re:ID

Spring 2010

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

NEXT GEN PACS

Is cryptography the future of physical access control?

Plus:

Feds launch "uses" for FIPS 201 IDs

Easy come, easy go for Miami transit

A business case for NFC?

Physical access systems are undergoing the most radical transformation since the switch from keys to cards and tumblers to electronics. Because physical access control systems typically have a lifespan of 10 years, this won't happen overnight, but industry visionaries agree that it will happen. Leading the charge for these next generation systems is the U.S. federal government. PKI is typically associated with logical access and digitally signing documents. When it was proposed for physical access it was something of a first. Making the leap wasn't that difficult though, says Bill MacGregor, a computer scientist at the National Institute of Standards and Technology. There were simply too many points of potential vulnerability with existing physical access systems. The cardholder 's unique ID number is stored on the contactless portion of the card through the Federal Bridge. And it forms the core of the trust model for the PIV credential. While using PKI for physical access control might be new, the technology is not. That it's been around for some time and there are standards around it means not having to reinvent the wheel. But there are still serious questions, including how long it takes to process a transaction and how it will affect existing physical access control infrastructures. In a PKI at the door implementation, as in traditional access control systems, the first thing that will happen is registration into the system. At this point in the FIPS 201 environment, the contact interface of the credential will be used to check the PKI certificate, PIN and fingerprint biometric template stored on the card. This process currently takes between 13 and 30 seconds and will have to be performed whenever the credential is to be used in another physical access system. For example, a State Department employee going to a Homeland Security office will need to have his credential registered into the system before it can be used. After that initial registration the cardholder can use the contactless interface to have the PIV authentication key, one of the four PKI certificate on the card, checked. This process, along with the usual challenge and response that takes place with contactless smart card transactions, currently takes one to three seconds. First, however, the existing infrastructure for most physical access systems would have to be upgraded. Typical access control systems use the Weigand protocol to communicate with controllers. Weigand is a one way communication. But for PKI to work there needs to be a back and forth with the system. Current systems are designed to send an ID number and not much more. But if you want to do authentication you need bi-directional protocols which you get with a network. PKI at the door will require Internet Protocol-based access control devices. Putting physical access control systems online raises security concerns to some, but just because you IP-enable a system doesn't mean it's available via open networks. The physical access readers and controllers will also have to undergo a makeover with PKI at the door.

PKI AT THE DOOR

There will be two choices for the architecture of new physical access systems: do the processing of PKI certificates at the reader or do it at the controller. Either way the processor on the device that is chosen will need additional cryptographic certification. Most likely the choice will be to go with a smart controller instead of a smart reader. The argument is that there's too much risk in putting the intelligence on the unsecure side of the wall. While upgrading the infrastructure for physical access control systems will be time consuming and costly, a bigger concern with PKI at the door is how long the transaction will take. Experts say it could take as long as a second and a half to open a door. This may not seem excessive but imagine trying to get through a turnstile with hundreds of other employees in the morning. Some fear that transaction duration could be the deal breaker in many environments. Others disagree. It's the difference between wave and go and touch and go. It does require some crowd behavior effort, but just as people learned how to get on and off an escalator they'll learn how the system works. To deal with the time issue some are suggesting a switch from PKI, or asymmetric keys, to a symmetric key scheme. People say that symmetric keys are faster than PKI at the door. But PKI is more secure and may actually be easier to deploy and manage than symmetric keys. With PKI the secret is stored on the card and it never leaves that card. There is a public certificate on the physical access control system but it's not a secret. It's widely distributed and there is no security vulnerability. With symmetric keys the same certificate stored on the card also has to be stored on the physical access control system. This leads to more complex key management than with PKI. Public keys don't need to be protected, but all these symmetric keys need to find their way to a reader on a door and must be protected in transit, in use and at the reader. This results in far more vulnerable situations and more opportunities for system compromise. Symmetric key management can be expensive and complex, especially when dealing with something the size of the federal government. A fact of large scale use is that key management drives the cost. It's expensive. While symmetric keys may bring a speed advantage the complexity of key management may be too much of a detractor. The General Services Administration has been pursing an expedited PKI at the door solution. The agency contracted with Exostar, a provider of collaboration solutions for the aerospace and defense manufacturers and their 40,000 supply chain partners and CertiPath, a credentialing authority for aviation, aerospace and defense organizations. The concept demonstrates how a single-credential system can provide secure access for both physical and logical assets, while also providing interoperability for employees, customers and partners. The need for the system arose for the greater security needed for federal physical access control systems. The system demonstrates the ability to perform the challenge response to the card authentication key on the contactless portion, but also how the system works with the contact portion including use of the biometrics and PIN. Additionally, it addresses ways to handle guests with and without PIV credentials. A visitor with a trusted credential can use it to pre-register via a Web site for a remote visit request. Upon arrival at the site the card has already been verified and after checking in the visitor can gain access to protected areas. Guests that do not have a trusted credential check in at an attended area and are issued a credential with an operational biometric and PKI certificate stored on the card. Now every defined population is using PKI for physical access control. HID Global is working to improve the speed of PKI at the door via caching. The company's caching status controller checks the certificate on the card once and then conducts

PHYSICAL SECURITY

periodic checks back to the revocation list to make sure the certificate is still valid. Initially the cardholder taps the badge on a reader and the PKI certificate on the card is checked against the Federal Bridge, a process that takes a couple seconds. From that point forward, the certificate is checked against the stored cache that is updated every hour against the Federal Bridge. In essence, at set time intervals the system validates the certificates from all cards commonly used in that specific access control environment. When a card is presented at an access reader, it need only be validated against the local cache, a process that is much quicker than validating against the remote system. You're extending the Federal Bridge right out to the door. Then you get virtually the same card performance as you do with a standard transparent reader and you're going with a smart, very secure edge appliance to do it. ID Technology Partners has created a solution for physical access control called Mutual Registration PIV, or MR-PIV, that speeds up transactions and potentially makes them more secure. The solution enables a credential holder to register the card in the local physical access control system and also register that system with the card. That way if anyone tries to sniff information off the card and the system doesn't have that

CRYPTOGRAPHY

mutual registration the card won't give up any information. Also, since it's a local identifier and not the global identifier the process is quicker. Rather than register the global identifier of the card we register the local identifier and a key to the physical access control system. This mutual registration speeds up the transaction to around half a second. The throughput is a five or six times performance increase. While it seems clear that PKI at the door is coming, not as clear is the role that biometrics will play with these new systems. Biometric authentication is the single best way to truly tie the credential to the holder. Biometrics are an intrinsic property of the owner. It adds to the high assurance and the non-transferability of the credential. This will become increasingly important as other weaknesses in physical access control systems are alleviated. In a PIV card system the contact interface of the card contains two fingerprint templates that can be used to confirm identity. These would be used to register into a new physical access control system. However, since the contactless interface doesn't have access to these templates, it would be difficult to use the biometric anywhere that high throughput is necessary. When a biometric authentication is required, would depend on the security policy of the particular agency. They wouldn't have to be used by credential holders on a daily basis. While general consensus seems to be that PKI at the door is the future for physical access control there are still challenges. One of the biggest maybe convincing those on the IT side and those on the physical security side to cooperate. But change is happening as the industry works to make it easier for the authorized to gain entry and make it more difficult for unauthorized

AVISIAN

CoreStreet®
An ActivIdentity Company

We Make Credentials Work

CoreStreet PIVMAN Solution for TWIC Compliance

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

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

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

No network connections. Just grab a handheld and go!

