Biometric Standards – 2nd Quarter, 2007." Both the spreadsheets and the Summary Report are available on the company's website: www.nationalbiometric.org.




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








The QR Code is not your father's barcode

New data matrix codes present exciting new options in mobile marketing and communication

Ryan Kline
Contributing Editor, AVISIAN Publications

Who would have thought that the lowly barcode, the stodgy grandfather of the identification technology world, would reemerge as a marketer's dream? Well, it is happening. A new generation of barcodes is adding an interactive aspect to advertising, product promotion and more.

Imagine a concert promo poster with a printed code that, when photographed by a standard camera phone, displays a menu of options: listen to this band, purchase tickets for their next show, or take me to their website. Select the option you want and presto, your mobile phone does the rest. Pretty powerful stuff from a marketer's perspective … but can all this be done with a barcode?

Two-dimensional data matrix bar codes have been around for quite some time. The basic data matrix code consists of a series of black and white squares arranged in either a square or rectangular pattern. Unlike regular barcodes, which read in a single direction only, QR codes encode data in two dimensions and allow information to be decoded at a much higher speed. The codes are very resilient—even if partially damaged, the data can still be extracted from the bar code.

The colorful Microsoft High Capacity Color Barcodes can be found on consumer products such as this XBOX 360 game.

The best-known 2D matrix code is QR Code, created by the Japanese corporation Denso-Wave in 1994. The "QR" stands for quick response, as the creator intended the code to allow its contents to be decoded at a high speed. With the capacity to hold 2,953 binary bytes, a QR Code can contain an impressive 7,089 numeric characters or 4,296 alphanumeric characters.

When compared to the matrix code that the United Parcel Service (UPS) created to help with logistics identification, the QR Code has a much greater capacity in about the same physical size. The UPS code holds just 138 numeric characters or 93 alphanumeric characters.

How do they work?

QR Code works in the same way as standard one-dimensional bar codes that are used on items in stores. There is a code and a reader to unlock the code. With traditional barcodes, reflected light or infrared light is used to read the code, but with QR Code, any lens can photograph the code and a software application reads the image. The large squares that often appear in the corners of QR codes are position detectors, which tell the reader where the code starts and stops.

"The possibilities of 2D Codes are tremendous, and the imagination is the limit," says UpCode's managing director Sture Udd. "If used wisely, it contributes to a complete cross media application." The simplicity of having a camera phone take a picture of a little square and have it redirect to a website, open a new SMS text message, or import contact

information to an address book makes this type of marketing and communication extremely powerful.

The small codes are big in Japan, but not so elsewhere

The QR Code is widely used in Japan for a range of applications:

- McDonald's customers can point their cell phones at the wrapping on their hamburgers and get nutrition information on their screens.
- Magazine readers point their phones at ads to receive insurance quotes.
- Film promoters send their movie trailers from billboards.

Despite the success in Japan, the use of QR Codes in the United States and much of the rest of the world has been minimal.

"Japan's mobile market is typically two to three years ahead of Europe, and four years ahead of the United States," commented Gavin Jancke, director of engineering for Microsoft Research and inventor of the High Capacity Color Barcode format, a 2D multi-color code. "Japan's culture," he continued, "is more mobile and gadget inclined … think Tamaguci/Digipet."

The use of the QR code in Japan can be attributed largely to the mobile phone providers, primarily NTT DoCoMo, the company controlling 54% of the Japanese mobile market. DoCoMo understood that in order for people to use the technology it had to be given to them, so the company began shipping phones with the QR Code reader on board. Today, more than 60% of DoCoMo users have QR Code reader-equipped phones.

If the service is not installed when phones are purchased, it is a challenge to get the QR Code application onto a handset. It can be done, but it is unlikely that consumers would do it en masse.

Most industry insiders agree that in order for matrix codes to take hold in other countries, the mobile phone manufacturers and providers have to change the way they think. "The ones driving it haven't understood the benefits," according to Mr. Udd.

The mobile Internet drives the most compelling applications

"More than 80% of the mobile phones in Japan have access to the Internet," according to the NTT DoCoMo spokesperson. "The popularity of QR Code was from the high ownership ratio of Internet-accessible phones and QR Code reader-equipped phones."

On the other end of the spectrum, only 4% of Americans use the mobile Internet (according to dotMobi, July 2006), although many, if not most, new handsets sold today are capable.

So in America, if a specific QR Code's purpose was to automatically redirect to a website, only 4% of Americans would be able to take advantage of the offer. Of course, there are applications for the codes that do not require Internet connectivity (e.g. importing contact information, obtaining basic details about an event, initiating an SMS message), but many of the most compelling marketing uses tie back to the web.

Increased bandwidth in the US by mobile phone providers could greatly facilitate the growth of QR Codes, as could a decrease in service fees charged for access.

Camera phone quality matters

Still, even if a provider pre-installed a QR reader application on its phones, there would still be problems with how QR Codes were captured. "The codes contain a lot of data and if one wants to keep it as small as the data matrix, the phone needs a special lens," says Mr. Udd. "Today's phones haven't got that." Camera phones need to be able to zoom in enough so that a passerby could simply point to a QR Code on a poster and zoom, instead of having to walk close enough to get all of the data readable from the code.

Settling on a matrix code standard

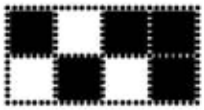
The QR Code, though the first and most widely known of the 2D matrix codes, is not the only game in town. A number of competing formats exist, each vying for a place in the emerging landscape. For the technology to succeed, a single format will need to be standardized (at least in a region by region basis) or application software will need to support multiple formats.

For instance, Finland based UpCode offers a 2D matrix code that looks exactly like a QR Code that could be read with a handset from NTT DoCoMo. But it is very different, encoded with a proprietary language that can only be read by an UpCode reader. But Mr. Udd himself stated that a standard was indeed necessary.

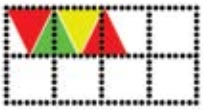
A Dutch company, ShotCode, has developed a matrix by the same name that uses a circular format. According to Dennis Hettema, founder of ShotCode, "you see a ShotCode once and you'll always recognize it in the future. The ShotCode reader was developed with devices in mind that had low processing power and bad lenses. This means that ShotCode is compatible with the largest range of mobile phones in the market."

There are two rings in the ShotCode that are made up of black or white blocks that either represent a one or a zero. Incorporated into the code is a checkbit so that the reader knows where the number sequence starts and ends.

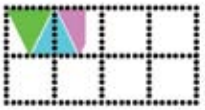
Coca-Cola printed ShotCodes on product packaging for a Sprite marketing campaign in Mexico (www.promosprite.com). Once the code was scanned, a trivia question automatically appeared. If the question was answered correctly, contestants instantly knew if they had won one of the millions of prizes. This was promoted as the first ever on-pack mobile barcode scanning campaign launched outside of Asia.



Black & White matrix code storing 1 byte (8 bits)
Uses 8 symbols



4 color barcode storing 1 byte (8 bits)
Uses 4 Symbols



8 color barcode storing 1 byte (8 bits)
Uses 2.66 Symbols

In the United States, Microsoft has developed a matrix code that includes color as an additional data-encoding variable. The company's High Capacity Color Barcode (HCCB) arose out of a biometric ID research project. "We wanted to store lots of biometric information in a small space," stated Microsoft's Mr. Jancke. "Existing 2D barcode formats were too big."

The difference between Microsoft's HCCB and other 2D codes is the color. "Using colors means it can store more information than black and white codes," said Mr. Jancke. "Black and white codes store one bit per symbol, 4 colors store 2 bits per symbol, and 8 colors store 3 bits per symbol."

Will there be a QR Code in your future?

Although QR codes have exciting marketing and information sharing potential, the handset manufacturers and service providers outside of Japan have yet to invest in the infrastructure (e.g. capable handsets and high capacity wireless broadband) to enable the technology. Other factors, including numerous competing wireless providers and the competing technologies such as near field communications, further complicate the issue. If these hurdles can be jumped, as they have been in Japan, perhaps we will all one day point our camera phones at the interesting little codes to access a host of special offers and services. ID

Follow the steps of this passerby as he watches a video trailer after being prompted by a ShotCode.

By visiting http://www.shotcode.com/download and downloading a reader for your phone, this shotcode would redirect you to http://www.secureidnews.com.

Mobot uses images rather than QR Codes or NFC tags to connect mobile user to marketers

If a matrix barcode is not your thing, a Mobot may be more to your liking. From the end user perspective, QR Codes and Mobots work similarly – the user snaps a photo of the Mobot using a camera phone and the captured image is sent via the web to retrieve some special offer, product info, or initiate some type of transaction. The Mobot isn't a barcode, but a realistic image with visual meaning for the user.

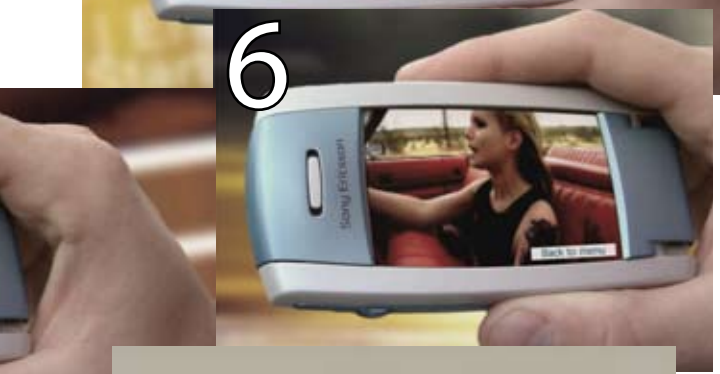
Mobot uses visual search and recognition technology to take the captured image from the mobile device and 'find' the associated URL to initiate the desired action. It was launched in 2004 to help marketers, content providers and carriers interact with the world's 1.5 billion mobile phone users.

"There is no relation between Mobot and QR Code," says Russell Gocht, CEO of Mobot, except the fact that they both use a camera phone to connect consumers to marketers. "Code-based solutions are decoded on the phone," Mr.Gocht added. "Mobot is server-based, so all image processing is done 'in the cloud.' And with Mobot no changes are required to the logo, advertisement, package, etc."

Mobot works simply by capturing an image and redirecting a browser to gain more information. "The call to action (telling consumers to take a picture) comes through any media which is part of the campaign, from (magazine) copy, to radio spots, to web sites." Mr.Gocht also added, "with camera phone penetration passing 75%, Mobot is poised to capture critical mass in the United States."

"Think of using Mobot just as you would your photo blog," Mr. Gocht explained. "Take a picture with your phone and send it to a machine. To reach this machine you either use a well-known email address such as pix@vzw.com (verizon's proprietary photo service) or a phone number (short code) such as 66268 (MOBOT). All images arrive at Mobot servers via MMS messaging (technically, MM7 protocol) – each of these messages includes the user's mobile number. Once decoded and uniquely identified, the appropriate response is sent back to the user as a message. In some cases, the user will 'click-through' a link in the message to get to a WAP site (mobile web site)."

If you don't use your mobile phone for much except, well, making phone calls, this may sound foreign to you. But just ask anyone under the age of 25 … they can explain it to you.



To test out Mobot, snap a picture of the AVISIAN logo below with your camera phone and send it to demo@mobot.com. You will then receive a special text message reply from AVISIAN publishing.

AVISIAN

Understanding the FIPS 201 product approval process

A guide for both product developers and compliant card issuers

Chris Corum
Executive Editor, AVISIAN Publications

If you are confused about what products you can and cannot buy for a FIPS 201 implementation, you are not alone. Both buyers and sellers of identity products are often found scratching their heads due to seemingly missing categories of products and sometimes confusing category names.

But in reality, it is an organized and defined process that has moved almost 300 products and services through a complex certification in just more than one year … not an easy task.

Talk to buyers and you will hear questions like this:

- I need certain piece of hardware or software but I can't find a category for it in the Approved Products List (APL). Does that mean I can't buy it or can I pick anything I want?
- I already have a bunch of card printers but the model is not listed on the APL. Are my existing products 'grandfathered' in or am I supposed to throw them away?
- If a product is listed on the APL can I buy it direct from the company, or do I have to go through the GSA schedule or some other source?

Talk to vendors and you will hear questions like:

- There isn't a category for my product. Can I request that one be added?
- My product fits in a number of categories but there is not one for that covers its total functionality. Should I go for approval in all the sub-categories or wait for a new category to be created?
- What is the difference between the GSA APL and SIN 132-62?

How did we get to this point?

A quick review … President Bush issued Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors, in August 2004. To meet the requirement for a secure interoperable credential, the National Institute for Standards and Technology (NIST) created the Federal Information Processing Standard 201 (FIPS 201).

In OMB Memorandum M-05-24, the Office of Management and Budget (OMB) required that agencies purchase only federally-approved products and services for implementation of HSPD-12. Thus, a means to approve products and services was necessary.

Because the General Services Administration (GSA) is responsible for acquisition of products by federal agencies, the GSA developed the FIPS 201 Evaluation Program. Understandably, the specific requirements prescribed in FIPS 201 and its special publications differ among the array of product and services, so categories were required. This effort led to the GSA Approved Product List (APL) for FIPS 201 – a comprehensive list of products and services that have been determined to be compliant with FIPS 201.

In addition to the FIPS 201 Evaluation Program, three other compliance processes exist for PIV products.

1. NIST established a compliance testing effort called the NIST Personal Identity Verification Program (NPIVP) to, "validate the compliance/conformance of two PIV components – PIV middleware and PIV card application with the specifications in NIST SP 800-73-1." NIST relies upon NVLAP-accredited test labs to certify middleware and applications submitted for consideration.

2. The Minutiae Interoperability Exchange Test (MINEX) is a NIST effort to establish compliance for template generators and template matchers.

3. Certification of Single Fingerprint Devices against the Federal Bureau of Investigation's (FBI) Integrated Automated Fingerprint Identification System (IAFIS) Image Quality Specifications (IQS).

Understanding the APL process

What must a company do to get a product approved for listing on the GSA APL? There is no better source to answer this question than Nabil Ghadiali, Technical Director, Information Assurance, Electrosoft and the Technical Lead for the GSA FIPS 201 Evaluation Program. Electrosoft, a 15-person information security company based in Virginia, is contracted by the GSA to provide technical support for the FIPS 201 Evaluation Program and serve as the gatekeepers – so to speak – for the APL.

The process begins online with the Evaluation Program Web Tool. "When a vendor wants to submit a product," says Mr. Ghadiali, "they fill in a login request form, send it to us (Electrosoft), then we send them a user ID and password."

With each category there is a separate set of required documentation that must be submitted, and for some categories, the actual product may need to be submitted for testing as well (e.g. PIV Cards, Card Readers).

Via the web tool, lab staff monitor the new application submission and can track the documents to see what has been submitted and what is missing. "There is a timeline," explains Mr. Ghadiali. "Within 10 days after creating the application, you must start to submit the documents and (once started) 5 days to complete the submission."

If the dates are not met, the application is rejected. This timeline was created to stop vendors from creating an application until their product or service was ready for evaluation.

"To this point we have only looked at documentation to see that it is physically there," adds Mr. Ghadiali. "Once it is complete, it moves to 'evaluation in progress' status and the lab begins its work."

There are different steps during the process (e.g. vendor documentation review begin, vendor documentation review complete, evaluation complete, evaluation report complete, awaiting government approval authorization) and the vendor can monitor these status changes via the web tool having visibility in the progress of their application through the evaluation.

When the lab finishes the evaluation, a final report is written and sent to GSA FIPS 201 EP program manager for review and final approval authorization. If the product is approved, it is added to the APL.

If the product is found to be non-conformant, the vendor is notified and the product is not listed. "The vendor can then request a non-conformance review to demonstrate how their product meets the requirements," says Mr. Ghadiali, "basically an appeal and review process."

If a product that was found non-conformant, is modified and released as a new version, it can be resubmitted, but the process must begin anew. It does tend to go more quickly the next time, suggests Mr. Ghadiali, because of the understanding gained in the initial review.

How many products are under review and what are the costs?

"On a weekly basis we may have between 5 and 10 applications (added to the web tool)," suggested Mr. Ghadiali, though he stressed this is only an estimate.

"We saw 70 or 80 in the weeks prior to April (2007)," he added, alluding to the cutoff date after which the fees for evaluations were to be borne on a cost-reimbursable basis by the vendor.

Just how much an evaluation will cost depends on the category. Because the scope of the tests required to confirm or deny conformance differs by product, so too does the price. "Some evaluations – like graphical personalization service – require site visits," notes Mr. Ghadiali. "A cryptographic module (on the other hand) may be fairly easy as the vendor already has their FIPS 140-2 validation from NIST."

Now that multiple labs will be certified to perform evaluations, the fees will be market driven. Mr. Ghadiali suggested that the simplest evaluation might cost anywhere from a few hundred dollars to a maximum fee of about a few thousand dollars. He stressed that vendors should contact the labs to determine the fee each would charge prior to making a decision on which lab to go with,

The new lab structure

Until April 2007, only one lab was approved to test products for the APL. The contract for this testing service had been awarded to Electrosoft, and the company subcontracted the work to Atlan Labs. Since then the Evaluation Program has developed requirements for lab qualifications in order to enable other labs to participate.

Electrosoft has moved into its new role staffing the Evaluation Program Management Office. Says Mr. Ghadiali, "We, along with April Giles the GSA Evaluation Program Chief Architect, make sure the Evaluation Program stays current with the requirements as NIST makes revisions to their documentation and all the labs have the documents and tools they need … we oversee the labs."

Based on the GSA lab qualifications requirements, Atlan Labs continues its testing functions as an approved lab without the involvement of Electrosoft.

To make the list, a lab must be a part of the NIST Voluntary Laboratory Accreditation Program (NVLAP). The program, according to NIST, "accredits public and private labs based on evaluation of their technical qualifications and competence to carry out specific calibrations or tests."

Because the NVLAP certifies all types of test labs, only those approved for Cryptographic Module Testing (CMT) are eligible for the FIPS 201 Evaluation Program as the skills required for testing have been deemed most closely related. The CMT labs test crypto products for compliance with FIPS 140 standards. Currently, there are 14 labs with CMT status.

Validation of the PIV card application and PIV middleware via the NPIVP comes next. Ten of the 14 CMT labs have been approved as NPIVP labs to date. Finally, these labs must have the GSA test methods added to their qualifications. With all these criteria met, the lab can apply to GSA for inclusion as an evaluation lab within the FIPS 201 Evaluation Program.

To date, only InfoGard has joined Atlan as an approved lab but more are expected soon. "As I understand there are a few labs that have GSA test methods under their belt so they could apply to GSA," suggests Mr. Ghadiali.

Cutting through the confusion

As suggested in the opening of this piece, a great deal of confusion continues to surround the APL. Much of it centers around products that are necessary for a FIPS 201 ID implementation but are not seemingly covered by a category on the APL. Vendors question how they can get their products approved, and issuers question how they can obtain these unlisted products.

Many of these concerns are alleviated by a single explanation. As Mr. Ghadiali explains, the categories on the APL were not 'selected,' rather they simply fell out of the actual FIPS 201 Standard. "We read the Standard and made a category when a specific requirement for a product or service was mandated … No requirements, no category."

"We aren't in the business of making new requirements," he explains, "only testing those established by the Standard." Thus it is unlikely that new categories will be added to the APL, at least until a revision is made to FIPS 201.

A caveat to that is that when it was deemed necessary from a security point of view, the FIPS 201 Evaluation Program did add specific security related requirements (e.g. addition of security controls around the storage of printed PIV Cards). This caveat applies primarily in the case of Service categories.

Here is an example that may help explain it in concrete terms. Obviously, to issue a FIPS 201 compliant credential a printer ribbon must be used in the ID card printer. Yet there is no category on the APL for printer ribbons. Does this mean that agencies cannot buy a printer ribbon? Obviously not. It simply means that the FIPS 201 documentation did not deem it necessary to create specific requirements for ribbons. So an agency is free to buy any printer ribbon they deem appropriate for their needs.

"If there is a product that is applies within the context of PIV, but there are no requirements," concludes Mr. Ghadiali, "they (the vendor) need not submit." And agencies are free to buy any product they require. The only stipulation is that if a category exists for the product, they must choose from the APL.

Buying APL products

To facilitate purchase of PIV-related products, the GSA established a dedicated category under Schedule 70 (the information technology purchasing schedule) called Special Item Number 132-62 (SIN 132-62). According to the GSA, the category is, "for products and services for agencies to implement the requirements of HSPD-12, FIPS-201 and associated National Institute of Standards and Technology special publications."

The components specified under SIN 132-62 are:

- PIV enrollment and registration services
- PIV systems infrastructure
- PIV card management and production services
- PIV card finalization services
- Physical-access control products and services
- Logical-access control products and services
- PIV system integration services
- Approved FIPS-201-compliant products and services.

Only products on the APL can be offered through SIN 132-62, however non-approved integrated solutions may be offered by system integrators qualified by GSA and listed on SIN 13-62 as well. The requirement, however, is that these solution providers must commit to delivering only APL products.

If the product is not listed on SIN 132-62 but is listed on the APL, it can be procured through another Schedule that it might be on or via the open market.

Clearing up the confusion

At the outset of this article, a series of commonly heard questions from both vendors and buyers of FIPS 201 products and services was presented. To conclude, these questions are directly answered based on the information presented in the article.

I need certain piece of hardware or software but I can't find a category for it in the Approved Products List (APL). Does that mean I can't buy it or can I pick anything I want?

Yes, if there is no category for a specific product an agency is free to select the product that best meets the identified need.

I already have a bunch of card printers but the model is not listed on the APL. Are my existing products 'grandfathered' in, or am I supposed to throw them away?

If an existing product is not listed on the APL, it hasn't been evaluated or approved by the FIPS 201 Evaluation Program. Agencies that choose to use such products may therefore be in non-compliance with the standard.

If a product is listed on the APL can I buy it direct from the company, or do I have to go through the GSA schedule or some other source?

Products can be purchased from the GSA schedule or can be procured on the open market. Schedule 70, SIN 132-62 covers PIV-related items however there is not a mandate that agencies acquire all components from this source.

There isn't a category for my product. Can I request that one be added?

No. Because the categories were pulled directly from the FIPS 201 specification, only those products that had specific, written requirements need to be approved. If there is not a category for your product, agencies are free to buy it if desired.

My product fits in a number of categories but there is not one for that covers its total functionality. Should I go for approval in all the sub-categories or wait for a new category to be created?

New categories will not be added unless future revisions to the FIPS 201 specification merit additions. If you would like to have your product on the list, it can be submitted for approval if it meets the category description as documented within that particular Approval Procedure. Products that fall under multiple categories will need to be submitted for evaluation under each category separately.

For example, a multi-technology reader that can read the Card Holder Unique ID Number (CHUID) from both contact and contactless cards could be approved in both the contact reader category and the contactless reader category.

What is the difference between the GSA APL and SIN 132-62?

The APL is the listing of PIV-related products that have been approved by GSA as compliant with FIPS 201 requirements. SIN 132-62 is the purchasing schedule that enables agencies to procure APL products. It is, however, not the only means to buy these products as they can be purchased through the open market.

Your leading "One-Stop-Shop" vendor for Smart Card equipment

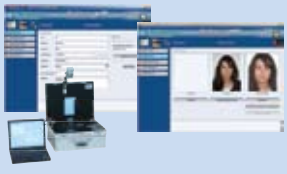
*Success needs experience - **Driver's License** production with Mühlbauer!*

Mühlbauer
High Tech International

Data Enrollment

incl. automatic picture enhancement

- Live and/or form enrollment hard- and software
- Automatic processing of pictures, signatures, OCR/ICR etc.
- Quality management module
- Capturing of alphanumerical, optical and biometrical data
- Data & security document as well as PKI management



Card Personalization

- Portfolio for central and decentralized manufacturing
- Highly flexible and modular systems
- Realization of any customer-specific demand possible
- Integration of various security features
- Suitable software solutions for personalization and production management

From low ... to high volume

complete solution incl.
CARD MAILING

...for high quality Driver's License cards

Mühlbauer provides complete turnkey solutions for the manufacture of high-security identification credentials, including driver's licenses that meet the requirements of the REAL ID Act. The company is active in over 50 identification projects worldwide, including driver's licenses, ID Cards and ePassports. Equipment from data enrollment over the production, and personalization to the mailing of any document is a particular area of expertise. Mühlbauer delivers hardware and software solutions for over-the-counter and central-issue environments.

TECURITY® - Complete Solutions setting the new Standards

Muhlbauer Inc.
725 Middle Ground Boulevard
Newport News, VA 23606-2512
USA
Phone: +1 757 873 0424
Fax: +1 757 873 0485
Email: info@muhlbauer.com
Internet: www.muhlbauer.com

FIPS 201 products and services from the GSA Approved Products List

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
Stellar ID Card Printers	Stellar ID CX-320/PVStar Printing Solution

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
Secure Network Sys.	SNS IdShield Credential Holder Dual
Identity Stronghold	Secure Book Cardholder

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
XTEC Incorporated	AUTHENTX IDMS/CMS Module

Facial Image Capturing (Middleware)

XTEC Incorporated	AUTHENTX Image Capture Middleware
Aware, Inc.	PreFace/PIVPack SDKs
Liska Biometry, Inc.	DCS.8500.FIPS

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
Green Bit Americas	VisaScan3
Green Bit Americas	PoliScan2

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

FIPS 201 products and services from the GSA Approved Products List

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
Green Bit Americas	Scan-IDe26
Green Bit Americas	DactyScan26
Green Bit Americas	DactyScan26i
Green Bit Americas	ICT401

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
BIO-key International	Vector Segment Technology, SW-2000005

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
BIO-key International	Vector Segment Technology, VST 6 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
SCM Microsystems	SCR3310 v2
Secure Network Sys.	SNS CRITSEC® CRP40
Secure Network Sys.	SNS CRITSEC® CRK40
Secure Network Sys.	SNS CRITSEC® CR40
Secure Network Sys.	SNS CRITSEC® CR30
Secure Network Sys.	SNS CRITSEC® CR10
Key Ovation	Goldtouch ErgoSecure SC 2.0
Hewlett Packard Co.	HP USB Smart Card Keyboard
OMNIKEY Americas	CardMan 5125 (USB Contact reader+HID prox)
AMAG Technology	XF2100-PIV
AMAG Technology	XF2110-PIV

GSA-chosen EDS begins FIPS 201 infrastructure work while competitor BearingPoint scores major agency win

Marisa Torrieri
Contributing Editor, AVISIAN Publications

Less than four months since EDS stole some of competitor BearingPoint's thunder by winning the General Services Agency's bid for a Shared Service Provider (SSP) to execute HSPD-12's ID card program, BearingPoint is making waves with a major agency contract.

BearingPoint announced a new contract on August 1 with the US Department of Health and Human Services (HHS) to perform an Identity and Access Management pilot and implement 112,000 Personal Identity Verification (PIV) cards that are complaint with the FIPS 201 technological specification. The cards are a requirement for all federal employees and contractors under the Homeland Security Presidential Directive 12 (HSPD-12).

Gordon Hannah, managing director for BearingPoint's security and identity management program, says HHS chose BearingPoint after an evaluation of three companies: BearingPoint, EDS and Lockheed Martin.

"In a side-by-side competition for procurement, some of the key things that differentiate us is we're both a management and technology consulting firm and a systems integrator," says Mr. Hannah. "We look at this as a business issue, which resonated with HHS."

By December, the company expects to have tested and issued about 10,000 cards in various divisions of HHS, Hannah says.

Because HHS is so large and encompasses smaller divisions including the Centers for Medicare and Medicaid Services (CMS) and the National Institutes of Health (NIH), a tailored solution is a better approach, Mr. Hannah says. For a large agency, the benefits of not opting for the "one size fits all" SSP program means greater flexibility.

For example, an agency may want the option to speed up the issuance of a new employee's card when necessary, a BearingPoint spokesman says.

Additional benefits HHS will experience include more automated workflow processes and a shorter amount of time in setting up accounts, activating cards and deactivating cards, the spokesman continued.

EDS consortium well underway with new SSP offering

BearingPoint's announcement comes nearly four months after the government selected EDS as the official Shared Services Provider for the FIPS 201 Card Rollout. The five-year contract, worth $66 million, was touted by GSA as a taxpayer bargain.

Upon issuing the award, GSA Administrator Lurita Doan said in a statement: "This award further enhances GSA's ability to provide critical national security systems while reducing the overall costs to the government and taxpayers."

BearingPoint was originally selected as the GSA's SSP one year ago, in a contract worth $104.6 million. Soon afterwards, BearingPoint helped nearly 40 agencies produce their first cards for the October 27, 2007 deadline.

The Shared Services Provider Program began in August 2006 to give agencies a one-stop shop for implementing standards-compliant cards and card-management systems.

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

At press time, an EDS spokesman said the company had already long since begun execution of plans to build the infrastructure and service centers that will support the ID cards. This is the first step in preparing the 42 government agencies which have signed up for the SSP program for the FIPS 201 identity card rollout.

"I know that's going on right now," says EDS senior spokesman Brad Bass, who works with the company's government contracts division. EDS's partners in this venture include Northrop Grumman Corp., ActivIdentity Corp., Data Systems Analysts, Identification Technology Group, L-1 Identity Solutions, Oberthur Card Systems and TIBCO Software Inc.

In selecting EDS, the government basically chose the most cost-effective proposal. But undergoing the task of building the infrastructure and issuing cards requires a huge multi-million dollar financial investment, says Jeremy Grant, the emerging technologies analyst at the Washington, DC, research arm of Stanford Group Company.

"From what we hear, they're doing a very decent job," says Mr. Grant. "And from my perspective, the EDS team was a sensible choice. GSA had to choose a vendor that was credible in this space. There was a very shaky coalition of federal agencies that signed up with GSA to deliver managed services. So GSA had to select someone those agencies would feel comfortable with, and EDS is certainly a company that has credibility in this space."

The high level of business risk prompted BearingPoint to drop out of bidding at the last minute, Mr. Hannah confirmed.

Prepping federal agencies for the October 2008 card-issuance deadline

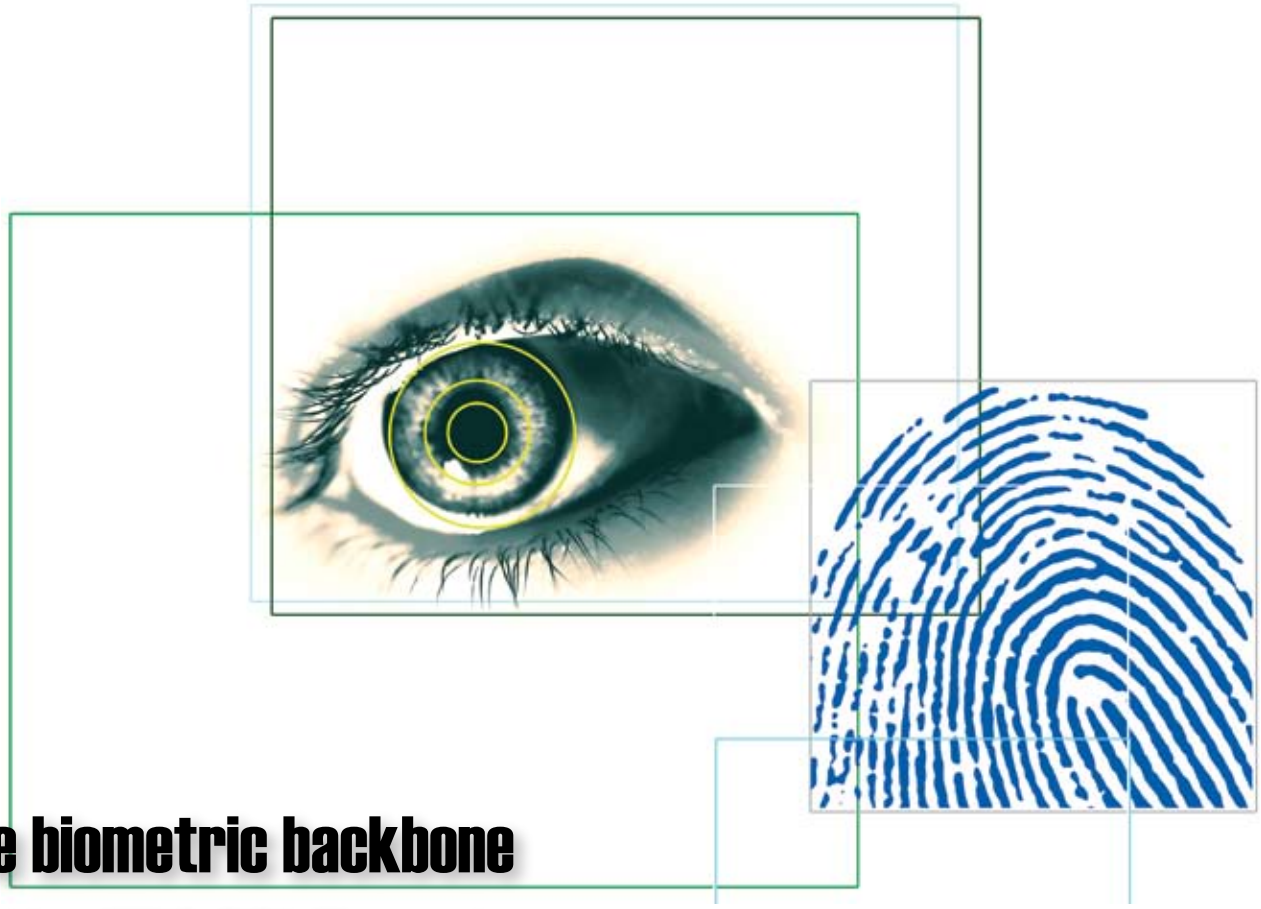
By October 2008, all federal government agencies are expected to have issued their first round of FIPS 201 cards. One of the biggest challenges facing technology providers is convincing agencies that this is important.