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

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

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

Contents

20
Cover Story
Is cryptography the future of physical access control?

36
Transit
Miami-Dade proves setting up contactless fare collection system is easy

42
NFC
Breaking down the business cases for NFC

48
Payments
Colorado town leading the way with contactless payments, rewards

54
Mobile
Tokens becoming more popular on mobile devices

6 | OPINION | The rumors of PKI's death have been greatly exaggerated

7 | OPINION | Physical access control readies for its great leap forward

8 | PODCAST | Conversations on the European eID and Mexican ID programs as well as the U.S.'s health ID initiatives

Spring 2010

INDEX OF ADVERTISERS

Blackboard 57
www.blackboard.com/contactless

CoreStreet 2
www.corestreet.com/TWIC

CPI Card Group 37
www.cpicardgroup.com

CSC 31
www.csc.com

CSCIP 45
www.smartcardalliance.org

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

Entrust 3
www.entrust.com/epassport

Evolis 23
www.evolis.com

Gemalto 67
www.gemalto.com/enterprise/smartguardian

HID Global 68
www.hidglobal.com/reliability/REID

IEEE 39
www.IEEEBiometricsCertification.org

ISC West 55
www.iscwest.com/reID

Kaba 35
www.kabaaccess.com

LaserCard 27
www.lasercard.com

Sargent 41
www.sargentlock.com

Smart Card Alliance Annual Conference 65
www.smartcardalliance.org

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

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

20 | COVER STORY | Is cryptography the future of physical access control?

21 | GOVERNMENT | Predictions for the pending revision to FIPS 201

25 | INNOVATION | Beyond convergence and PKI: Fusion

26 | BIOMETRICS | The biometric problem in physical access

28 | PHYSICAL SECURITY | Next generation PACS

32 | GOVERNMENT | ICAM: A roadmap for PIV applications

34 | INITIATIVES | 2010: When ideas become reality?

36 | TRANSIT | Miami-Dade proves setting up contactless fare collection system is easy

40 | BIOMETRICS | Fingerprint scanners on mobile devices enable apps

40 | NATIONAL ID | Mexico deploying multi-modal biometric ID

42 | NFC | Breaking down the business cases for NFC

44 | NFC | Risks & Benefits for NFC business case options

47 | INNOVATION | NFCNews at GSMA Mobile World Congress

48 | PAYMENTS | Colorado town leading the way with contactless payments, rewards

51 | DRIVER LICENSES | 3D photo technology for secure driver licenses

52 | AUTHENTICATION | Problems with some two-factor authentication

54 | MOBILE | Tokens becoming more popular on mobile devices

58 | INNOVATION | Will your next card include a display, a battery, a button?

59 | TRENDS | Biometrics and payment card security on tap for 2010

60 | INNOVATION | Sesames winners announced

63 | ISSUANCE | Applications being added to ID cards demand more from printing software and hardware

66 | APPLICATIONS | NFC enables communication from beyond the grave

Perspective

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

EDITOR
Zack Martin, zack@AVISIAN.com

ASSOCIATE EDITOR
Andy Williams, andy@AVISIAN.com

CONTRIBUTING EDITORS
Daniel Butler, Ryan Clary, Liset Cruz, Seamus Egan, Autumn Giusti, Meredith Gonsalves, Ross Mathis, Ed McKinley, David Wyld

ART DIRECTION TEAM
Darius Barnes, Ryan Kline

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

SUBSCRIPTIONS
Regarding ID is available for the annual rate of $39 for U.S. addresses and $87 for non-U.S. addresses. Visit *www.regardingID.com* for subscription information. No subscription agency is authorized to solicit or take orders for subscriptions. To manage an existing subscription or address, visit http://subscriptions.avisian.com and enter the Customer Code printed on your mailing label. Postmaster: Send address changes to AVISIAN Inc., 315 E. Georgia Street, Tallahassee, Florida 32301.

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

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

The rumors of PKI's death have been greatly exaggerated

Zack Martin
Editor, AVISIAN Publications

I'm a bit of a geek so when I think of next-generation physical access control I imagine a system that would recognize my body temperature, iris, face, fingerprint, and vein pattern all at once. This is the system I want on the front door of my house. I wouldn't even have to slow down to fumble for keys while carrying in groceries.

Sadly, we're not going to live my science fiction dream yet, but advances are being made. Most people won't notice the change. They will still present an ID to a reader to gain access. More users may be presenting biometrics, most likely fingerprint though iris is a possibility too.

But it is behind the scenes, where things will be very different.

The federal government is suggesting, and soon possibly mandating, that agencies use public key infrastructure at the door for secure access to facilities.

Why PKI? Because the consensus is that it can't be hacked. In an industry where consensus is an uncommon event, that alone is significant. Moreover, it provides a way to verify a credential's authenticity and ensure it has not been revoked across interoperating systems.

Our cover story explores the next generation of physical access systems. This concept of PKI at the door is truly fascinating. Especially since people seem to sound the death knell for PKI every other year.

When I first started covering the industry I remember talking to an editor who described PKI as "expensive and complex" and that was for logical access systems. He didn't think it would last. But now you can't talk to anyone in ID without PKI being brought up.

It hasn't been easy getting to this point. The U.S. Defense Department blazed a trail for PKI and the Common Access Card had its share of misadventures but without that experience the industry wouldn't be where it is now.

And if you talk about an advanced credential and you don't mention PKI and digital signatures many people will say there are significant pieces missing. It's not enough to be using smart cards and biometrics … ID issuers need to digitally sign all that information so it can be verified later.

So with PKI at the door around the corner it has to be just a matter of time until I get my full-body biometrics scanner, right?

Physical access control readies for its great leap forward

Security through obscurity and availability failed, but security through cryptography can 'fix' physical access control

Chris Corum
Executive Editor, AVISIAN Publications

At Re:ID, we try to listen to the early buzz and dig into a topic that is *about* to be hot in the identity space. I am particularly pleased to see this cover story take shape, because it addresses one of my longtime beliefs: that the card reader on the door is less a security feature than a convenience feature.

In fact, I argue that the switch from physical keys to card-based access control has been a zero sum gain in regards to security. We may have advanced the ability, or likelihood, that a lost key is disabled within a system, but we have actually made it easier to create fraudulent keys.

Let's segment access control media into three phases:

Previous generation media centered almost exclusively on physical metal keys.