"Combined, all federal agencies have only issued roughly 5,000 PIV cards," Mr. Grant says. "If you talk to vendors in this space, they'll tell you the same sob story – it's moving very slowly."

"It's an unfunded mandate," continues Mr. Grant. "The OMB says you have to do this but agencies are wondering 'could this go away after the Bush administration goes away?' This has been a tough sell among some of the agencies."

EDS and its partners will be evaluated on a continuing basis, to ensure they're following through with their end of the contract.

The government has the right to pull the contract and re-bid for a new SSP should they not follow through, says Mr. Grant. "I think it'll be a question of: are they issuing cards or not? Do they work? I think they need to step up and show that it does."



The biometric backbone of the FIPS 201 ID card program

David Benini
Aware, Inc.

Following the publication of the FIPS 201 standard in 2005, a series of specifications evolved defining the functionality and interaction of the components that together make up a comprehensive biometrics-enabled credentialing system. The requirements set forth in FIPS 201 were divided among twenty product categories and three services that form the GSA's Approved Product List (APL). There are six categories that cover specific biometric technologies. Because PIV cards utilize fingerprint and facial biometrics, the categories are split between the two technologies.

Fingerprint biometric product categories:

- Template Generator
- Template Matcher
- Fingerprint Capture Station
- Single Fingerprint Capture Device

Facial image biometric product categories:

- Facial Image Capturing (Middleware)
- Facial Image Capturing Camera

Fingerprint biometric product categories

The first set of biometric categories covers hardware and software required to capture and verify fingerprint biometrics on PIV cards.

The "Fingerprint Capture Station" is the equipment used to capture an individual's full set of fingerprints at the point of enrollment. The "Template Generator" is the software that generates the INCITS 378 compliant biometric template from the captured prints.

An approved "Fingerprint Capture Station" product must be an FBI-certified fingerprint live scan device or card scan solution, but must also include software to generate both NIST NFIQ image quality scores and fingerprint images within ANSI/INCITS 381 compliant data files.

Moving from enrollment to utilization, the "Single Fingerprint Capture Device" is used in the field to capture the live fingerprint images for matching against the enrolled template. The "Template Matcher" software performs this matching process.

Products in the fingerprint minutiae based "Template Generator" and "Template Matcher" categories must be submitted to NIST's MINEX program for certification. NIST tests the software for interoperability between templates and matchers from different vendors. The software submitted for testing must be able to exchange template files compliant to the ANSI/INCITS 378 data interchange format for fingerprint minutiae templates.

Facial image biometric product categories

Hardware and software for facial capture are covered by two different categories: the "Facial Image Capturing Camera" is simply a digital camera with sufficient resolution and the ability to prevent over-compression. The software to format the image is the "Facial Image Capturing (Middleware)."

INTRODUCING ...

FIPS 201.com

THE PREMIERE RESOURCE FOR COMPLIANT CREDENTIALING

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

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

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

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

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

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

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

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

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

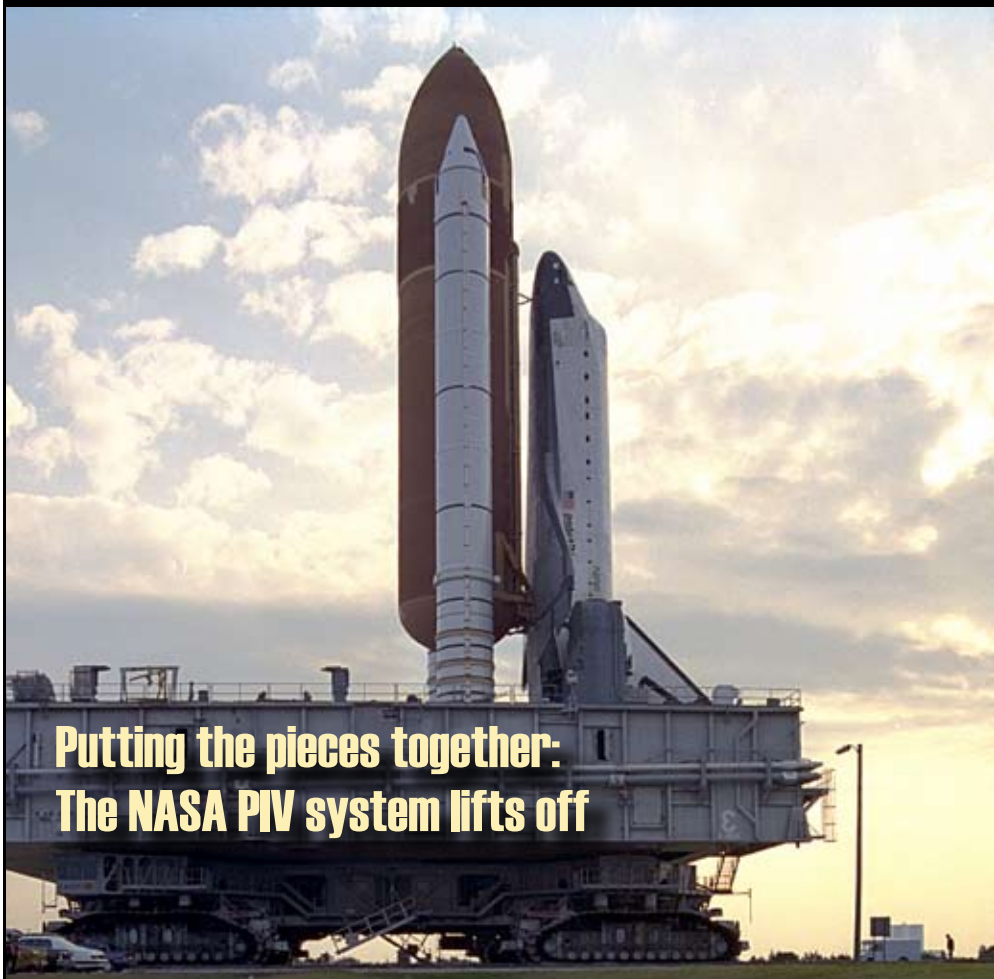
AN AVISIAN ID TECHNOLOGY RESOURCE

The "Facial Image Capture (Middleware)" product category serves as a catch-all for facial image and data requirements. Software products in this category should create data structures compliant with ANSI/INCITS 385 and also validate that the captured facial images are compliant (e.g. dimensions, size of the head in the frame, resolution and compression ratio). It includes a requirement that if the facial image is compressed using the JPEG 2000 "region of interest" (ROI) technique, the product must support prevention of the compression of the inner facial region beyond a ratio of 24:1. JPEG 2000 ROI is recommended when optionally storing facial images on the smart card because of its significantly improved compression performance over JPEG.

Generally the term "middleware" refers to software that enables connectivity between large distributed applications, web services and service-oriented architectures (SOA). But in the smart card vernacular, the "middle" is relative and refers to something quite different. The "PIV Middleware" product category actually refers to software serving as an interface for communication between the PIV application on a PC and the smart card itself. FIPS 201 specifies this interface, and products in the PIV Middleware category must be independently certified to be compliant. This shouldn't be confused with biometric middleware products on the market that are typically servers performing centralized tasks such as biometric data routing and processing.

Biometrics required for PIV but not categorized on APL

Some facets of PIV system biometrics are not addressed by FIPS 201 standards, except to say that they are required. While FIPS 201 identifies strict requirements for background checks to the FBI and OPM that require biometric verification, these elements are not detailed in FIPS 201 and thus are not categorized on the APL. This is because there are well-established procedures for fingerprint image compression, quality and data formatting that are addressed by legacy standards and certification programs (e.g. the FBI's "Appendix F" image quality certification for fingerprint scanners, and the ANSI/NIST ITL-1 2007 standard for background check file formatting).



Putting the pieces together: The NASA PIV system lifts off

NASA was well-prepared for HSPD-12, deploying an operational pilot system with approved products more than six months before the pending October 2007 deadline. Like many agencies, NASA already had an identity management system, a card management system, and a fingerprint background check submission system in place. The agency was issuing employee ID cards well before HSPD-12 was announced.

While PIV imposes new standards for card issuance procedures, physical card properties, data formats and interfaces, it is the introduction of biometrics for identity verification that is perhaps the most disruptive to an agency's legacy systems … and NASA's is no exception. NASA's identity management and card issuance systems had operated completely independently from its fingerprint background check system, so the introduction of biometrics to the identity system enrollment process provided a strong incentive to combine these functions in a single enrollment station. The FIPS 201 requirement to use the same biometric for background check and for generation of minutiae templates to be stored on the ID cards solidified this need.

NASA designed an architecture that would utilize the same registration workstation for both PIV enrollment and background checking. A new registration workstation collects biometric images and biographic data for both functions during a single enrollment session. This workstation includes products from several APL categories to perform multiple tasks, including a pre-enrollment search of the IDMS, ten-fingerprint auto-capture, facial image auto-capture, and biographic data collection and formatting for the PIV card and the fingerprint background check.

A new central server was installed, used to a) aggregate enrollment traffic from the geographically distributed enrollment stations, b) prepare data for card personalization and enrollment, and c) forward background check files to the legacy background check server. This central server facilitated this modular "overlay" upgrade achieving PIV compliance, mitigating risks and costs of a broader modification of existing systems.

How Can We Claim Software House® is the Most Secure?

Easy.

- The first full access control panel to be listed on the FIPS 140-2 pre-validation list
- FIPS 197 validated software
- Our iSTAR eX controller features 256-bit AES encryption, double most others in the industry
- Industry-first Multi-Technology readers, read all PIV II cards
- Solutions that feature superior, digital certificates; preventing “man-in-the-middle” attacks

Download our Government-Ready toolkit from www.swhouse.com

SOFTWARE HOUSE®

tyco

Make your plans now to attend this year's CARTES and IDentification event

Identification, NFC, contactless and Japan will all be major focal points during the 22nd edition of CARTES, coming your way November 15-17 in Paris at the Paris-Nord Villepinte Exhibition Centre near Roissy Charles de Gaulle International Airport.

One of the major changes this year, according to CARTES Communication Director Hélène Tsounguy, is the coming of age of CARTES' IDentification, which has been somewhat of a CARTES stepchild since its introduction in 2005. Then, it was an area dedicated to secure technologies but this year, it "takes its independence as a true exhibition near CARTES," she said.

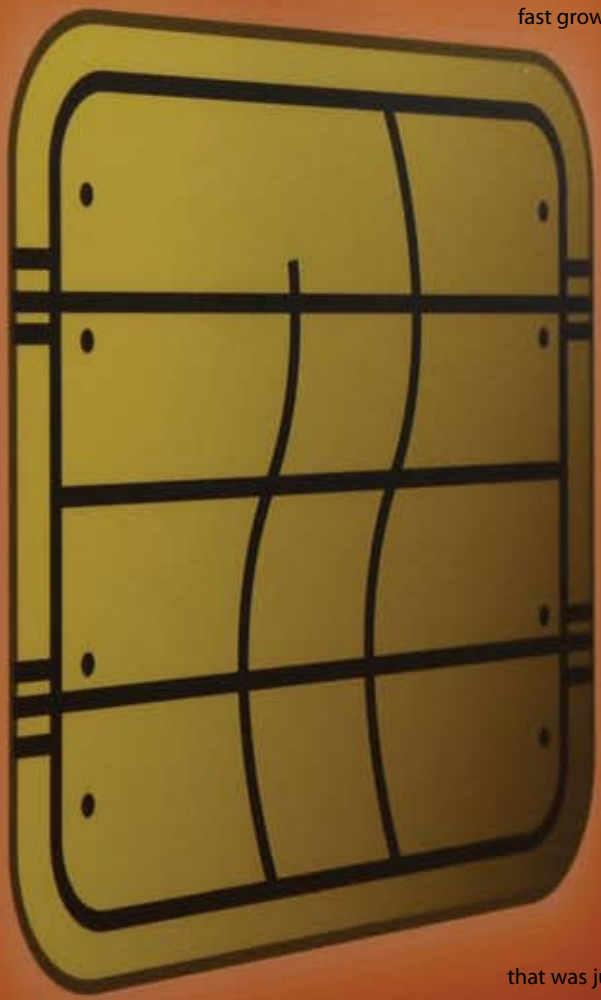
The international show, which got its start in 1985 as the International Plastic Card Forum, is expected to draw more than 20,000 visitors this year, an increase over last year's 19,576 visitors. The word, *cartes,* she said, "simply means both 'smart cards' and 'chips' in French."

When CARTES was first created, it was just "some little stands (booths)," at a local hotel, explained Ms. Tsounguy. But as the smart card market has grown, so has CARTES. "As the event became bigger and bigger, it moved from a hotel to a convention center in Paris, then to another one just near Paris," and finally to its current location, she added. This year there will be some 480 exhibit booths.

With CARTES' focus this year on security and contactless technologies, it makes sense that IDentification should have its own … well, identity. "Benefiting from a separate promotion, IDentification will have its own exhibition and will bring together all others in physical and logical access control, network security, strong authentication, cryptography, biometrics, secure documents, and so on," said Ms. Tsounguy.

Why attend?

"As a professional in this market, you can't miss CARTES & IDentification because it is the biggest show in the world where you can meet all the players of the industry," she adds. "You can also listen to the CEOs of the leading companies during the opening 'World Card Summit,' and meet key speakers from all over the world. It is a unique opportunity to discover innovations," she said. "CARTES & IDentification is now the world leading event in digital security, smart cards and identification. The success of our event is that we always try to adapt and to follow a fast growing market."



NFC featured at the new TechZone

One of the latest innovations is NFC (near field communication). With the focus also on the newest in contactless technology, "we are organizing a new area (at CARTES) called 'Mobile Transactions TechZone' in partnership with the NFC Forum," she said. "NFC technology will be in the spotlight with demonstrations of applications in everyday life, educational presentations of new products using contactless and prototypes."

Country focus: Japan

Each year, CARTES recognizes a country it considers leading the way in innovation or smart card strategies. Last year, Canada was tapped for its countrywide EMV migration that was just gearing up. This year, CARTES returns to Asia, spotlighting Japan. "This country is a true technology lab and a forerunner concerning biometrics, multi-applications, payment by mobile phone and contactless technologies," said Ms. Tsounguy. "Japan is opening the way to tomorrow's applications and new consumer behaviors."

Some 113 million smart cards were sold in Japan in 2005 equaling 40 billion yen or about 265 million euros. Japan, too, is undergoing an EMV migration and is expected to have 340 million smart cards in use by 2010.

Sesames Awards

There's another reason CARTES is so popular in the industry: Its annual Sesames Awards. Founded in 1996, the contest rewards the best innovations and applications in the marketplace and gives the recognized companies bragging rights. This year's applicants set a new record, 211 companies, which will vie for awards in 10 categories: hardware, software, identification, IT security, transportation, banking/finance/retail, health care, mobile, e-transaction and loyalty.

Planning your schedule

In all, there will be 19 conferences and 200 speakers. While many of the speakers and subject matter haven't yet been finalized (as of mid-July) here, then, is a capsule overview of the areas that will be covered at the 2007 CARTES and IDentification.

Tuesday November 13, 2007

World Card Summit, 10:00 am – 4:30 pm
This event, which marks CARTES' official opening, will feature leaders in the smart card and identification industry presenting their most recent technological advances. The morning will be dedicated to the activity and role of the smart card and the afternoon to the identification sector.

Bank Identification, 9:30 am – 5:30 pm
A number of technologies and products are being implemented to make the banking environment safer. What's the current status and what does the future hold in this area?

Biometrics in Everyday Life, 9:30 am – 5:30 pm
Often combined with security, biometrics actually extends to many sectors. In the past it was mainly used for access control, but now biometrics can be found in the payment industry as well.

Card Basics, 9:30 am – 5:30 pm
As the title suggests, it's an overview of smart cards.

The SIM's Future, 9:30 am – 5:30 pm
The versatility of the SIM (Subscriber Identity Module) chip is one of the main drivers in the cell phone market today. This section will look at the SIM's future in terms of capacity, security and innovation.

RFID: The Solutions, 9:30 am – 5:30 pm
Regarded as an effective means to manage the supply chain while tracking a product's movement, this section will cover this mature technology, including testimonials while looking at the various achievements this technology has accomplished.

Wednesday November 14, 2007

Cards & Payments 2007, 9:30 am – 5:30 pm
Whether by contactless or by mobile phone, the payment environment is in the middle of a significant evolution. What's ahead? How will the banking world take to these new payment methods?

Multi-applications, 9:30 am – 5:30 pm
Combining several applications on one card allows the cardholder to manage his preferred applications in his everyday life. This will investigate some of the many projects currently underway.

Digital Identity, 9:30 am – 12:30 pm
Whether at the state level with an electronic ID card or at the corporate level with in-house identity management, or even individually with e-commerce, digital identities are now an integral part of our lives. Yet issues regarding security and proper ID management remain.

Card Security, 2:00 pm – 5:30 pm
How secure is the card? How can it be improved? Does the appearance of new types of fraud jeopardize card security? And, importantly, how can cards be hardened against these new types of fraud?

Personalization: Services with Added Value, 9:30 am – 5:30 pm
A true technological tool, the card is an efficient marketing instrument that can be used to target a specific population. Is this a phenomenon with limited use, or a real market with great potential?

Theft Identity, 9:30 am – 5:30 pm
Logins and passwords are the most common tools to authenticate and validate a person's identity. Despite these precautions many are stolen. What measures should be taken to limit this fraud? Do we all need the same level of security? And what about protecting the data embedded in mobile phones?

Java Card, 9:30 am – 5:30 pm
The Java Card technology is in its tenth year of development. Primarily used as an interface, the Java Card technology has been able to combine simplicity and ease of use with effective security. What's next with the new versions?

Mobility, 2:00 pm – 5:30 pm
This market has had to adapt to the new mobility requirements for people constantly on the go who are using different communications tools … Blackberry anyone? Or iPhone? This has led to the merger of several technologies. But how are they working together, particularly in the payment or transport sectors?

Thursday November 15, 2007

Cards & Payments 2007, 9:30 am – 5:00 pm
A wide-ranging economic environment is being built in the European banking world: the SEPA (Single Euro Payment Area). Many ideas are circulating on this issue. What is to be expected from the SEPA? In which new areas will the card be used? And who are the new actors in this redefined banking landscape?

Loyalty and Gift Cards, 9:30 am – 5:00 pm
The loyalty and gift card market is in full development. Ideas and market opportunities are numerous for those who wish to target specific persons and areas.

Electronic Documents, 9:30 am – 5:00 pm
Electronic administration is undergoing significant development. In addition, the activity in the e-passport sector continues to grow. With specific application examples, this day-long session will provide an overview of what's available now and what's coming.

POS & Kiosks, 9:30 am – 5:00 pm
Payment terminals have adapted to different market evolutions (contactless, biometrics, etc.). Due to their effectiveness and ease of use, consumers are using them more. Now, multi-function kiosks that promote integration are cropping up.

NFC and Contactless, 9:30 am – 5:00 pm
Thanks to near field communication, contactless technology has gained more popularity. What development opportunities are available and which sectors will benefit the most from NFC? More importantly, when will its international deployment take place?

Photo credit: Anne-Emmanuelle Thion

New York and Utah pioneer use of bank-issued contactless cards for transit fare collection

MasterCard, Visa, and Amex cards replace the ticket in high-profile public transportation trials that could change transit forever

Andy Williams
Contributing Editor, AVISIAN Publications

A new way of riding the rails and roads – or rather paying for those trips – may be in the wind at two transit agencies across the country from each other. Both involve contactless payments, but what sets these initiatives apart from contactless fare collection programs around the country and world is the use of branded payment cards (e.g. MasterCard, Visa or American Express).

Most transit agencies – or their vendor of choice – issue their own cards, process their own transactions and handle their own settlement. But what if this effort was handled by traditional payment card issuers and processors? That is the question that transit managers in New York and Utah set out to answer.

New York City, operator of one of the largest public transportation agencies in the world, is in the midst of one such pilot in some of its subways. It recently extended that pilot by at least six months and is getting ready for a second trial involving buses. The Utah Transit Authority (UTA) completed its pilot last fall on the buses that take skiers and employees up to four of the state's ski resorts. That same trial will continue this fall while UTA prepares its infrastructure for a full-scale rollout of contactless payments.

While a lot of geography separates both systems, they do have a link: Craig Roberts, UTA project manager, and Paul Korczak, New York City Transit's (NYCT) assistant chief officer for the MetroCard, co-chair the Smart Card Alliance's Transportation Council.

It's not our goal to deliver cards in 48 hours.

HID Priority Plus™ combines our unrivaled know-how with our unmatched can-do.

We know that when you order new credentials, it's not about stocking up, it's about security. That's why we have HID Priority Plus Credentials Service guaranteeing the shipment of 100 to 1,000 standard credentials, Prox or iCLASS® technology, within 48 hours anywhere in the United States and Canada. The reason we do it is simple – we can. No one manages more technologies, makes more credentials or has a longer track record. And, of course, every credential comes with a lifetime warranty from your trusted source, HID.

HID

hidcorp.com

ACCESS service.

"Both trials worked out very well," commented Randy Vanderhoof, executive director of the Smart Card Alliance.

The two systems have different types of riders with different needs. New York's transit system has one goal in mind: getting its passengers from Point A to Point B, often during heavy morning and evening rush hour. UTA is looking to provide better services to students, employees with company ID cards, and even federal agencies supplying the FIPS 201 compliant ID cards.

"What they were trying to do (in New York) is a proof of concept to show that an account-based fare system can be operated cost effectively and with a financial institution partner where the transportation authority acts as a merchant rather than a card issuer," said Mr. Vanderhoof. "This is a fundamental change in the transportation model where a transportation organization issues their own cards and settles their own accounts."

The New York experience

In July 2006, in partnership with MasterCard and Citibank, the Metropolitan Transit Authority (MTA) and NYCT launched a trial of standard, contactless bank-issued smart card devices to pay transit fares directly at the point of entry without the need to purchase fare media. MTA is a regional governing body that oversees the transportation area around New York City, Long Island, all of New York's boroughs and Connecticut. NYCT is the subway operator.

With annual revenues of $2.8 billion, NYCT's combined subway and bus services provide nearly seven million daily passenger trips, most of which are paid using the MetroCard automated fare collection system.

"We focused on our Lexington Avenue Line, our most heavily traveled route," said Mr. Korczak. The pilot involved 30 stations, each with one MasterCard-supplied contactless reader at a designated turnstile.

At each entry point, one fare gate was equipped with a standard ISO/IEC 14443 and MasterCard PayPass-certified smart card reader. The reader and the fare gate were branded with a logo designed specifically for the pilot. These gates can also accept NYCT's standard MetroCard.

Through partner Citibank, customers participating in the trial have the option of selecting a contactless credit or debit card (with a traditional magnetic stripe) or a key fob.

Proof of the pilot's success comes from "our executive leadership deciding to extend the pilot to buses," said Mr. Korczak. "The ballpark goal is to include about 275 buses in the pilot. These will be buses that are part of MTA transit bus routes."

When the subway trial kicked off, "we initially decided to use (the standard) value-based fares, but in buses we'll actually have value-based as well as three different types of passes

– day, weekly, monthly as well as bus-to-bus and reduced fares for seniors and handicap riders," he added.

Reader placement caused some problems. "We had to place it on the front of the turnstile" a little lower than was possibly needed. But NYCT had to work within the existing constraints of the other equipment already there. "If you go to Washington, Boston or Atlanta (where closed contactless automatic fare collections systems are in place) the reader is placed higher and on an angle so it's very visible." With NYCT, riders "are having to look down and to the side," he added.

The bus trial will include another major change. It will involve all card brands and issuing entities "which put out some kind of contactless instrument," said Mr. Korczak. "At some point, we'll have a reader that says Visa, Amex, MasterCard."

"I tap at the turnstile and it charges me for that ride. It tells me (rather it tells NYCT) that I entered at 9:14 a.m. at Union Square. Then there's the payment transaction which appears on the customer's bank statement."

He says early indications are that "card companies are very excited about this extra opportunity."

The scheduled six-month bus trial will involve 275 buses with a contactless reader being installed on all of them. "We haven't selected the bus routes yet. We're trying to pick some cross town routes that will enable bus customers to transfer from subway to bus, and we will include some north-south lines so customers can transfer from bus to bus."

While the subway trial was expected to end earlier this year, it has been extended with no ending date yet set, said Mr. Korczak.

Utah's ski resorts ride high

UTA, headquartered in Salt Lake City, could almost be considered the state's transit agency since it serves 83% of the state's 2.6 million people, said Mr. Roberts. Last year, UTA began a contactless trial with the four ski resorts the agency services.

For 30 years, UTA has used a paper-based ticketing system. The agency saw the ski resort trial as a chance to test what to UTA was a new technology. Mr. Roberts said he had heard a lot about contactless payments and had investigated it quite a bit. Its ski resort fleet is a special service UTA offers the resorts using specially configured buses to carry skiers and resort employees the 15 to 20 miles up to the resorts. At just $3 for a one-way ride, it is the best deal in town.

The agency had been accepting season passes and employee IDs for ski resorts, what he calls "flash passes," which means the card is "flashed" to the bus driver as the rider enters. "But both the resorts and UTA were unsatisfied with the method being used to count those trips," said Mr. Roberts. It was manual with the bus driver "making ticks on a piece of paper."

UTA's operating division "came to us and wanted us to develop a technical solution. We

thought about bar code readers but at the same time we were investigating electronic fare collections. One of the interesting things from UTA's standpoint was that we didn't have an automatic fare collection legacy. All we did was accept cash and tokens and paper tickets. We were intrigued by the fact that a contactless product was being launched then. We looked at (MasterCard's) PayPass and Chase's blink card. We decided the best way to learn was to do it rather than study it."

The agency issued an RFP (request for proposal) in January 2006. While UTA's main goal was accounting for the passes issued by the resort, "we also wanted to accept all these other media, contactless debit and credit cards. MasterCard came on board first, then Visa and Amex followed," he added.

In the RFP, "we required the proposals to include a reader certified for (reading credit/debit cards). ERG (the fare collection system integrator selected for the project) included their standard reader to read passes and an OTI (On Track Innovations) reader to slave off their reader (to read the credit/debit cards)," he said. ERG didn't have time to get their own reader certified, which meant two readers had to be installed at the buses' entrances, said Mr. Roberts.

The ski resort pilot kicked off December 7, 2006, less than one year from the release of the RFP. "When we did that," says Mr. Roberts, "we didn't know it was possible because some people told us things didn't happen that fast."

But happen it did. "One of the reasons we picked (the ski resorts) for the pilot was because it's a manageable number of businesses. We could get a pretty good test of the technology." The trial, which officially ended last April, was deemed a success and skiers and resort employees liked it, said Mr. Roberts. UTA intends to run a similar program for the 2007 ski season. "We've created expectations on the part of the ski resorts and customers and we don't want to lose the benefit of the learning curve."

Collecting your money

There are some major advantages to using credit/debit cards rather than tickets. But it also means the financial industry has to look at transit a little differently.

What's so attractive about this payment method, whether it be a contactless card, key fob or cell phone (using near field communication) is that the relationship is between the customer and the issuing bank, not NYCT, said Mr. Korczak. "It's like a retail purchase. You know you can take your bankcard and go from Target to Tiffany's. Customers don't think about the different payment mechanisms."

But transaction cost is obviously of great concern to transit bodies and the traditional fee structure associated with branded card payments created a chasm that many thought impassable. Mr. Roberts, explains, "the structure of interchange fees in normal transactions has a flat fee component. If (the flat fee) is a significant percentage of the actual fare, it doesn't make sense to do it," he said.

The banking industry realizes that for micropayments to be attractive to the merchant (including NYCT and UTA), transaction aggregation will have to be allowed. "That's where you bundle up a bunch of transactions by the same customer into a single payment transaction. It makes single payments economical and banks can do things to their fee structures which can be beneficial to us," said Mr. Korczak.

Mr. Roberts cites iTunes as a good example of aggregation explaining, "you can order one tune at a time if you want, but Apple waits until they collect a bunch of those transactions before sending them off to the payment network."

In UTA's pilot with the ski resorts, "we were allowed to do aggregation by MasterCard, but not by Visa and American Express. But over time, I think aggregation will be allowed by all of them," he added.

Mr. Roberts sees several other viable strategies that UTA could use when conducting credit card transactions, but all would involve acceptance by credit card companies. "They could create a different business category for transit agencies. I think that was the pattern when they got into grocery stores," he said.

Another option, similar to prepaid, is for UTA to "set up an account-based system, an alternative to an open payments platform, with MasterCard, Visa and American Express, where we get charged the same rate. The cards would only be used for credentials to reference a prepaid account. Every time they touch their card in the system, it would apply (to the rider's account). When we see the transaction, the first thing we'll check is whether this cardholder has a prepaid account and then we'll apply the cost of the trip to that account. If a (prepaid) arrangement didn't exist, the trip would apply to his credit card."

NYCT is also considering the prepaid option. "Visa, MasterCard, they all issue some kind of prepaid card," said Mr. Korczak. "About 200 of our retail MetroCard merchants actually offer that for those who purchase at their stores. We may have some customers who say they don't have a bank account, or they don't want one, so a prepaid account solves that problem. They can go out and get one of these and if it's contactless, they're good to go," he said.

SCA's Mr. Vanderhoof says of UTA: "They are creating a new business model that hasn't been done before." It's been a give and take negotiation on both sides, (but UTA has) already demonstrated they can successfully aggregate multiple credit card transactions and process them as one larger transaction, and that's a way to reduce the fees associated with smaller values."

"What the New York pilot is saying is that 'we're in the transportation business, not the card business,'" adds Mr. Vanderhoof. "It lets us see if we can figure out how to leverage the existing infrastructure and still be financially sound. By leveraging the payment transaction networks already in place, we're able to tap into those existing networks and utilize the same payment technology and have it apply directly to the point of entry in the New York subway system while avoiding the extra step of converting cash and value from one card issuer to the next."

Cost of ticketing versus payment cards

"Everyone recognizes there's going to be fees associated with processing these transactions," continues Mr. Vanderhoof. "Those fees are being balanced against the cost savings the operator has of not having to issue cards or collect cash."

Mr. Korczak and Mr. Roberts agree that operators must examine, not only transaction fees, but also the actual cost of collecting those fares.

"We can save substantially over issuing our own fare medium," said Mr. Roberts.

"When you collect fares in cash, it's very expensive," said Mr. Korczak. "Once you start making these comparisons, you'll find that this is very economical."

He said one thing agencies should consider is "what percent of revenue does it take to do automatic fare collection? It's something that's a useful tool for comparison across one property or the next. For every dollar I spend, how much do I spend on collecting it? The banking payments way could be cheaper. Each property has to do its own analysis. Which of those work best? And when customers pay, which is the most cost effective – cash or debit/credit? And if a transit ticket becomes the same as your banking card the cost of ownership gets shifted over to whomever issues the card."

In other words, he added, "If you lose your card, you call the bank, not the transit agency."

That can be a big plus, particularly in New York City.

"Customers completely understood the notion of banking payments," said Mr. Korczak. "They had to get used to contactless payments and when we tested with focus groups we found that when something went wrong, their immediate reaction was to call the bank. That's entirely positive. Customers are trained to know that the banking system works and if it doesn't work, oh gee, I didn't pay my bill, etc. So they call their bank instead of calling us. We were all smiling about that."