Current generation media includes bar codes, magnetic stripes, proximity cards, and even some smart cards – specifically those that do not rely on cryptographic checks for access transactions. These could include contact or contactless cards that use only the unsecured card serial number as the identifier.

Next generation media are microprocessor-based credentials that can come in a variety of form factors, from contact or contactless smart cards to mobile phones, wristwatches and more. The key to this new media is its ability to cryptographically "participate" in access transactions.

The previous generation of media, metal keys, relied on *security through availability*. Because it took a trained locksmith with dedicated hardware and special "blanks" to produce a duplicate key, the ability to make fake media was not readily available.

Current generation media continued to rely on *security through availability*. In the early days, blank card stock was hard to obtain, card printers were expensive and sold through dedicated channels, mag stripe encoding was a separate issuance process and prox card stock and equipment were hard to find. In this world, *security through availability* worked fairly well.

But availability can no longer be a security approach in a world where card printers encode mag stripes and prox cards inline, blank card stock is a commodity and both are available for purchase on Craigslist or eBay.

Security through availability simply does not work. Enter *security through obscurity*.

The concept of *security through obscurity* is that a system can be secured by hiding components of its design and thus its vulnerabilities. If the bad guys don't know how it works, they can't uncover weaknesses. This approach to security, however, has fared little better than prior attempts at security through availability. The problem with obscurity is that it is an all or nothing method. Once the secret is exposed, it is easily shared and security is compromised across the board.

When I think of *security through obscurity*, the old mag stripe prepaid systems come to mind. Photocopy cards and vending cards on college campuses were big in the 80s and 90s. The value was not stored in an account but rather was actually written to the mag stripe and deducted with each transaction. The systems used proprietary data formats to encode the value making it "hard" to rewrite data and give yourself free money. These systems also positioned magnetic read/write heads at an angle to make it difficult for off-the-shelf hardware to interact with the cards. These "secrets" kept the systems secure … at least as long as they remained secret.

To many, the hack of the Mifare Classic security architecture two-years ago was another example of the dangers of *security through obscurity*. Critics cited a relatively weak cryptographic implementation obscured by layered secrets. When the layers were peeled away – both literally and figuratively – so too was the chip's security.

Security through obscurity doesn't cut it any more than *security through availability*. Most experts agree that the only true protections come from *security through design*, or what I prefer to call *security through cryptography*.

So we circle back to why I am excited about this cover story. Physical access control is on the verge of taking a great leap forward toward true security. Adding public key cryptography and advanced cryptographic design enables things never before possible.

- We can finally achieve interoperability of credentials across systems in a way that doesn't dilute core physical security principles such as immediate revocation.
- We can virtually eliminate counterfeit or cloned credentials.
- We can protect the integrity and privacy of personal data held on the credential.

Enjoy the issue and get ready for the great leap forward.

ID

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

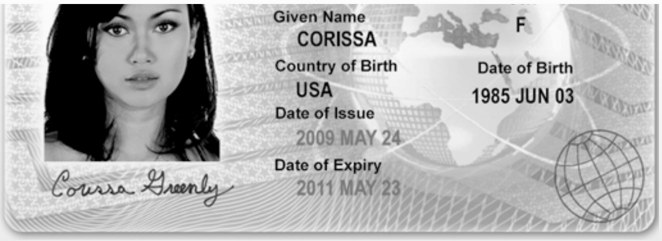
Episode 42: What's ahead for ID & the government?

2009 was when the discussion started on the problems with identity in the federal government. Will 2010 be the year where solutions to these problems come to light? Regarding ID Editor Zack Martin spoke to Kelli Emerick, executive director of the Secure ID Coalition, to see what might happen in the coming year with different ID projects.

Highlights: "The recognition that identity management is critical to the Obama administration agenda is starting to come through. 2010 is the year you will see some of those areas bear fruit."

"You'll start to see many of the policies for these programs develop in the next year and the implementation will happen over the next couple of years. The good news is the Obama 2010 budget recognizes that using information technology solutions to improve government requires security and privacy protection for everyone."

To listen, visit SecureIDNews.com/tag/Podcasts and select "Episode 42"



Episode 45: The European eID landscape

Many European countries are starting to issue electronic IDs to citizens with mixed results. Frost & Sullivan Analyst Yiru Zhong talks about the different initiatives with Regarding ID Editor Zack Martin.

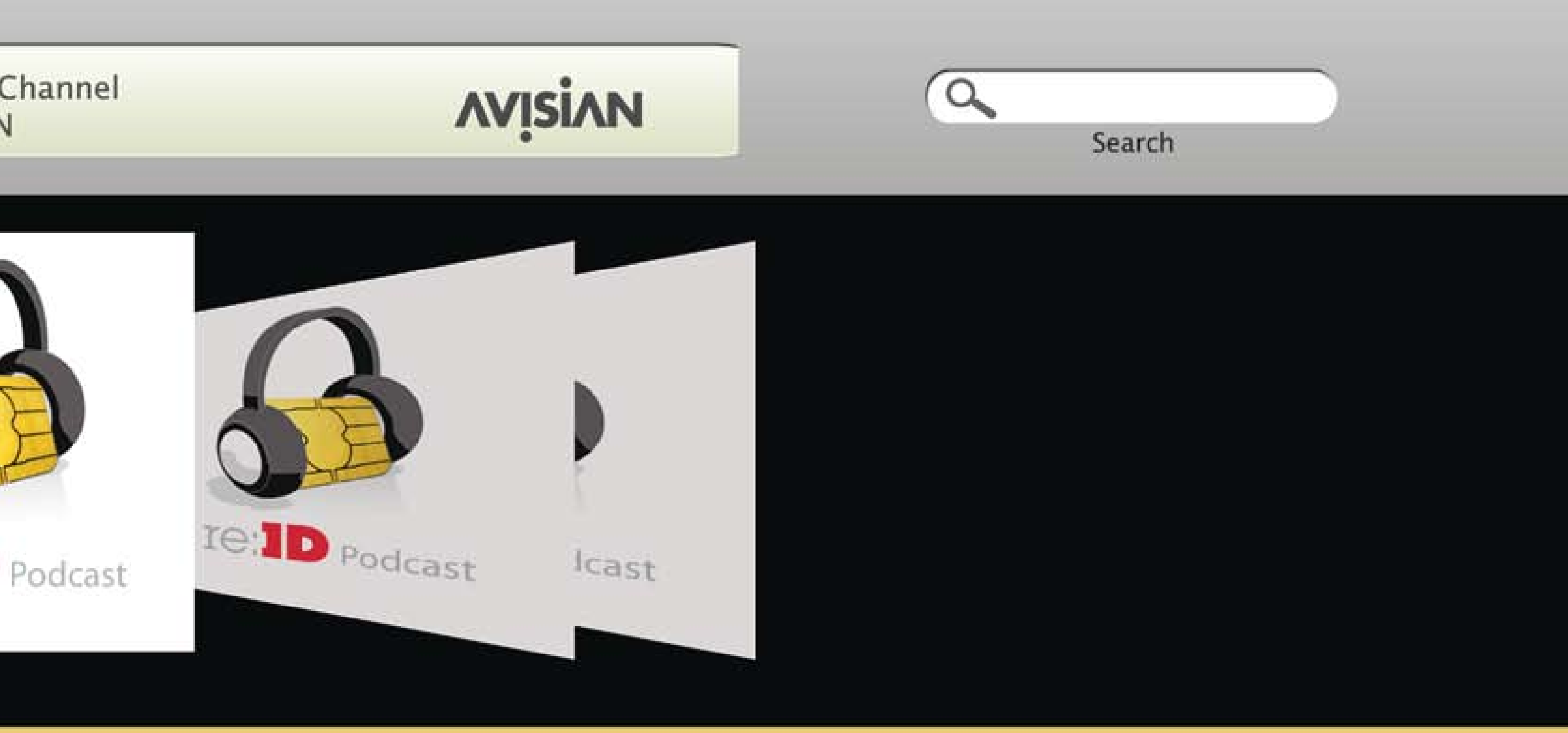
Highlights: "eIDs are creating a lot of interest in Europe. Italy and Spain have already rolled out eIDs and have had varying degrees of adoption.