Lessons learned

Were there any problems in New York? "The short answer is no," said Mr. Korczak. "The equipment has performed extremely well, and customers are aware of the positives. They took to this like fish to water."

He said the "lessons we learned from the MetroCard is that customers' transportation needs are very flexible, and if you have a pilot limited to one area, you might get customers who say it's not what they need. For example a customer would say to us, 'I like it but wish it were a monthly pass.'"

Security right now isn't an issue either. "I was at a conference run by the Federal Reserve recently and the conclusion of this forum was that you have more security concerns from your waiter than from your contactless card. And on the (stolen) ID side, you have more of a threat from the stuff not shredded in your waste basket," said Mr. Korczak.

Added Mr. Roberts: "One of the things we learned is if you have an exciting idea, the technical people get excited and make it happen. But on the business side, it takes a little longer. It really is a lot more work to deal with the institutions and business side as opposed to the technical vision that a number of people have had within this industry. (Another) is that we needed to involve everyone within our agency who will be touched by this new system … people who are responsible for customer service, operations. We had to liaison with our partners (ski resorts). Everyone has to be involved. They're the ones who need to plan and figure out the rules and processes. Engaging them and getting their support is a critical part of deploying this technology."

What's next in New York?

"We haven't made any decisions other than the pilot," said Mr. Korczak. "We have to get to the second step and get through it first."

MTA has already joined in what Mr. Korczak calls "a strategic alliance with the Port Authority of New York and New Jersey to test the banking payment solution on the Port Authority's Path Train, a commuter rail line that comes into Manhattan. We're looking at testing anywhere

Over
10 Years
Experience in
Contactless Card
Manufacturing

BOOTH 275

Learn more at...
ASIS International
September 24 - 25, 2007
Las Vegas, NV

cpi card group™

1.800.446.5036
contactless@cpicardgroup.com
www.cpicardgroup.com / contactless
An ISO 9001:2000 registered manufacturer

from two to six New Jersey transit bus routes too to show the potential for regional travel."

He added: "One of the things we'd like to try to do is to encourage customers to ride regionally over a broader area using a different series of transportation companies, Path, Jersey Transit, etc. They're all separate entities, but we're trying to find a common thread on how to pay, to make it seamless."

Mr. Vanderhoof said of the Port Authority pilot: "The interest will be in seeing how the pilot of the Port Authority can co-exist with the pilot going on in New York City. The hope is that those systems will be compatible. You'll have the added complexity of multiple merchants co-existing together with a common payment platform that didn't exist before."

UTA: full steam ahead

The ski resort trial showed UTA that it could act as a merchant and accept credit and debit cards. The pilot also enabled UTA "to educate its constituencies (about fare collection and contactless cards). We were able to manage the ski cards and we showed that we could accept contactless cards," said Mr. Roberts.

Earlier this year UTA issued an RFP seeking to take the agency and its riders directly to contactless. As with the ski resort trial, riders will be able to wave their bank-issued cards over a reader. In addition, he wants UTA to be able to handle the ID cards issued by many of Utah's employers and educational institutions.

UTA "made a policy decision to not do mag stripe within our system," he said. That would be like going backwards. "We chose to leapfrog to contactless. Most agencies I know would like to be completely contactless." However, UTA may keep mag stripe around for a while to handle those colleges or businesses that haven't made the jump to contactless.

Mr. Roberts is also investigating the possibility of the system accepting the more secure, FIPS 201 compliant ID cards being issued by some of the federal agencies located in Utah. "Why not use the FIPS 201 cards, read them and bill the federal agencies?" asked Mr. Roberts.

All this is in the future. Right now, UTA just wants the infrastructure established.

When the RFP for the multimillion-dollar system went out, "we were worried we wouldn't get any (responses), but now we've gotten several. We're in the process of evaluating the proposals," Mr. Roberts said.

Mr. Robert's ambitious plans include kicking off the first phase by late spring next year. "I don't know if we can do it or not, but that's what we would like to do."

"The thing about Utah," said Mr. Vanderhoof of the initial ski resort trial, "is it demonstrated that players could come together using existing technology and do a totally new and innovative fare payment system in a matter of months."

"Historically, it would have taken several years to develop a new system like that," he adds. "Utah was able to demonstrate they could put together the requirements, go out to proposal, get off the shelf solutions to deliver their transit fare system and have it up and running in a matter of months. That step has encouraged them to do the same thing system wide and be able to convert the entire system over which should be a model for other transportation operators, particularly tier 2 or tier 3 (the modest to mid-size transit) markets with a small infrastructure."

Mr. Roberts readily admits that without the New York pilot, things might have been more difficult in Utah. "What we've been doing couldn't have been done without the leadership provided in New York," he said. "They had a lot of conversations with Visa and MasterCard and essentially, what happened when we put out our RFP to do contactless debit and credit, because of the work done in New York and in the Smart Card Alliance, [is that] we had people who could look at our proposal and tell us they could participate. If New York hadn't done what they had done, it would have been too big a sell."

He added: "Visa, MasterCard, Amex and the various banks had already done this work in contactless payments. We had the good fortune in coming on the scene and saying let's stop talking about it and do it." ID

Industry group explores options for branded cards in transit

A white paper from the Smart Card Alliance's Transportation Council titled, "Transit and Contactless Financial Payments: New Opportunities for Collaboration and Convergence," addressed the issue of how to accept branded payment cards cost-effectively in transit industry.

One suggestion from the white paper is for an aggregation system of payment "which identifies repeat transactions that use the same payment instrument (such as a credit card) and aggregates the charges up to a certain value or time to process a smaller number of higher value transactions.

The council also offers "other approaches that may make micropayment transactions more cost-effective." These include:

- Subscription-based payment. An up-front payment covers "all you can buy" over a particular period of time.
- Prepaid account. An up-front payment is stored in a customer account and decremented as purchases are made.
- Postpaid account. Where an authorization is made up-front, transactions are aggregated and later settled when a threshold amount or time-frame is reached.
- Direct payment. Micropayments are billed individually and processed over standard payment networks, at fees ("discount") negotiated between the merchant and the acquirer/processor. ID

The *Original*
Multi-Technology Readers

The Most Versatile, Secure Readers in the Industry

XceedID®
Xceeding The Ordinary

To learn more please visit: www.xceedid.com

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

Corporate ID programs require convergence beyond just physical and logical security

Robert M Fee
General Manager Business Unit North America, LEGIC Identsystems

Establishing a corporate contactless smart card program can be a daunting task when considered in its entirety. While the physical security team might drive the project, the end result can easily turn into a corporate-wide, all-in-one credential that provides many departments with a tool to reduce costs, improve efficiencies, and eliminate waste. Best of all, it is also increasing security for environments that require both physical and logical access.

True convergence, however, covers more than just IT and physical access. It impacts the organization at all levels and in all departments. With this fact in mind, an enterprise-wide vision should guide your corporate ID program. The following is an overview of some key attributes that have helped launch successful contactless smart card programs.

1. You need a cheerleader! Senior management involvement & support

Now, not too many executives really like to be called cheerleaders, so you'll have to be careful on this one, but the idea is that you are creating and implementing change for your organization. Jürgen Müller of Cosmo ID, a smart card consulting organization, recommends that you, "look for the senior level management change agent in your organization that will help you with both internal and external obstacles encountered." You're going to be moving beyond a single application to a tool that can add to the overall bottom line. Remember, our C-level executive thinks in these terms and that this will change your credential program from an expense to a cost-savings program that benefits the entire organization.

A well-designed smart card program allows you to reduce operating costs, improve operational efficiencies, enhance use of existing assets, reduce resource requirements and yes, of course, increase corporate security. And another great benefit is that you introduce the technology, but you don't have to manage other departments' use of the card.

2. Team creation & hands-on involvement

Whether the application is physical access control or combined physical and logical access, it's a team project. Physical security, IT and human resources should work together, suggests facilities manager, Corina Gerber, of PricewaterhouseCoopers in Switzerland. She encourages the creation of a team to execute a successful program and to spread this success throughout the organization. The core team tasked with strategic implementation will work with other departments to create a wish list with 'must have' and 'like to have' applications.

Why HR? The HR department interfaces with every single employee and can help construct a training program detailing how the new ID program will be introduced and used with minimal impact on day-to-day operations. Depending on program construction, the HR department might even be issuing the credential to new employees.

Other departments that can take advantage of the new smart card applications can include:

- R&D, finance and sales for secure printing applications
- Cafeteria/POS: Speed up checkout, reallocate resources/headcount
- Vending machines: cashless payments reduce cash handling issues
- Manufacturing: time and attendance to reduce "buddy-punching"
- Facilities management: employee lockers, parking facilities, janitorial, lockers and external off-line buildings and locks

3. Clearly established goals, objects and expectations

Mr. Müeller, of Cosmo ID tells his clients, "With a clear plan and help early on, your program will be implemented faster with less issues and it will have a greater impact on your company." The desire or need to improve existing security requirements typically drives implementation of a contactless program. Department goals such as physical security and IT logical access can easily be combined with corporate goals that focus on reducing head count, utilizing existing resources more efficiently, and even saving time via activities as basic as getting through the lunch line faster.

Once the new smart card has been issued, each department wanting to take advantage of the new technology can run pilots and make independent evaluations of other departments' projects. Each project can then be implemented in its own time frame and with a choice of vendors. Since smart cards can be updated in the field while in use, new applications can be added or removed with minimal impact on day-to-day operations or inconvenience to employees.

4. Implement smart card best practices

Any identity management system must take into consideration not only built-in smart card security features but also privacy issues. Implementation of best practices can help protect both your employee and your company. Why use personally identifiable information such as a social security number when alternative models work as well?

To help you identify and define what you need to evaluate, the Smart Card Alliance published a document entitled *Best Practices for the Use of RF-Enabled Technology in Identity Management*. The document and an associated FAQ, *Best Practices for the Use of RF-Enabled Technology in Identity Management*, is available on the Smart Card Alliance's web site at www.smartcardalliance.com.

5. Testing/evaluation of smart cards technologies

As with access control software, you have a very wide choice of smart card technologies. Contactless, contact or even dual-technology

smart cards that utilize a contact chip with an antenna are readily available. Hybrid cards and readers that can contain multiple technologies such as 125K Prox and 13.56 MHz contactless to help address migration issues are also available. Because this is evaluated as a corporate investment, you need to consider both short-term and long-term impacts.

Remember, there are two components to the testing and evaluation of smart cards: readers and credentials. The credential is a data input device designed to provide selected information once formal and authorized communications have been established. Leading contactless technology platforms (reader & credential chips) include major chip providers such as LEGIC Identsystems, NXP and INSIDE Contactless. Your underlying choice of contactless technology could enhance or limit your abilities to expand use of the credentials. ISO standards such as 14443 or 15693, while providing interoperability in certain cases, do not guarantee interoperability between reader and credential vendors at the data level. The key to any system is testing all of the components.

Here are several functions that your contactless reader should provide:

- The reader should have flash memory to allow future feature enhancements to be added in the field and to be configured independently by different suppliers.
- The reader must support the use of encrypted RF data transmission, mutual authentication and anti-play-back mechanism while communicating to any access credential.
- The reader should be capable of supporting the required application. Does the application require that the readers read and write to the credential or just read application data from the credential?

Some key questions related to the credential include:

- Does the credential support open or structured file management system as your choice determines future system enhancements, flexibility and supplier interoperability?
- Does the credential have sufficient memory capacity to support today's physical access control system and tomorrow's ePurse and biometric requirements?
- Does the credential limit the number of application segments to a pre-defined set or does it provide flexibility to efficiently add applications for future system enhancements?
- Are you locked into your credential supplier or are you free to evaluate and select from competing vendors? What are your testing criteria for card durability and printability?
- Have you evaluated printers and personalization equipment with each vendor's credential?

6. Application selection

Smart cards support multi-applications – different applications often offered by different vendors. If you select a specific vendor's smart card, can it be used by other departments for other applications? Have you asked your vendor this question? At the end of the day, who actually owns and controls the credential, you or your vendor?

Smart cards provide you the flexibility to add applications at any time to the existing card population. Depending on the underlying smart card technology, there is no set sequence in which applications are implemented. Here are just a few of the most popular smart card applications in use today:

- Physical access control
- Logical access for computer and network login
- Time & attendance
- Biometrics for physical/IT access and time & attendance
- Cafeteria and vending machine payments
- Parking control
- Printer/fax/copy machine management and payments
- Follow-me-print applications designed to keep documents stored in a print spool waiting to be released to the printer until the employee has authorized it, preventing documents from being forgotten at the printer and read by other employees

7. Roll-out process

Here's where the rubber meets the road. Depending on the size of your organization, you might take the plunge and do it all at once or consider slowly migrating to the new smart cards department-by-department or building-by-building. In any case, consider only implementing one application at a time starting with physical access or IT logical access and then add new applications once all the kinks are worked out.

On your side is your vendor. Let them help you address the rollout process based on their experience in similar situations. They want a smooth rollout as much as you do which is why they typically offer a full line of single technology and hybrid readers. Hybrid readers contain multiple reading technologies that allow you to continue using older technology such as 125K prox credentials for certain applications while you implement newer smart card based applications. In any case, keep the following in mind:

1. Credential issuance process
   - Will it be centralized or localized?
   - Who has responsibility and authority to issue credentials?
   - How are temporary IDs issued to guests, vendors and consultants?
   - How do you address misplaced, lost or stolen credentials?
   - How do you address the daily question "I left my ID at home"?

2. Employee training on use of credential
   - Who, when, and how is this done?

3. Revocation process
   - Do your systems utilize a single database or multiple independent databases? Remember, multiple databases mean multiple steps to remove a credential from all systems.

Finally, remember that a successful smart card program takes time and attention to detail. The resulting program can be a showcase for your organization, but don't rush things. The headache you might choose to avoid today can turn into an expensive migraine further down the road.

HID iDENTITY

Easing multiapplication smart card issuance for physical and logical security convergence

Andy Williams
Contributing Editor, AVISIAN Publications

With a series of significant acquisitions, HID Global has been expanding its access control empire. Earlier this year, the company combined some of these new resources and capabilities – specifically those from AccessID and Synercard – in a new company called HID Identity. The new entity's mission is to offer a comprehensive set of solutions for the deployment of contact and contactless smart card-based identity credentials.

"End-users are frustrated by how difficult it is to issue a single credential that works across all their applications – physical access control, logical access, time and attendance, cashless vending," said HID Identity general manager, Dennis Caulley. "With HID Identity, this problem is eliminated, and the credential is provisioned for multiple uses right out of the printer."

The new organization aims to benefit end-users by providing solutions and expertise to help streamline and simplify the acquisition and issuance of access control and multiapplication credentials. HID Identity will also help end-users achieve an important identity management goal – issuing a single secure credential that links the enterprise's diverse set of applications.

The new organization leverages AccessID's strength in providing secure card solutions for the electronic identification market, including iCLASS®, DESFire®, barcode, magnetic stripe and contact smart card technologies, all on one card. Adding to that strength, it uses Synercard's badging software development skills. Its interoperable photo ID and ID card application control software allows organizations to create, manage and verify an individual's credentials. One of its software products is Asure ID, a control solution for organizations that need to collaborate and share data or need their smart photo ID cards to work with other enterprise systems.

A major reason for the creation of HID Identity was that AccessID and Synercard "had many similar channel partners," explained Chris Sincock, vice president of sales and marketing for HID Identity. That included the identity systems channel, the sale and support of ID systems, badging software, printers and consumables, he added. Now, he said, HID Identity is "the group within HID Global that has a high level of expertise in designing and deploying credentials."

"We recognized that, under one roof, we had a very high level of expertise and that, by focusing our expertise on this market, we would bring together skills that our customers were requesting," said Mr. Sincock. "We have some very knowledgeable people relative to card issuance, card manufacturing and software development, and we wanted to get these resources working together as a base for the rest of the organization."

Configuring multiapplication card with a click of a mouse

HID's iDIRECTOR™ technology platform was launched earlier this year. The latest in the Asure ID photo identification software line, it allows multiple applications to be loaded onto a smart card via a single, seamless process. The software incorporates application modules from several HID technology partners: RF IDeas Air ID for logical access control, QI Systems' QiWave™ Purse for electronic vending, and Bioscrypt Fingerprint for biometrics,

Smart Card Alliance

Smart Cards: The Future of Digital Transactions

Compelling Content, Convenient Venue

The Smart Card Alliance brings together the entire industry in a comprehensive overview of recent market developments and trends and technologies that lie ahead. For anyone with a stake in digital transactions or ID security, the Annual Conference 2007 is the place to make or renew professional contacts, take stock of this changing industry and lay plans for the year ahead.

Interest continues to grow in smart card technology for transactions of all types, including contactless credit/debit, two-factor authentication, government-issued ID, transit fare payment, and a movement towards convergence among identification, access, and payment systems around a common card or device, such as mobile phones. Following this year's conference theme, Smart Cards: The Future of Digital Transactions, we'll feature an expanded look at these payments and identity applications, and speakers with first hand knowledge about the latest smart card implementations.

A conference agenda with over 50 speakers features leaders from the financial services industry, analysts, government officials, end users, and technology insiders in an interactive, instructive forum on the business issues, implementation milestones, and technology advancements happening in the smart card market. The highly regarded Smart Card Technologies and Standards Workshop follows the conference. The Marriott Long Wharf Boston gives you quick access by airport, car, train or subway, room to network with 300 attending colleagues and access to the city in the evening.

Conference Tracks Cover Every Key Topic in Today's Market:

- Payments
- Mobile/NFC
- Identity
- Security
- Government
- Healthcare
- Transportation
- Emerging Technology

A Key Component in the Digital Transactions Revolution

Get ahead of the curve: This year's conference takes a close look at the changing world of digital identity and financial transactions.

- Secure identity program rollouts
- Contactless payments stakeholders panels
- Mobile payments and NFC pilots reports
- HealthID and payments convergence
- Privacy and security best practices
- Emerging smart card technologies

New: Early Bird Discounts

Get 10% off if you register by September 14
Visit www.smartcardalliance.org today or email us at events@smartcardalliance.org

Smart Card Alliance Annual Conference 2007

October 9-11 • Marriott Long Wharf • Boston, Mass.
www.smartcardalliance.org

all accessible through a drop down menu. Now, explained Mr. Sincock, multiple applications can be loaded onto a smart card in one step at the point of issuance.

"On the identity issuance software, such as Asure ID with iDIRECTOR, if an organization uses a QI system of cashless vending, they can go to a drop down list of drivers to see how to provision that card with that application."

Better servicing core markets

Mr. Sincock says the emergence of HID Identity will help HID Global increase its offerings to some of its core constituencies, like the education market, government and healthcare. "We are there to support all sales organizations and channels within those (core) markets."

Education
HID products can be found on an installed base of around 200 colleges, and the organization recently bolstered its commitment to the education market, hiring Mark Doi to support the sales and migration of HID technology to that market. With prior experience at Ingersoll Rand Security Technologies and Onity, Mr. Doi's main goal is to work with campus administrators migrating to multi-function iCLASS cards via HID Identity."

"We want to help colleges understand the technology choices they have. A majority of schools are still on very insecure legacy technologies like mag stripe or bar code," said Mr. Sincock. "Through iCLASS, we can provide the ability to store multiple data sets besides just access. We can install application data for libraries or food services, etc.," he added.

"When you look at the education card, colleges have been leveraging the power of the card for multiple applications for a long, long time. They're getting people into facilities, using it for meal plans, libraries, plus it has other uses, scraping frost off a wind shield, for example," he laughed. "We've developed specific card formulations for that marketplace that allow the card to withstand more abuse."

Government
As the FIPS 201 standards develop and gain adoption, Mr. Sincock sees HID Identity getting involved with more government projects. "With FIPS 201, our expertise is in card manufacturing, and the current specification requires a minimum of one embedded anti-tampering feature, such as a hologram," he said.

Healthcare
With healthcare, he said there is increasing concern for credential security, "and you need cards with embedded security features here, too. In many ways it's a campus-type environment because, oftentimes, meals and cafeterias are subsidized. Plus, healthcare providers are looking for HIPAA compliant cards that allow the cardholder to securely log on and log off (to a patient's record)," he said.

This is also where iDIRECTOR can help, he believes. "Everybody in the market is enamored with smart cards, whether they're contact or contactless," Mr. Sincock said. "While smart cards are useful for many applications, the key question is 'how can I get all these data sets on one card?' A badge often needs to serve multiple functions – access control, time and attendance, e-purses for use at the cafeteria. How do you accomplish all that with one card? And wouldn't it be better if, when you issue the card, all these functions could be enabled at that time? iDIRECTOR satisfies that need."

The reaction so far …

What kind of industry reaction has HID Identity generated so far? "We've created a bigger buzz than we could ever have hoped for," said Mr. Sincock. While continued North American growth is one of its goals, "we'd also like to see the growth of cards and credential sales within HID Global worldwide," he added. "We want to leverage our expertise in custom printing and security. Likewise, we look forward to continuing the development of Asure ID credential issuance software so it continues to incorporate more features, especially regarding our iDIRECTOR™ smart card provisioning technology."

What's next? "I think HID Identity has a tremendous opportunity to have an impact on HID Global's growth. At the end of the day, we don't care which channel provides the solution to the end-user, we just want to make sure that the end-user's problems are solved."

Contactless expertise helps CPI become a leading producer of secure cards

New ownership brings new capital, capacity and expansion

Andy Williams
Contributing Editor, AVISIAN Publications

cpi card group™

CPI Card Group is ready for prime time. Not that it hasn't been all along, but thanks to extensive investments in equipment and personnel, the Colorado-based card manufacturer is getting ready for an "exploding" card market, whether contact or contactless. And prime time or not, it also now has a new owner.

A made-up word best describes the company's current situation. With extensive investments, the company is currently at what Bob Clarke, the company's vice president of sales and marketing, calls "over capacatized. We figure if we build it, we'll be able to deliver." When that will happen isn't known, but when it does, CPI Card Group will be ready.

The company started out as Plastic Graphics, a small San Diego, California company with annual revenues of about $700,000, said Mr. Clarke. In 1987, Antonio Accornero, who was operating a badge and trophy business with his brother-in-law, producing badges and buttons for Disney and others, bought the small, non-certified facility. After about a year, Mr. Accornero moved the company to Los Angeles, where he built it "into one of the largest and most technologically advanced facilities on the West Coast," said Marisha Barber, CPI's marketing and communications manager.

"(The company experienced) an explosion of growth with the prepaid phone card market," added Mr. Clarke.

From there, Mr. Accornero started thinking about the secure market. "It didn't make sense to expand his existing business," added Mr. Clarke. So in 1995, he acquired Colorado Plasticard, a privately-owned company based in Littleton, Colorado, "that had a very high quality reputation."

In 1999, Plastic Graphics was changed to California Plasticard. When it moved to Las Vegas, Nevada, it was renamed after its sister Colorado operation, CPI Card Group - Nevada, Inc. Obviously, to have both the Colorado and Nevada companies under one umbrella meant dropping "Colorado" from the company name. CPI Card Group was the result.

What does "CPI" stand for? As Mr. Clarke explained it: "Literally we are very Passionate about this business and very Innovative." The "C" stands for "Confident." Mr. Clarke oversees sales, marketing and customer service. Before joining CPI, he was a national account manager for DataCard Group.

The move allowed the company to segment its production. The Colorado plant produces cards that demand security, while the Las Vegas operation concentrates on non-secure cards, such as loyalty or gift cards.

A "heck of a learning curve" establishes CPI as a leader in contactless card production

It was around 1995 that CPI Card Group got involved in a new technology that opened more doors. "We started working with Motorola on a project they had in mass transit. They needed a dual interface, contact and contactless card, and they eventually selected CPI Card Group to manufacture these cards," said Mr. Clarke. It led to what Mr. Clarke describes as "a heck of a learning curve" because the company had never manufactured contactless cards before. "We worked very closely with Motorola, and eventually we introduced that process in both facilities."

Even with its expertise in contactless applications, Mr. Clarke says that CPI Card Group considers itself "technology agnostic. We're not married to a specific technology. We will manufacture cards as requested. That gives people a good comfort zone because they're not being held captive by the technology."

Yet, with its contactless background behind it, CPI was invited to participate in Chase's MasterCard PayPass project in 2003. "We manufactured 100% of the cards at the time," said Mr. Clarke. "They (Chase) selected us for their contactless pilot in Orlando, and we got very good feedback from all parties involved about our cards."

In 2004, CPI was certified by Discover and American Express, and in 2005, "we participated in the initial launch of Chase's blink contactless cards," he added. "We've participated in five additional launches in 2006" with several other well-known banks.

Added Benoit Guez, vice president of smart cards and international sales, "We're working (now) with more than 20 different issuers in the US, Mexico, Canada and Central America."

Mr. Clarke estimates that the company produced some 720 million cards last year with 166 million of them secure cards. "That would rank us as the highest provider of secure cards in the US."

CPI recently launched a program known as "Kick Start" designed to help more issuers, primarily the smaller ones, get involved with contactless payment cards. "It's an initiative with MasterCard and INSIDE Contactless (a semiconductor company dedicated to producing contactless chips) in order to help the second and even third tier MasterCard issuers enter contactless technology," explained Mr. Clarke.

"With INSIDE Contactless, we are offering a very cost-effective price for MasterCard PayPass. It is really helping the smaller banks. This has been an initiative that MasterCard has supported very actively," said Mr. Clarke. "So when (a smaller bank) asks for a quote on 10,000 PayPass cards, we can offer them a promotion that can have these guys start the program. Instead of charging the standard price, we're charging them the sponsored price," he added. However, while it garnered a lot of print and requests for more information, not many have signed up yet as the program is still in its infancy.

The company has also been working for the past 18 months, said Mr. Guez, to build a card that will comply with FIPS 201. "We have been successful in passing all tests. We did that through an independent company that showed CPI was green on all the tests. We were among the first to have these resolved, a clear achievement for us."

He added: "The strategy here is to present CPI as a US-based card manufacturer able to produce cards meeting all the FIPS 201 requirements." While CPI hasn't yet delivered cards in this area, "we are in communication with several opportunities, projects that we're working on where CPI is being considered for card manufacturing," added Mr. Guez.

According to Mr. Guez, CPI is working on having its card listed on the Government Services Administration's Approved Products List (APL) for FIPS 201.

Financial and identity cards seen as key high growth markets

"We have been involved with contactless for the last few years, and we do believe there is a huge opportunity to grow in this field," said Mr. Clarke. Those opportunities are in two major markets, financial and identity. "We have offerings for both markets. Obviously contact would not necessarily be in the US market, more like Latin America or Canada. A dual interface might also be used in Canada" as the country comes to grips with EMV compliance. "Contactless is more in the US. These are two segments where we want to be a strong player."

The think-ahead mentality has certainly helped. "Our current capacity positions CPI as Number one in North America. We have a huge production capacity for contactless cards," said Mr. Guez.

"In the last three years we have reinvested heavily into building a platform in both facilities," said Mr. Clarke. "In Las Vegas, we moved into a new 156,000 square foot facility from our California plant."

In 2005, CPI expanded its Colorado location so its 70,000 square foot plant can now handle some 300 million secure cards a year, he said.

"We're unique in how we approach the market," said Mr. Clarke. "We produce secure cards only in Colorado. The integrity of the counts is critical. For us to bring different products in here would be difficult. And with financial cards it is a very different product then others. You can't mix the two in the same plant and be effective and focused as well."

New ownership brings new capital and opportunity

The next major change for CPI occurred in late June, when Mr. Accornero announced his official retirement. A "partnership" was reached with Tricor Pacific Capital, Inc., a private equity firm with offices in Lake Forest, Illinois, and Vancouver, British Columbia. At his retirement, Mr. Accornero turned over the CPI reins to the company's top management: Mr. Clarke, Russ McGrane, director of operations, and Scott Heck, chief financial officer, all who are also now shareholders under the new arrangement with Tricor.

Essentially, Tricor now owns CPI Card Group, but suggests it will be taking a hands-off approach with the company. "We found these people (Tricor) to be just dynamite to work with," said Mr. Clarke. "We wanted to pick a culturally similar group of people with a similar outlook and work ethic. We were the ones who initiated it (the sale)," he added. He reiterated that the company didn't need the money, but the company's major shareholder just wanted to retire and move on.

"We chose Tricor because it represented a very good fit and we've had a good reception from our customers in the marketplace who find this an exciting opportunity for us," he added. "This partnership allows us to continue to grow and invest in the future of CPI."

"We are proud to partner with CPI," commented Tricor's Brad Seaman. "Their recognition in the industry and progressive approach to growth complements Tricor and our initiatives."

Tricor invests in profitable, middle-market companies located in the West and Midwest regions of the United States and Canada. It has approximately $800 million of funds under management.

Meanwhile, for CPI, it's business as usual. "I think one of the attractive things we offer is a very stable product," said Mr. Clarke. "And (thanks to its recent investment in equipment), if the market explodes, we're capable of meeting the demand."

Mr. Guez put it another way: "We're ready for the big volumes. We're not afraid of it."

Exhibitions & Congress

13 - 15 November 2007

Paris-Nord Villepinte Exhibition Centre - France

SECURE TECHNOLOGIES AND BIOMETRICS EXHIBITION

iD IDENTIFICATION

Showtime for Identification!

The widest international offer
8 Dedicated conferences

Co-located with:
The world leading event in
digital security and smart card

22 Years Supporting the Smart Card Industry
CARTES 2007

Prepare your visit on

www.identification-show.com

Free badge • Exhibitors list • Exhibitors news
Special events • Congress registration • Practical information

FOCUS on ASIA — Japan at the honor

CARTES & IDENTIFICATION 2007
70, Avenue du Général de Gaulle
F-92058 Paris la Défense Cedex
cartes@exposium.fr

Cartes & IDentification, exhibitions organized by **EXPOSIUM**
www.exposium.fr

Slippery Rock University breaks ground with its contactless cell phone payment

Leading payments processor, Heartland Payment Systems, joins the ranks of campus card providers

Andy Williams
Contributing Editor, AVISIAN Publications

Contactless technology is coming to the 8,600-student strong Slippery Rock University in Pennsylvania. But it won't be a card. It's coming via cell phone, thanks to a small tag not much bigger than a postage stamp.

When Slippery Rock's students arrive for classes this fall, they'll be greeted with a new campus card and an accompanying 13.56MHz contactless token designed to stick to the back of any cell phone.

Both tag and card are being delivered by Heartland Payment Systems, the sixth largest payment processor in the world. It has been processing Slippery Rock's credit and debit card transactions for the past 10 years, so it seemed a natural fit when the university decided it wanted to introduce a new technology for the college's campus card. Dr. Robert Smith, the university's president, wanted to involve the cell phone in the new program because of its ubiquity among students.

Barry Welsch, manager of IT priorities for Heartland and the project manager for the Slippery Rock implementation, is also vice chairman of the SRU Foundation Board. He recalled that one day Dr. Smith, "wrote me a letter asking if I knew of any products that could make their current on-campus Rock Dollars program (the university's declining balance program) more robust" while enabling off-campus merchants to accept the card.

As Dr. Smith explained later: "We want to leapfrog the current technology and go to the cutting edge, and we want to add value to our student's experience at Slippery Rock. We believe this is the future and want to be educators of our students in the management of this technology … to take a responsible role in helping them learn to manage it."

Once the scope of the initiative was developed and deliverables were identified, the university solicited competitive bids from a variety of potential vendors. With its advanced technology and visionary approach to the future of campus payments, Heartland earned the right to be Slippery Rock's exclusive provider of this service.

Dr. Smith added: "We needed a partner who was courageous enough to bring it to the US and work with us on the introduction of this application. We knew we couldn't do this by ourselves, and frankly, there wasn't anyone we could have more confidence in than Heartland to do this for us."

Mr. Welsch consulted with Heartland's chairman and CEO, Bob Carr, and the two decided Dr. Smith's request was very feasible. "He (Dr. Smith) wanted to leap past the current mag stripe technology … and give students exposure to new technology they will be seeing when they leave the university. He also wanted to raise the image of the institution," said Mr. Welsch.

"It was Mr. Carr who suggested contactless," said Mr. Welsch. "We talked about using the cell phone as the access device because it's the most commonly carried item by far."

A student focus group drove that point home. "We asked the students several questions: 'How many of you have at least one dollar in change in your pocket?' Only four of about 50 in that group had at least a dollar," recalled Mr. Welsch. "About 75% had their student ID cards. But every single student, except one, had a cell phone. And that student had lost his the day before. It was very clear to us that a cell phone goes with a student everywhere. Mr. Carr told me later that students know they've lost their cell phones four times quicker than if they've lost a wallet."