"Spain is more successful in terms of (issuance) because it's compulsory and by end of 2008 a third of the population had an eID. Ten million have been issued to date.

"It's not compulsory in Italy and have only seen 1.5 million issued."

"We had hoped for 2009 to see rollouts from Germany and France but it didn't happen."

To listen, visit SecureIDNews.com/tag/Podcasts and select "Episode 45"



Episode 46: Mexico's national ID card

Within the next six months Mexico will start enrolling up to 110 million citizens in its multi-modal biometric ID card system. Regarding ID Editor Zack Martin spoke with Terry Hartmann, vice president of identity solutions at Unisys, about the program and why it's groundbreaking.

Highlights: "It's essentially the first national identity system in the works that will capture iris and use it.

"The Mexican government wants to improve the ability of the government to uniquely identify citizens to provide them services."

What technology will the ID use? "There's a very good chance it will be a smart card because they will want to use biometrics for identity verification."

Are more countries looking at national ID systems? "It's mainly in the countries that don't have a national ID or don't have a biometrics because they recognize the problems with identity fraud."

To listen, visit SecureIDNews.com/tag/Podcasts and select "Episode 46"

Episode 47: Health ID initiatives

Health care is not only a hot political topic but also one of great interest in the identification industry. How patients and caregivers will be identified is a discussion that is taking place all over the country. Regarding ID Editor Zack Martin talks with Randy Vanderhoof executive director of the Smart Card Alliance, about the organization's health care initiatives in 2010.

Highlights: "Our council is really concerned that the innovation being driven by stimulus fund and the high tech act is racing toward a set of recommendations and solutions … that don't actually recognize how we're going to identify patients with electronic medical records."

Will the health care industry use PIV or PIV-I? "The biggest challenge the health care industry has to face is how do we come up with a way to identify tens of millions of people and health practitioners in a way that meets requirements … the government spent four years developing a set of standards and policies and operational systems to deal with its identity management system that were covered under HSPD-12."

To listen, visit HealthIDNews.com/tag/Podcasts and select "Episode 47"

EMV hack may be overstated

Researchers at the University of Cambridge in the UK released a report claiming to have identified vulnerabilities with the EMV payment scheme. Industry organizations are meanwhile defending the technology, saying the hack would be difficult to pull off in the real world.

The attack uses a fake chip card connected with wires to custom electronics, a computer with specially designed software, and a stolen EMV chip & PIN card. The fake card and equipment sit between the stolen card and the point-of-sale terminal; the attack fools the terminal into thinking that the correct PIN had been presented and makes the stolen card believe that no PIN was required.

The Smart Card Alliance has reviewed the hack along with other industry organizations and concluded that widespread implementation of this attack is unlikely and that there is no evidence that the attack described has happened in the real world.

These conclusions are supported by the following points:

- The attack requires the use of a stolen EMV card that has not yet been reported as stolen; this limits the scalability of this type of fraud since it must be done with one card at a time and in a potentially short window of time.
- The combination fake card and stolen chip & PIN card cannot be used in an ATM for a cash withdrawal, as ATMs rely on an online PIN verification.
- The fraud requires using a fake chip card with wires coming out of it, running up the sleeve of the fraudster and connecting to a hidden circuit board, computer and stolen EMV card, making detection likely at an attended merchant point-of-sale.
- The attack is technically difficult requiring highly sophisticated software and customized hardware that could only be created by individuals with extensive knowledge of EMV protocols.
- Countermeasures are already available, either in EMV, within payment system products and networks, or within issuer host systems.
- Electronic audits of data from suspected transactions would protect cardholders and merchants from responsibility for fraudulent charges made to their card with this type of attack, if reported properly.

Additionally, such an attack would not compromise the smart card as the PIN would still remain secure inside the card.

State bill bans biometric ID cards

The New Hampshire Legislature is considering a bill that, if passed into a law, would ban the use of biometric data on ID cards issued privately or by the government with exception granted only to employee ID cards, according to press reports.

The bill was formed out of fears surrounding the leak or theft of an individual's irreversible personal data, but groups have come out against the bill citing the ID management benefits behind the use of biometrics.

Among the groups coming out against the bill is the Security Industry Association (SIA). Aside from requesting the state halt a vote before conducting a study on the benefits of the technology, SIA believes there is a misunderstanding regarding the privacy safeguards that have already been put into place with most of the technology available to placate the exact worries the bill intends to.

Another group that has come out against the bill, International Biometric Industry Association (IBIA), has pointed towards its inappropriateness citing the many examples of useful applications of the technology to protect citizens.

Local bank secured with VASCO DIGIPASS

VASCO DIGIPASS is being used to secure employee and cash management at Virginia Heritage Bank, a community bank in Northern Virginia. The bank is using VASCO solutions to improve security for both employees and customers.

The VASCO DIGIPASS Pack for Remote Authentication has already deployed to more than 100 employees at Virginia Heritage Bank, providing each with secure remote access to company networks. The DIGIPASS Pack confirms the identity of all users logging into corporate networks with two-factor authentication technology.

Gemalto introduces World Traveler program for U.S. banks

Gemalto has introduced the World Traveler program, which includes a globally accepted dual interface EMV payment microprocessor card and complete issuance service for U.S. banks and card issuers.

EMV is a global standard for chip card payment managed by Visa, MasterCard, American Express and JCB. The Gemalto EMV based World Traveler card contains a microprocessor which provides global acceptance and a more secure payment technology in the same convenient form factor as other payment cards.

With most countries around the world moving to EMV based payment for greater security, U.S. travelers are increasingly having trouble using magnetic stripe bank cards abroad, especially in offline applications like unattended ticketing/payment kiosks.

Gemalto's new World Traveler program enables any U.S. issuer to provide cards to their customers in less than two months. The card program provides U.S. banks and card issuers with a complete portfolio of service offerings including return on investment and technical consulting to ensure a quick and easy introduction of this product to their top tier customers.