To make this happen, the most obvious choice would have been near field communication, a technology developed several years ago by chip makers NXP and Sony that gives cell phones RFID capability, allowing them to be read by contactless readers. But the technology is still new and not yet widely available in the US. So Heartland went the next best step: producing contactless-enabled tags that can be affixed to the student's cell phone.

Why tags? Heartland and SRU got some reinforcement for this decision from the same focus group. "Another thing quite interesting we learned," said Mr. Welsch, "is that students said when they visit with family members and friends and someone pulls out a credit card branded with a university name rather than a vanilla Visa card, they felt envious. Students were really excited about the fact that students from other universities won't have this. President Smith loved this idea."

How does it work?

Students, faculty and staff this fall – about 10,000 of them in all – will be receiving a half inch wide by 1.5 inch long contactless token with a strong adhesive backing they can attach to their cell phones. It then works like any contactless card, meaning that it can communicate with the reader without physically touching it. The readers have lights that indicate whether the tag is being read or not.

"We tested it on the outside of the phone, and you can scan within an inch and a half. When inside the phone, you need to be about an inch closer," said Mr. Welsch. He suggested that some students may want to remove the phone's battery cover and insert the tag there.

If a student changes phones, he can remove the tag and reattach it to the new phone. If the tag won't come off, the student can apply for a new tag.

The tag "has a very durable exterior. It can't be scratched, and it seldom will show signs of wear," he added.

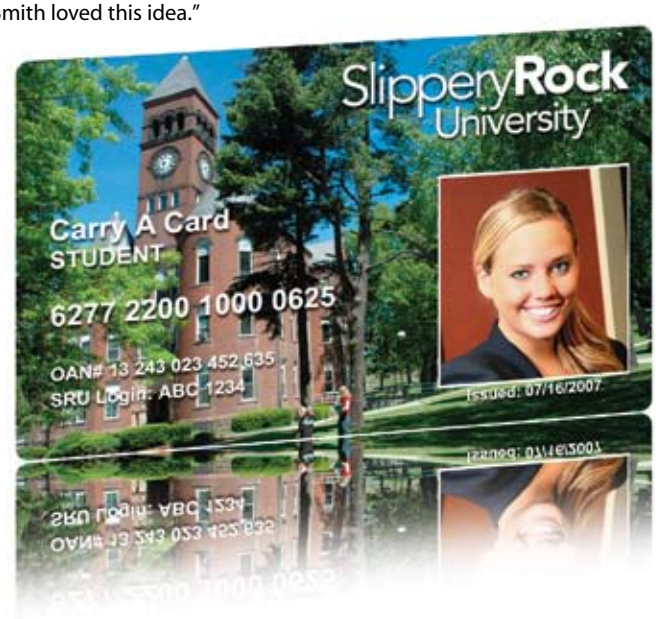
Heartland is also issuing new student ID cards since the company will, for the first time, be processing the student Rock Dollar accounts. Before, Heartland processed only the traditional credit and debit charges students and parents use to pay tuition, room and board and to buy books, Mr. Welsch said. "We've not had anything to do with Rock Dollars. It's something the university has maintained on campus with proprietary readers and terminals."

The Heartland-issued ID cards, however, are still equipped with mag stripes rather than contactless chips. Dual technologies mean making sure the university has readers that can handle both. "Everything we're building – the laundry, vending machines, merchant-attended POS terminals – will all have readers that can read the contactless token" as well as the mag stripe cards," Mr. Welsch continued.

"As far as we can tell, this dual technology is unique. It's the first application in a higher education institution in the US to go this way."

Once the new cards are issued, Heartland will transfer the old Rock Dollar balances to new accounts. In this manner, students can seamlessly migrate from their prior cards to the new system without losing deposited funds or having to maintain two accounts.

"On Track Innovations (OTI) is supplying the tags, and we manufacture the readers through our micro-payments division," said Mr. Welsch. That division includes longtime campus card reader manufacturer Debitek, a company Heartland purchased in 2005. "Heartland has



re-engineered the (Debitek) technology," added Mr. Welsch, "bringing it up to state of the art."

Taking Rock Dollars off campus

The second phase of the project is recruiting merchants off campus to accept Rock Dollars. Initial reaction has been positive, reported Mr. Welsch, stressing it's a winning combination for both the university and the merchants. The university doesn't have to process merchant accounts or cut them checks, and merchants get paid daily.

To no one's surprise, the first merchants to sign up were restaurants. "We're also looking at supermarkets, retail clothing stores, a shuttle service and nail salons," said Mr. Welsch.

Before, merchants were paid monthly. There were no off-campus merchants, but still, the on-campus bookstore and foodservice providers had to wait for their money. "Under our system, we process the transactions nightly and generate an ACH deposit to them the next day, exactly the same time as credit card (payments)," he said. Merchants can purchase or rent terminals, starting at $25 a month. The transaction fee varies depending on the amount of the purchase, but averages about 1.5%, plus 25 cents per transaction.

"We do not use proprietary terminals," noted Mr. Welsch. "The merchants like that. They only need one terminal to accept credit, debit or Rock Dollars."

Dr. Smith said the most "perplexing problem" has been the university's insistence to provide greater protection for the students by requiring a PIN when they use their contactless tokens. That's not something merchants usually expect from someone paying with a debit card, specifically at restaurants. "This is creating a challenge," added Dr. Smith.

For on-campus use, that's not an issue since all vendors have a PIN pad. But some off-campus merchants don't currently have a PIN pad. Mr. Welsch said Heartland hopes to have this problem alleviated shortly. Heartland's readers/terminals all have PIN pads, but, said Mr. Welsch, there are also other packages available that include PIN pads merchants can use. Bottom line: if merchants want the students' business, they will need to be able to accept a PIN as part of the transaction.

For smaller transactions, such as those performed at vending machines, no PIN is required.

Managing your account on the web

Another advantage to Heartland's program is that students can go to a web site to check their balances or their transaction history, said Mr. Welsch. The web site option is new. Before Heartland's involvement, students could only utilize a reader to find out their balances.

Students who lose their cards or tag-enabled phones can visit the same web site to get their accounts frozen until a new card and tag can be issued. They can also contact Slippery Rock's card office and receive support through a toll-free number. "The web provides 24/7 access for cardholders and doesn't limit students to having to visit the administrative office during normal business hours to have a freeze put on their accounts," said Mr. Welsch.

"One of the other great features isn't so much contactless but the whole web-enabling structure," added Dr. Smith. "The individual can review his/her account and charges – as well as reload the card from the web or via phone. It's more than just a chip. The whole concept is somewhat revolutionary for us."

All accounts are maintained in an FDIC-insured bank, Mr. Welsch emphasized.

Changing the way financial aid is delivered to students

Another big change is the way students receive financial aid. "Nearly two-thirds of Slippery Rock's students are the first generation (in their family) to go to college, so financial aid plays a big part," said Mr. Welsch. "When financial aid comes in now, the university will take out tuition and room and board and distribute the excess to students."

In the past, this excess was distributed by check, but now that money can be direct deposited into the student's Rock Dollars accounts. "We've gotten quite a few calls from students already excited about the new system," said Mr. Welsch. "All that's been released has been the financial aid form with a new check box allowing for the money to be direct deposited."

Additionally, on- and off-campus paychecks can be deposited directly into the same account.

Giving something back

Another feature involves charitable giving. Remember that 1.5% transaction fee merchants have to pay to accept the student's Rock Dollar card or contactless token? Heartland doesn't profit from it. The money goes back to the students or the charity of their choice.

"We are rebating back to the students through the Give Something Back Network," said Mr. Welsch. Students will be able to go online and select their favorite charity to have this money donated to, or they can have it credited to their own account.

"That's another important feature about our system that the university liked. Universities struggle to get their students to give something back down the road when they become successful. Slippery Rock is trying to build that thinking in their students. The Slippery Rock Foundation will be listed as the first charity they can donate to. Students will at least see the concept of giving back."

A new player in the campus card market?

Mr. Welsch hopes Slippery Rock is just the beginning for Heartland in the campus card business. "We're looking at doing this at other universities. It will be a product offering under our campus card product line" in the company's micro-payments division. The company, which is traded on the New York Stock Exchange, provides credit/debit/prepaid card processing, payroll and payment services to 150,000 merchants – including restaurants, hotels, and retailers – and 300 colleges throughout the US.

What will determine whether Slippery Rock University's card program is successful or not? "We're going to judge it by the number of merchants we sign up. Obviously we also want to sell them credit/debit, and payroll processing – as well as remote check deposit services," said Mr. Welsch. "We will judge the success of this project on the merchant participation and the future of selling or renting additional readers to the university."

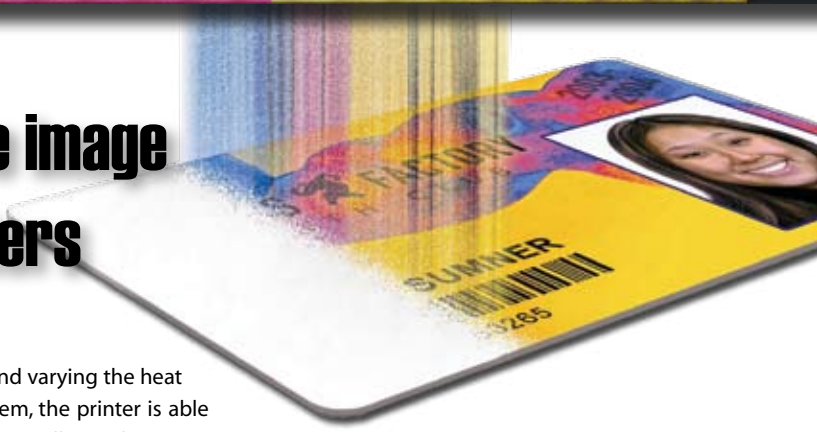
Dr. Smith likes what he's seen so far. In fact, he has been a guinea pig, of sorts. "They gave me one (a contactless tag), and I've gone around using it. Since it was Heartland's money on an experimental card, I had a great time," he laughed.

"We're going to see where this goes," he added, "but from a branding standpoint, we couldn't be more thrilled. Heartland is out there encouraging all these retail establishments to accept these Rock Dollars, and the merchants are signing up. That means they're looking for a Slippery Rock patron."

He said the contactless tag concept has also created "quite an international buzz. This kind of reputation for us is, to borrow the MasterCard line, 'priceless.'" ID

Sponsored by: FARGO

Choosing between reverse image and direct to card ID printers



When shopping for an ID card printer, you're liable at the outset to be hit with two choices: direct-to-card or reverse image transfer? Making an informed choice depends on what kind and how many cards you're trying to print.

Direct-to-card (DTC) printing is the most common technology used in desktop ID systems to print images directly onto the surface of a plastic card. It does this by heating a special print ribbon beneath a thermal printhead, resulting in the transfer of color from the ribbon to a blank card.

With reverse image technology, the printer first prints images onto a special film that is then fused into the surface of a blank card through heat and pressure. Because the graphics and text are printed on the underside of the film, the image is "sandwiched" between the film and the card. This process produces excellent print quality, is durable, and provides the ability to print with a wide variety of card technologies and on many card types.

Both of these printing technologies share two printing methods: dye-sublimation and resin thermal transfer.

Dye-sublimation is the process used to print smooth, continuous-tones that bear photographic-like realism. This process uses a dye-based ribbon that is partitioned by a number of consecutive color panels. The panels are grouped in a repeating series of colors – cyan, magenta, yellow, and black (CMYK) – along the length of the ribbon. During printing, a printhead containing hundreds of thermal elements heats the dyes on the ribbon that vaporize and diffuse into the surface of either the card or the film. A separate pass is made for each of the different color panels. By combining the colors and varying the heat used to transfer them, the printer is able to produce up to 16.7 million colors.

Resin thermal transfer uses a single-color ribbon to print sharp black text and crisp barcodes that can be read by both infrared and visible-light scanners. This process uses the same thermal printhead as dye-sublimation; however solid dots of color are transferred rather than a combination of colors.

When you're printing contact or contactless smart cards, the "printing technology of choice" is reverse transfer, says Fargo's Steve Blake, vice president of product marketing.

Why? Smart cards have embedded chips. "Anything with electronics embedded in the card doesn't always end up with a flat surface. A dye sub process … creates some issues (with print quality). By printing to reverse transfer film instead of the card surface itself, you have none of those problems. It's very forgiving with electronic cards," said Mr. Blake.

The dye sublimation process is also known as direct-to-card printing. As Mr. Blake explained it: the ribbon comes in direct contact with the card. "If you have a contact chip in a smart card, that chip is supposed to be flush to the card, but that's not always the case. There might be a little ridge or bump and if the printhead contacts the chip on the card, it can blow a pixel out (on the printhead)." Then you have the costly problem of a damaged printhead that, in many cases, costs about half (or more) of the printer's original purchase price to replace.

What's more, a DTC printer can leave blotchy white spaces around the chip. You therefore end up with a bad card that you "have to throw away. That might be a $4 card so you're damaging an expensive inventory item," he said.

Reverse imaging technology "really doesn't care whether the card is smooth or not because the printhead is contacting the ribbon which contacts the film. The film is then attached to the card in a single pass through the printer," said Mr. Blake. "The film can produce a much better image – the colors are truer, you have a higher resolution and a crisper, cleaner, truer look. It resembles a preprinted card that you get from a card manufacturing plant."

Reverse imaging also makes it easier to produce secure cards equipped with a hologram. "Historically, holograms had to be put on by a lamination module attached to the printer," explained Mr. Blake.

But reverse transfer film can be produced with an embedded holographic image. "You don't need a laminator module. This is wonderful news for the middle and entry level (organization)."

"With smart card growth, people are telling us more and more that they want that high definition printing technology, but at an affordable price," Mr. Blake said. Reverse image has become the technology of choice for both its superior image quality and its ability to print high-quality images on contact and contactless smart cards. In most cases, these printers cost more than their direct-to-card counterparts, though many printer professionals suggest that reductions in the total cost of ownership outweighs the additional upfront costs.

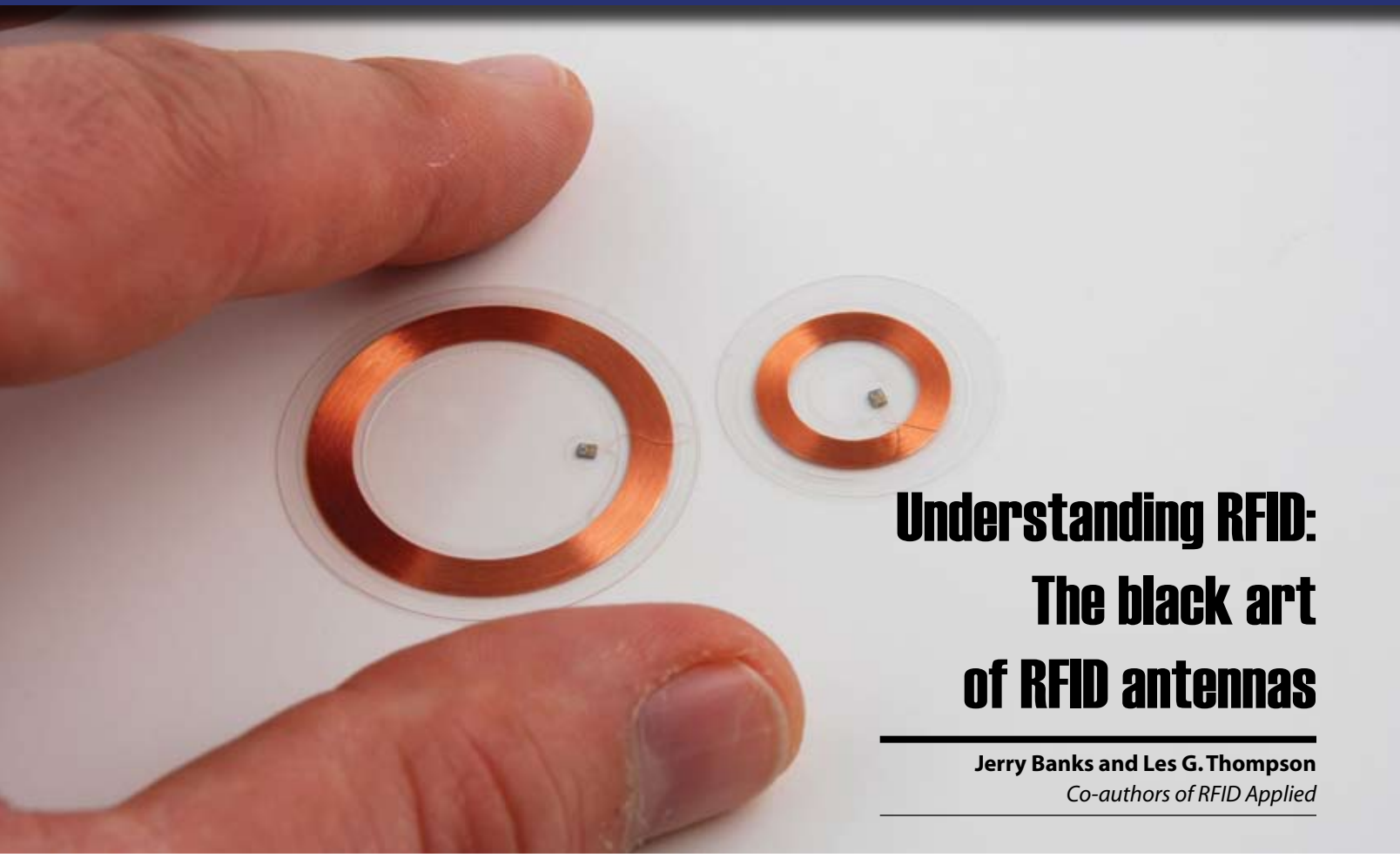
Improving Campus Life

Campus Card Systems · Access Control and Integrated Security Solutions · Web-based Ordering
Housing Assignment Systems ·Judicial Conduct Tracking · Food Service Management Tools
Catering and Event Management Systems

On-campus, off-campus, and in the palm of your hand, CBORD is improving campus life for those you serve and employ.