The portfolio leverages Gemalto's global footprint and expertise in payment products to provide full card design and production, personalization data preparation and personalization of EMV dynamic data authorization contact and contactless dual interface cards ensuring global acceptance and forward compatibility for both online and offline payment transactions.

Gemalto will provide banking cards containing its secure digital technology for EMV payments, as well as a magnetic stripe for paying in the United States. By providing encryption for the payment transaction, the World Traveler card ensures global acceptance for both online and offline transactions while significantly reducing the risk of payment card fraud and identity theft for cardholders.

Rwanda goes with De La Rue for eID

De La Rue Identity Systems, a provider of secure e-government identity solutions, announced that it will design and roll-out East Africa's first national eID project for the Government of Rwanda.

The plans for systems integration, to combine data from the current ID card, passport and driver license, are already underway. The first eID documents will be distributed later this year, following completion of the pilot.

Rwanda's existing national ID card, also produced by De La Rue, is held by all citizens over the age of 16. It is envisaged the new eID card will replace this and contain additional e-government information, such as health and social security details.

Juniper: mobile ticketing set to take off by 2014

Juniper Research published a report predicting "massive growth" for mobile ticketing by 2014, according to Mobile Marketing Watch. The report states that some 15 billion mobile tickets will be in use by 2014, compared to the current mark of 2 million.

As of now, the Far East and China regions are leading the way in mobile ticketing, but Juniper predicts that Western Europe will take the lead by 2014, due to advancements in device integration.

The report also predicts that in the next few years mobile ticketing will break out of the transportation industry and into entertainment, with cinema chains, sports teams and major concert venues offering the new technology.

Juniper cites NFC technology as the main catalyst for the predicted growth because it significantly reduces the steps between purchasing the ticket and receiving it. According to Juniper, once more devices in the west are integrated with NFC, we'll see mobile ticketing go mainstream.

atsec certifies Codebench for FIPS 201

atsec information security, a laboratory for the GSA FIPS 201 Evaluation Program which runs a product approval program for PIV-related products, announced the successful evaluation of four Codebench products. Codebench is the first company with solutions evaluated for GSA product categories Caching Status Proxy, PIV Authentication System, and CHUID Authentication System.

Codebench's PIVCheck Plus Desktop Edition with PIVCheck Certificate Manager, PIVCheck Plus Mobile Edition with PIVCheck Certificate Manager and PIVCheck Desktop Edition (both the SCVP Client and PIV Authentication System) were tested and evaluated in atsec's Austin, Texas lab.

As a result of its evaluation, atsec has determined that Codebench's products meet FIPS 201 requirements on behalf of GSA, who ultimately grants the approval.

These products are now listed on the FIPS 201 Evaluation program Approved Product List, which only lists those products and services that are in compliance with the current version of the standard and its supporting NIST Special Publication 800-116, which provides recommendations for the Use of PIV credentials in physical access control systems.

LaserCard unveils new standards-compliant IDs

LaserCard Corporation launched its newest generation of multi-technology credentials compliant with key North American and European identity program standards. The cards enable governments to meet the demanding requirements of both North American registered border crossing and European foreign resident card programs.

For the North American market, LaserCard has introduced a Western Hemisphere Travel Initiative (WHTI) compliant credential incorporating a Gen 2 UHF RFID tag in combination with LaserCard's optical security media.

Governments worldwide are increasingly calling for powerful multi-purpose ID credentials that will cost-effectively maintain the highest levels of security while addressing secondary objectives related to more rapid processing, facility access control and e-government services. In this WHTI-compliant card, the RFID facilitates the processing of individuals at busy land border crossings, while the tamperproof optical security media provides visual and physical security countermeasures against counterfeiting and fraud.

LaserCard has also introduced an optical security media-based credential that is compliant with European Union Regulations defining Community-wide uniform standards for Foreign Resident Permit credentials. Manufacturing processes enable the combination of an ICAO-compliant chip, mandated by EU standards, with optical security media, which is formally approved within the standards as a supplementary "national security feature."

For those European nations that incorporate an optional contact chip for e-government applications into their foreign resident permits, LaserCard offers either a finished card or chip-ready card stock suitable for chip embedding by a third party.

These new standards-compliant credentials are the result of LaserCard's manufacturing techniques to combine optical security media with the most commonly used machine-readable technologies. Technology inclusiveness of this kind ensures compatibility with widely installed infrastructures while capitalizing on the optical media for essential secure visual and physical identification plus tamperproof portable data storage.

Gemalto acquires Valimo Wireless

Gemalto announced that it has acquired Finnish mobile authentication systems provider Valimo Wireless Oy. Valimo's technology enables mobile phone users to digitally sign documents and confirm legally binding transactions by entering a self-chosen passphrase or a PIN code. Valimo Mobile ID solution provides secure online banking, mobile payments, governmental services, electronic and mobile commerce and identity and access rights management for enterprise applications.

According to Gemalto, Valimo has pioneered the use of two-channel, two-factor authentication based on Public Key Infrastructure, combining an over the air platform with a software client in the SIM to generate a legally binding electronic signature, any time, any place.

Olivier Piou, Chief Executive Officer, Gemalto, commented: "Mobile digital signature has been on the horizon for a few years and we believe that we have now reached a tipping point. Enabling people to conveniently sign legally-valid transactions is opening up a whole range of new applications for the mobile, at the service of citizens".

Kentucky awards L-1 driver license contract

L-1 Identity Solutions was awarded a contract by the Commonwealth of Kentucky to provide a secure driver license solution with facial recognition biometrics as part of the Kentucky Transportation Cabinet's effort to protect the public and prevent fraud.

The contract with L-1 includes a base three-year term valued at approximately $11.1 million and three additional two-year extension options that bring the total contract value to approximately $33.7 million.

Kentucky uses an over-the-counter system for secure driver license issuance that includes fraud prevention processes such as photo image capture and enrollment. The state also uses facial recognition technology designed, developed and maintained by L-1 to prevent persons from establishing duplicate identities.

Carrefour goes with Hypercom for contactless EMV terminals

Global retail giant, Carrefour, will deploy Hypercom's Wynid server-based payment solution and more than 12,000 EMV contactless readers at 210 of its French hypermarkets, as well as at all of Carrefour's petrol stations in France.

The Carrefour Group is the largest retailer in Europe, and the second largest worldwide, with more than 15,000 stores under banner in 33 countries and more than 490,000 employees.

The multi-million dollar agreement is believed to represent one of the world's largest deployments of EMV contactless readers.

Streetcar App now online

Streetcar announced its new app for iPhone and iPod touch is available from the iTunes App Store. The Streetcar App enables users across the UK to locate, book and open a car using their iPhone or iPod touch coupled with smart card technology.

Users can unlock the rentals using either their iPhone or iPod touch, or a remotely activated smart card. Once the customer is finished with the car, he or she can return it to a dedicated Streetcar parking space.

Independent research conducted by Transport for London shows that each car club vehicle on the road replaces an average of 26 privately owned cars. Each rental car has an average of 40 users and, of those, over half chose not to buy (or replace) a car when they join the club. Streetcar has already taken approximately 20,000 privately owned cars off the UK's streets and is aiming to prevent the emission of around 50,000 tons of CO2 over the next two years.

SCM's small, portable smart card reader GSA approved

SCM Microsystems announced that its thumb-sizedSmartFold smart card reader has been approved by the General Service Administration for use by U.S. government agencies and employees.

The SCR3500 SmartFold is ideal for mobile government employees that have notebooks without integrated card readers. The tiny, foldable and portable contact smart card reader will fit on an employee's key ring or in their pocket. When unfolded and inserted into a free USB port of a notebook, the employee can insert their PIV or CAC card into the reader to enable secure access to government systems and data.

The SCR3500 SmartFold is now on the GSA Approved Products List which means the reader is compliant with all FIPS 201 and PIV/CAC card requirements, and is ready for purchase by government agencies and/or their purchasing agents.

idOnDemand releases Software as a Service PIV smart card

idOnDemand introduces the a new PIV full lifecycle employee smart card using the Software as a Service approach. With an idOnDemand SmartID, customers can compile visual, physical and logical authentication into a secure digital identification card using a pay-as-you go model that eliminates complex infrastructure.

The software consolidates credentials that are traditionally separate like building access cards, VPN tokens, usernames and passwords onto a single card that can be used to protect corporate information, wherever that information may reside.

The card features a secure SAS-70 global identity environment utilizing a hardware-based PKI infrastructure that enables global businesses to manage their employee smart cards from any authorized location.

ID SHORTS

MorphoTrak algorithm ranked first by NIST

MorphoTrak announced that the company's matching algorithm for biometric systems provided by Sagem Sécurité earned the top ranking form the National Institute of Standards and Technology following a test for latent fingerprint accuracy by the organization. The test compared searches for features such as minutiae and extended feature sets that were manually marked by examiners.

UK's Stansted Airport deploys biometric e-passport gates

Stansted Airport has rolled out its new facial recognition security gates, which use document scanning from 3M.

Passengers with new biometric e-passports travelling to the UK via Stansted can use the Autogates that scan their face and check their passport photo in seconds.

The Autogates use the 3M RTE8000 Full Page Scanner to validate British or European e-passports with an electronic chip and are helping the UK Border Agency process passengers more efficiently.

A live image of the passenger standing at the gate is captured and biometric technology then compares this with the image stored on the chip embedded within the document by measuring specific facial points. If there is a match and they clear security, the automatic gates allow the traveler across the border.

Stansted Airport handles around 23 million passengers annually. The trial at Stansted is being run in partnership between the UK Border Agency and airport operator, BAA.

Following the trial, the UK Border Agency is expecting to roll-out Autogate systems to 10 additional UK airport terminals as part of the new £1.2 billion e-Borders system helping the UK Border Agency target terrorist suspects, known criminals and would-be illegal immigrants.

Colorado county sheriff gets iris identification technology

The Arapahoe County Sheriff's Office in Colorado has unveiled new identification technology that is expected to replace fingerprint-based identification with iris-based identification, according to media reports. Arapahoe is the first county in Colorado to receive the technology, which was paid for thanks to a $10,000 National Sheriff's Association grant.

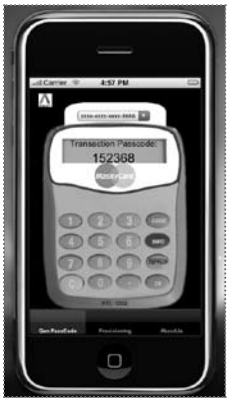
The new system will be utilized for more than checking and registering criminals' identifications. It also will be used for The Children's Identification and Location Database (CHILD) project and Senior Safety Net as well.

Both the CHILD project and the Senior Safety Net utilize voluntary registration to help lost children or senior citizens with memory loss or dementia find their caretakers.

Smart Card technology for wine tasters

A new joint venture between Napa Technology Partners and Vintry Wine and Whiskey employs the use of a smart card for wine tasters. The WineStation holds up to four bottles in a temperature-controlled dispensing and preservation system. After inserting a smart card, customers can sample the wines of their choice. The hospitality, entertainment and food service industries are utilizing the WineStation as a new way to serve, preserve and increase sales of their wines.

Arcot extends MasterCard's authentication service to mobile phones



Arcot, a leader in fraud prevention technology, announced an EMV authentication solution for MasterCard holders. ArcotOTP is a mobile application designed to lower the cost of providing EMV authentication and increase convenience for cardholders on the go.

ArcotOTP uses the Chip Authentication Program in its application that enables cardholders to authenticate themselves using existing EMV banking cards and a personal card reader. The Chip Authentication Program utilizes part of the transaction data in generation of the password, resulting in a unique signature for each transaction.

In addition to increased security for the cardholder, the ArcotOTP application gives customers the ability to make banking transactions from their mobile phone no matter where they are in the world.

HID releases Dutch-compliant smart card reader

HID Global announced the launch of its Rijkspas-compliant iCLASS smart card reader designed for Dutch government agencies adopting MIFARE DESFire EV1 smart card technology.

Protecting data transfer between the credential and reader as required by the Rijkspas specification, it enables government entities to utilize their existing card population while migrating to the new Dutch Rijkspas.

Offering a range of mounting methods and accessories with support of both MIFARE Classic and HID Prox, the reader is capable of reading legacy cards and the new Rijkspas cards. The new reader is built on HID's iCLASS architecture and enables numerous output configurations to address migration challenges.

Field upgradeable using reader firmware cards, Rijkspas-compliant iCLASS readers have the option to be re-configured to support additional or substitute applications including traditional iCLASS credentials.

VITAband keeps your medical information on your wrist

VITAband has developed a medical ID bracelet that aims to bring improvement to health information exchange and patient care.

It stores personal health information that enables first responders and medical professionals to gain access to important information in the event of an emergency. The device stores a person's identification, any relevant medical history and emergency contacts.

VITAband has partnered with Microsoft HealthVault to enable users to collect and store their health information in one location. Users can create their own HealthVault account or use a preexisting one to import their Emergency Response Profile to the VITAband wristband.

VITAband can also double as a contactless payment device. Using a prepaid contactless payment technology users simply wave their wrist at the point of sale to make a purchase.

LaserCard to produce ID cards for Hungarian government

After winning the contract from Hungary's Public Transportation, LaserCard announced that initial deliveries of the International Certification Card have begun. LaserCard is supplying Hungary's professional drivers with an optical security card containing facial imagery, biometrics and demographic information.

In an effort to more efficiently secure its borders, the Hungarian government will issue the IDs to bus drivers, truck drivers, ship captains and airline pilots who operate Hungarian registered commercial vehicles internationally.

Israeli airport introduces biometric security system

UNI-PASS, a self-check digital security system developed by Israel's Airport Authority, has been deployed at Ben Gurion Airport near the city of Lod.