Visit www.cbord.com to learn more.

The CBORD Group, Inc.
61 Brown Road · Ithaca, NY 14850 · TEL: 607.257.2410 · FAX: 607.257.1902
www.cbord.com



Understanding RFID: The black art of RFID antennas

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

The design of the antennas used by RFID tags and RFID readers is one of the most critical pieces in RFID infrastructure. This is because the antennas facilitate the communication between an RFID reader and a tag through free space. Both the reader and the tag utilize an antenna to transmit and receive data. In the case of passive RFID systems, the antennas have the added burden of being able to efficiently collect and radiate energy, respectively. Without well-designed antennas there can be no efficient communication between the tags and readers, and, in the case of passive tags, there may not be enough energy to power the tag.

Characteristics of antennas

Most antennas are made of a highly conductive material such as copper so it is sensitive to electrical and/or magnetic currents found in radio waves. When an antenna is receiving, the conductive material comes in contact with radio waves and converts the radio wave's electrical and/or magnetic currents into signals and energy that can be consumed by some type of circuit. The opposite is true for a transmitting antenna.

In most cases, antennas possess a property called reciprocity. This means that if an antenna can transmit well at a certain frequency, it can receive equally well at the same frequency.

Most antennas are tuned to operate within a certain bandwidth. This means that the properties of the antenna, such as construction materials, length, and structure, are all precisely chosen to work efficiently in a specified, usually very narrow, range of frequencies. The frequency at which the antenna works best is known as its resonant frequency. When an antenna works well at multiple frequencies, the antenna is said to have harmonic resonance. In most cases, antennas that are designed to work at multiple frequencies are not as efficient as antennas that are designed to work in a very specific frequency spectrum.

As discussed, the construction material of an antenna enables the antenna to convert electric and/or magnetic currents into usable forms of energy. The two components of electromagnetic radiation are the electric component, E field, and the magnetic component, H field. Based on an antenna's design, it will make use of one of these components.

Near field vs. far field antennas

RFID tags that operate within one wavelength's distance from the reader's antenna make use of the magnetic component. If an antenna is

SEPTEMBER 11-12, 2007 • JACOB JAVITS CONVENTION CENTER • NEW YORK, NY

ISC EAST 2007

ISC® EXPO

INTERNATIONAL SECURITY CONFERENCE & EXPOSITION

The most important names in security will be here. Be among them.

SECURITY IS THE ISSUE. NEW YORK IS THE CITY. THIS IS THE SHOW.

Let the best in the industry SHOW you the best in the industry. Come to learn. Come to network. The most respected leaders in security will be at **ISC East 2007** to discuss all the newest and most relevant technologies, products and strategies to secure your business, including:

- Access Control
- Alarms & Monitoring
- Biometrics
- CCTV
- Fire Control
- Remote Monitoring
- Systems Integration
- Wireless Applications
- and more...

Plus, special NEW features covering today's most current topics:

Urban Security - Hundreds of solutions specifically for securing and safeguarding large populations and property.

SmartHome@ISC - Home automation is hot! Connect with designers of the products that are part of a fully connected and automated residence.

Infosecurity New York - ISC East will once again be held alongside Infosecurity New York, the largest IT-security event in the East. With the growing convergence of IT and physical security, you'll have access to the products and companies that bring it all together.

SECURE YOUR PLACE. REGISTER FOR FREE AT **www.isceast.com/ID**

CODE: AD21

SPONSORED BY: SIA

CORPORATE SPONSORS: DSC, HID, Honeywell, VERINT

PRODUCED BY: Reed Exhibitions

ENDORSED BY: NBFAA

International Security Conference East® is a registered trademark of Reed Elsevier Properties Inc., used under license. ©2007 Reed Elsevier Inc.

designed to operate at 13.56 MHz, its antenna should be designed to operate in the "near field" and utilize the magnetic component. This is because the wavelength of a 13.56 MHz wave is approximately 22 meters. This is not to say that the tag will function at a distance of 22 meters. It won't. The tag's antenna would not be able to derive enough energy from the electromagnetic field at that range. It is important to recognize that the wavelength of the target frequency directly influences how the tag's antenna is constructed.

Any RFID tag that is designed to operate at 13.56 MHz will function best in the near field and will most likely have an antenna that is shaped like a coil. A coil antenna configuration works best for making use of the magnetic component of electromagnetic radiation.

It is important to note that the wavelength of a radio wave is inversely proportional to its frequency. Thus, a radio wave with a frequency of 13.56 MHz will have a wavelength (approximately 22 meters) that is much longer than that of a radio wave with a frequency of 915 MHz (approximately 32.8 centimeters). The wavelength of any radio wave at a certain frequency can be calculated by the equation $\lambda = c/f$, where λ is the wavelength and c is the speed of light in meters per second.

Far field antennas operate most efficiently outside of one wavelength's distance of its target frequency. Far field antennas are usually manufactured as straight lines as opposed to coils because far field antennas utilize the electric component of the electromagnetic radiation. The most common type of far field antenna is the half-wavelength dipole antenna. The half-wavelength dipole consists of two antennas, with each antenna being a quarter of the target frequency's wavelength. Most RFID tags place the tag's processor between both antennas. Based on the previous example, a half-wavelength dipole antenna that is designed for the 915 MHz spectrum would require each dipole to have a length of 8.2 centimeters which is one quarter of the 32.8 centimeter wavelength. This antenna would be 16.4 centimeters in total length.

The principle of gain

An antenna's gain is a key characteristic for RF engineers. Gain refers to the radiation pattern of an antenna. Low gain antennas radiate their energy equally in all directions, while a high gain antenna is direction biased.

High gain antennas have a strong direction and a weak direction. Gain is a very important factor in RFID systems because it allows system designers to "shape" RFID coverage areas. Antennas can be arranged in a portal style configuration where they are directionally biased toward the inside of the portal. Passive systems benefit from this type configuration because the reader's antennas can concentrate most of their energy on the location where the tag is most likely to be; thus providing more energy to power a tag as it passes through the portal.

Active tag systems benefit from gain as well. In a real-time location system (RTLS), a directional antenna allows system designers to tweak their coverage areas and strictly define the boundaries of the "zone" to be covered by an antenna and reader. If an RTLS zone, for example, is defined by the RF layout designer to only cover a single room, the engineers can use the antenna's gain characteristic as one of the tools to make sure that the antenna does not read tags beyond the borders of the room.

Enhancing performance through antenna design

There are two basic rules for designing a passive tag antenna. First, the longer the antenna, the more energy it can collect. There is a point of diminishing returns with regards to the length of the antenna, but for the most part, longer is better. With respect to coil type antennas, increasing the number of rings of the coil is equivalent to increasing the length of the antenna.

The second antenna characteristic that is beneficial to collecting energy is the surface area of the antenna. As the width and height of the antenna increases so does its energy collecting efficiency. As discussed earlier, the layout of the antenna depends on how the tag is intended to be used and at which frequency it will operate. Tags that operate at lower frequencies and work in the near field have antennas that are coils. The higher frequency tags that work in the far field have straight-edge antennas.

RFID tags are very rarely placed on stationary items. There is usually no point in tracking something that does not move unless you want to make sure it does not move! RFID tags tend to move regularly and may be placed in many different orientations as the object they are attached to is shipped, carted or carried. The laws of physics dictate that an antenna will achieve its best reception when its element is oriented orthogonally to the radio wave. This means that the antenna works best when it intercepts the wave at a 90 degree angle; orientation is crucial, therefore, if a tag is to achieve its maximum range and transmission data rate capabilities.

Passive RFID tag antennas sometimes look strange because they may be offset at abrupt angles. These angles allow the tag to present some part of its antenna to the radio wave at an angle most conducive to coupling. The half-dipole antenna mentioned earlier is extremely efficient when its orientation is correct, but can be completely useless when it is not. Dipole antennas should only be used in applications where the antenna's orientation can be ensured, so this is why many RFID antennas are "squiggle" type.

Active tag antennas

Most of this discussion has focused on passive RFID technology, but it is important not to forget about the active RFID world as it has its own set of antenna challenges. Active tag antennas do not have the added burden of collecting energy from radio waves to power the tag because the active tag's battery provides all the power required. This additional power gives active tags some flexibility on how the antenna is constructed. The laws of physics have not changed, but the ability to blast a signal at a relatively high wattage when compared to passive tags can nullify many of the primary design considerations associated with passive tag antennas.

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

RFID in the airline industry:
Bad news at the baggage carousel is good news for RFID

David Wyld
Contributing Editor, AVISIAN Publications

A recent research report from ABI Research projected that the overall systems revenue for RFID in the area of airline baggage handling will grow from $11.8 million in 2006 to an estimated $27.5 million in 2011, representing a compound annual growth rate of over 18%. From the perspective of Lorne Riley of the IATA: "It's reaching the tipping point. The business case itself is relatively strong." The business case is so strong precisely because luggage handling is proving to be an "Achille's Heel" in their customer service equation.

Professors Brent D. Bowen of the University of Nebraska at Omaha and Dean E. Headley of Wichita State University, leading academic analysts covering the American airline industry, recently released their 2007 Airline Quality Rating Report (AQR). For sixteen consecutive years, these professors have taken monthly Department of Transportation (DOT) data and analyzed all domestic US airlines annually for performance on four key customer service metrics:

- On-Time Arrivals
- Denied Boardings
- Mishandled Baggage
- Customer Complaints (including flight problems, reservations, fares, refunds, disabled passenger issues, animal handling, etc.)

The Airline Quality Rating score is based on a formula combining these four measures. Based on the 2006 data, the best-rated US airlines were Hawaiian, JetBlue and AirTran, while the worst rated were three regional carriers – Comair, American Eagle and Atlantic Southeast. Overall, AQR scores for the industry have declined significantly over the past five years, and worsening baggage handling statistics are a major reason why. In fact, US airlines performed considerably worse in successfully delivering checked luggage in 2006 than in the previous year, losing almost a half a bag more per thousand passengers.

Surveys have consistently shown that misdirected, delayed and lost baggage is a major headache for both the airlines and their passengers. Tales of airline customer service are often intensely personal ("I'll never fly XYZ Airlines again, after they lost my bags for five days with all my skiing clothes and ruined my Colorado vacation!"). While they are anecdotal in nature, they quite often grow in magnitude as they are passed along, both in person and today, via blogs and email. Sometimes though, baggage woes are systemic, as was the case with the 2004 "Christmas nightmare," when US Airways baggage systems were overwhelmed with holiday traffic and weather. Quite literally mounds and mounds of misrouted baggage – over 10,000 pieces – accumulated at the carrier's Philadelphia hub and were broadcast over and over and over again on news outlets. After the 2006 air terror scare, when the US Transport Security Administration put in new restrictions on carry-on liquid items, more and more flyers have elected to check their bags rather than deal with the new security procedures at airport checkpoints. This means that today, US airlines are handling anywhere from 10-20% more checked bags than in prior years, further exacerbating their baggage handling problems.

While the business case is there, the question remains as to whose business baggage transport really is? There is no question that there are multiple stakeholders in the need to successfully identify, track and ultimately deliver checked baggage. Not only do air carriers and passengers have a stake in having better and more secure baggage tracking, but so do airports and public safety officials (and, by extension, society and the economy as a whole). Also, as airlines baggage problems have worsened, they have spilled over to affect other travel-related businesses, including cruise lines, hotels and rail lines, which depend on successful delivery of both passengers and their luggage to their sites for successful enjoyment/delivery of their services. Passenger doubts about the airlines' abilities to deliver their luggage have led to increased business opportunities for companies such as FedEx and UPS, along with a number of rapidly growing third-party service providers who employ shipping companies to assure "door-to-door" delivery of air travelers' luggage – for a fee.

Indeed, aside from an early trial by Delta in 2004 and pilots abroad (Air-France-KLM and Asiana), the majority of the focus on RFID to date has been on the part of airports seeking to differentiate themselves through better baggage service, most notably the highly publicized installations at Las Vegas' McCarran International Airport and at the Hong Kong International Airport. According to the analyst firm IDTechEX, as of early this year, twenty-four airports around the world are either conducting trials of RFID baggage tracking systems or putting such installations in place. Airports are increasingly competing to become gateways for both passengers and air carriers, and they see smart baggage tracking systems as a way to distinguish their airports from a service and cost perspective.

Airlines now have the ability to seriously consider piloting and implementing RFID-based luggage tracking, given the recovery of the industry as a whole. Such systems may be a key-differentiating factor for airlines to reverse their poor customer service. Indeed, in local markets where RFID-based baggage systems are trialed, either alone or in conjunction with an airport partner, the piloting carrier can market the fact that such service is unique to the market. And, the first carrier that makes the leap to a system-wide RFID implementation will likely enjoy a significant first-mover advantage in this competitive marketplace, giving them a benefit to tout to customers and enabling them to differentiate their airline through improved service rather than price in what has been an intensely fare-conscious traveling public.

However, RFID-based systems do have significant cost benefits as well, as the ability to more accurately route and track baggage will enable airlines to significantly reduce their expenditures compensating passengers for delayed, misdirected and lost baggage, while reducing the labor needed to manually intervene in the baggage handling process to read tags and correctly load baggage on the proper flights. Additionally, airlines and their passengers will see significantly fewer flight delays caused by the need to reconcile passengers and their checked luggage – as RFID-based systems could quickly locate a specific bag of a non-boarding passenger in the cargo hold of an aircraft, rather than what is today a process that can cause delays of an hour or more as bags are manually inspected in aircraft cargo holds to find one or two suspect pieces of luggage – bags that could indeed represent terrorist threats.

While US airlines do have significant capital expenditures on the horizon in terms of fleet replacement and refurbishment to meet the needs of today's business and leisure travelers, it is unlikely that any investment could pay greater financial and customer satisfaction/loyalty dividends than shifting to RFID-based luggage tracking, especially in light of the global IATA standards that are in place. Even with competing needs for resources, it is time for airline executives to tackle head-on their intractable problem of baggage handling by implementing RFID technology.

One technology

connecting

multi applications?

Ask us!

Looking for the Missing Link?

RFID and smart card technologies are moving ahead as fast as the world we live in. And ASSA ABLOY Identification Technologies (ITG) is leading the way to connect one application with another – with smart technologies. Supporting our customers with an optimized mix of components and technologies for converged ID and security solutions. For maximum convenience. One partner for all your integration challenges: **ITG**

ITG

ASSA ABLOY

www.aaitg.com

An ASSA ABLOY Group brand

HIGH DEFINITION PRINTING™ IS NOW AFFORDABLE

©2007 Fargo Electronics, Inc.

Introducing the HDP5000 Card Printer.
Starting at under $4,000.

For the best image quality and reliability available,
see the HDP® difference at www.fargo.com/hdp

For more information call 800-327-4694 or e-mail us at sales@fargo.com

FARGO®
Part of HID Global HID