The security system utilizes biometrics in issuing a smart card to passengers traveling abroad. Passenger screening requires travelers to swipe their smart card at each security checkpoint and is said to speed up the security process as whole. In addition the IAA said the system creates an identical screening process for each and every flyer.

UNI-PASS replaces the standard question-answer method currently practiced at airports, an IAA spokeswoman tells the Jerusalem Post.

Currently UNI-PASS is being tested with El Al Frequent Flyers Club members.

Gemalto buys XIRING's banking group for $29 million

Gemalto and XIRING announced the acquisition by Gemalto of XIRING's banking activity for more than $20 million.

The purchase focuses on XIRING's EMV-based strong authentication solutions for e-banking and e-commerce. The company has more than 12 million of these readers already deployed in Europe.

The contract includes the transfer of the technical and commercial team and all the associated products, IP and technologies. The transaction has no impact on XIRING's activities outside of the banking arena.

Wyckoff Heights Medical Center deploys smart card patient IDs

SMART Association announced that New York's Wyckoff Heights Medical Center is slated to issue more than 110,000 smart cards to patients.

Over the next two years, patients will be issued the smart card carrying individual demographic information and important medical information such as medical conditions, allergies and medications.

Patients will be able to have their information read at the admissions department and emergency department, easing the admissions process. All information stored on the card is encrypted within the smart card chip.

ActivIdentity buys CoreStreet for $20 million

Strong authentication and credential management provider, ActivIdentity, announced its acquisition of CoreStreet, a leading provider of distributed identity credential validation solutions.

The $20 million acquisition is intended to support ActivIdentity's vision of making every digital interaction trustworthy by adding distributed identity credential validation solutions and physical access control products to the company's portfolio of strong authentication and credential management offerings.

CoreStreet's PKI certificate validation technology is deployed by public and private organizations around the world to validate the credentials of individuals as they interact with their secure IT applications, including digitally signed email and secure forms. Additionally, CoreStreet's PIVMAN system enables authorized personnel the ability to control access to any site with confidence by quickly authenticating and validating the roles and identities of individuals wishing to enter an area.

Anakam to upgrade Equifax I-Card

Anakam was chosen to provide its two-factor authentication solution to the Equifax I-Card initiative. This service will make the Equifax I-Card the first of its kind to contain Level 3 authentication security.

Anakam's two-factor authentication uses different channels to offer a variety of solutions for the secure authentication of users and customers. The company leverages voice biometrics over existing devices such as cell phones and traditional phones to deliver a secure, one-time pass code that confirms that the person possessing the device is the one attempting to access the systems.

Since 2008 the Equifax I-Card has been assisting consumers and businesses conduct online transactions or verify identity.

American University pilots SmarTrip ID card

Students and faculty at American University are piloting student ID cards compatible with the Washington D.C. Metro's SmarTrip contactless fare collection and ticketing system.

At the beginning of the year, twenty student IDs were produced with SmarTrip functionality. The cards were distributed to a combination of students and staff for testing.

Student Government President, Andy MacCraken, stated the biggest challenge in making the campus cards compatible with SmarTrip readers was the card's technology. SmarTrip relies on a proprietary contactless smart card technology from transit provider Cubic.

If all goes well and the test is successful, the entire American University community may one day have the option to combine their student ID and SmarTrip card.

Mississippi rolls out driver license kiosks

L-1 Identity Solutions introduced new automated kiosks for processing driver license renewals and replacements in Mississippi. With more than half of all license transactions relating to replacements and renewals, the self-service kiosks are designed to streamline Department of Motor Vehicle operations and offer the public a faster and more convenient alternative to waiting in line for agents.

The first two L-1 kiosks will be made available to the public at Mississippi Department of Public Safety (DPS) headquarters in Jackson, Miss. Six additional kiosks will roll out by the end of the month across state public safety offices with additional kiosks expected to be installed in 2010.

Customers use a touch screen menu and are led through a series of prompts to securely enter personal information that will be used to locate their record in the DMV system. The kiosk then takes a photo and performs a one-to-one facial recognition match against the existing photos in the DMV database to verify the identity.

Once the identity details are confirmed, the consumer's credit or debit payment is processed on the kiosk using a card swipe. If the state uses an over-the-counter issuance system, the kiosk dispenses a bar coded receipt that can be exchanged at the express window of the DMV office for the new card. For states using central issuance, the kiosk produces an interim document/receipt for use until the secure card is received in the mail.

The unit does not retain any personal information. Data collected is transmitted via a secure encrypted line from the kiosk workstation to the DMV host server and database system where it is stored and managed by the State. Photos taken at the kiosk are purged from the machines after they are taken and transmitted to the central image server.

Homeland Security behind on PIV issuance

The U.S. Department of Homeland Security is behind on PIV issuance, according to an inspector general's report. Only 7% of Homeland Security employees have been issued the credentials, just 15,567 out of 250,000.

The deadline for PIV issuance was October 2008, and although agencies throughout government are behind, the inspector general's report takes Homeland Security to task. The vast majority of credentials have been issued to employees at Homeland Security's headquarters, with 11,875 issued. But Customs and Border Protection, the Transportation Security Administration and Immigration and Customs Enforcement have issued only 22 credentials between the three agencies.

"Due to weak program management, including insufficient funding and resources, and a change in its implementation strategy, the department is well behind the deadline for fully implementing an effective HSPD-12 program," the report states. "In addition, the department faces significant challenges in meeting HSPD-12 directive requirements for logical access to its information systems. Furthermore, system security and account management controls are not effective in protecting personally identifiable information collected and stored from unauthorized access. Existing security issues must be addressed to allow for the deployment of a robust, efficient, and secure interoperable identity card and issuance system department-wide."

The report makes 15 recommendations for the agency to make in order to get credential issuance on track, including:

- Ensure that the program management office has the staffing and funding necessary to effectively coordinate and oversee the department-wide implementation of HSPD-12.
- Develop a regional implementation plan that includes detailed information about how the program management office will centrally manage the department-wide deployment of its HSPD-12 program.
- Discuss and coordinate with OMB on the department's updated milestones and implementation of HSPD-12 requirements.
- Estimate the department-wide cost to comply with HSPD-12 and FIPS 201-1 requirements and prioritize the department's costs to ensure that physical and logical access interoperability requirements will be met.
- Identify the facility access points and information systems that will require the use of PIV cards.

FedExField deploying biometric credentials

Telos Identity Management Solutions, LLC has delivered the MobileAssure Access Control system to credential and verify the identities of employees and contractors at FedExField, home of the Washington Redskins.

Employees will use fingerprint scanner for verification. The system is also capable of integrating with HR management, scheduling and payroll systems.

The MobileAssure Access Control system is capable of using simple matching or multimodal biometrics, and its verification software can operate on mobile or even handheld verification devices.

The Telos system is scalable and capable of exchanging data with multiple human resources management, scheduling and payroll systems, helping staff scheduling, time and attendance reporting and reconciliation, and payroll processing. Telos ID's MAAC solution has enrolled over 7,500 FedExField employees and contractors, creating a credential for each.

MorphoTrak buys tattoo matching technology

MorphoTrak acquired the tattoo matching technology, developed by Michigan State University, that enables corrections and law enforcement community to more accurately and efficiently search tattoo image databases to identify suspects, criminals and victims.

This content-based image retrieval and matching technology uses features such as color, shape, and texture present in tattoo images instead of labels or keywords, to compute the similarity between images.

According to a 2006 Pew Research Center survey, more than 36% of individuals between the ages of 18-40 have at least one tattoo. This proportion is much higher among criminals and members of criminal gangs.

Consequently, federal, state and local law enforcement agencies have been collecting images of tattoos for years. Although a tattoo alone cannot identify a person, this alternative trait provides valuable information that can help narrow the field and identify gang members.

A typical tattoo search today involves matching a text description of the tattoo. This makes the process slow and inaccurate. With image-based tattoo matching, agencies will now have the ability to more fully exploit their large repositories of tattoo images for the identification of suspects and victims. Tattoos are particularly important for criminal identification as they often contain subtle clues to a suspect's background and history, such as gang membership, previous criminal convictions, claims of criminal activity and number of years spent in jail.

CenTrak RTLS ensures caregivers keep hands clean

In hospital environments, RFID-based real time location systems (RTLS) are often used for tracking equipment, patients and staff. But now RTLS provider, CenTrak, is making a move to promote cleanliness with the release of its new hand hygiene compliance system.

Battery powered monitors can be mounted to any dispenser, canister, pump, or sink to track usage. The system automatically captures a caregiver's badge ID upon entry and exit from patient care areas along with hand hygiene events, based on specific hospital compliance regulations.

The dispenser's monitor communicates each event to the network to record each caregiver's compliance performance. Data is stored on CenTrak's local or hosted server and can be accessed by compliance management and reporting solutions.

The system can be deployed standalone or in combination with a full scale CenTrak system and the dispenser monitors have a battery life of five-years, eliminating the need for in-room wiring and enabling quick and easy installation.

Deciphering the German airport hack

The original German news report stating that physical access control systems at some of the country's airports were compromised may have been overstated. The system, however, is vulnerable to attacks similar to the original Mifare hack in 2008.

More recent reports suggest that hackers did not actually gain access to restricted airport areas, as originally reported. Instead they talked about how it may be possible to gain access to the areas. Also, EU regulations state that airports must have multi-factor security in place and it takes more than a badge to gain access to airside areas.

In December the Chaos Computer Club announced the vulnerability with the Legic Prime contactless system used at some German airports. Legic began offering a more advanced and secure contactless solution called Legic advant in 2003 but the airport location is still operating the older generation product.

Chaos Computer Cub member Karsten Nohl stated that cracking the older Prime technology was not much of an issue. However tapping into Prime communications requires some specialized equipment, including a Proxmark3 type RFID test device, an oscilloscope and a mathematical logic analysis method. Simulating a card also demands more software, a special emulator and IT knowledge.

Since the attack was released Legic's has been telling users to add another factor of security, such as PIN video monitoring or biometrics, to the system. The company also states that many airports have already begun the migration to the advant system. "Prime uses a fixed encryption method which reflects the technical capabilities of contactless transponder technologies at the time the product was launched in 1992," says Klaus U. Klosa, Legic Identsystems Ltd's CEO. "Such methods are based on keeping the algorithms which are used secret. Currently popular methods are based on open algorithms and secret keys. Compared with current methods, older methods are scrutinized more intensively."

Hagen Zumpe, editor-in-chief of PROTECTOR, says there is a need to put things into context: "I'm surprised that the Prime technology, which came onto the market in 1992, is still used in many high-security applications. For over five years now, Legic has been supplying its successor technology, Legic advant, which is secure up to AES levels which is currently state of the art."

Updating the system at the Hamburg airport would require replacing 15,000 cards.

The attack is reminiscent of the '08 announcement by Nohl and others that the security of the original Mifare contactless technology was compromised. Similarly, the technology was still widely used though newer more secure versions had been released to the market years before.

New York Red Bulls to implement contactless smart cards at new stadium

Major League Soccer's New York Red Bulls are set to implement a contactless smart ticketing system at the team's new stadium.

The new system will allow season ticket holders to load cash for use in concessions and purchasing within the stadium onto the contactless smart cards via the team's Web site. The cards will also be used to gain entrance to the stadium.

The cards will expedite concession purchases inside the stadium.

The Red Bulls, who are expected to move into their new stadium in March, will be the first U.S. soccer club to implement contactless technology. Several clubs in England's Premier League, including Arsenal and Manchester City, have already introduced similar systems.

Nokia nixes plans for NFC-enabled 6216

Nokia has canceled plans to issue 6216 classic handsets with built-in NFC technology. The mobile device would have been Nokia's first to have the NFC element on the SIM card, Single Wire Protocol, rather than a trusted element in the phone. Nokia had planned to launch the device in the third quarter 2009.

Most NFC devices thus far have relied on the trusted element in the phone but mobile carriers want to start using the Single Wire Protocol. News reports stated that the consumer experience using the protocol was not where it needed to be, thus the cancellation.

Nokia hasn't stated when it will release a mobile device with Single Wire Protocol but says the decision regarding the 6216 doesn't signal a change in its support for NFC.

Aside from Nokia, China Unicom has announced plans to introduce an Single Wire Protocol-equipped NFC service in the next six months, putting them in competition with China Mobile's RF SIM system.

N.J. now motivated to recycle thanks to RFID

Burlington, New Jersey residents have another reason to recycle thanks to RFID systems integrator, Aviant Systems, and RecycleBank.

The new program attempts to motivate people to recycle by rewarding them with points that can be redeemed at participating local and national retail outlets.

The Burlington recycling trucks are equipped with an on-board RFID solution that collects data at each pick-up location. The automated arm that lifts and empties recycling containers is equipped with an RFID reader to read the tag on the container and record data to the on-board database. Information is automatically transmitted to data processing centers via a T-Mobile cellular network.

Aloft Hotels, no check-in required

Starwood Hotels & Resorts announced a Smart Check-In program at its Aloft Hotels that enables guests to skip the front desk at check-in and head directly to their rooms.

Guests who opt to participate are issued an enhanced Starwood Preferred Guest / Aloft-branded RFID keycard to be used for room access. On the day of a planned arrival, a text message is sent to the guest's mobile phone with their room's number.

The program will allow hotels to eliminate the routine task of issuing room keys and allow them to focus on the guests' overall experience rather than the transaction. The pilot program is currently being tested at the Aloft hotel in Lexington, Mass.

2010

MARCH

ISC West 2010 Conference and Exhibition
March 23 – 26, 2010
Sands Expo and Convention Center
Las Vegas, NV

APRIL

RFID Journal LIVE! 2010
April 14 – 16, 2010
Orange Country Convention Center
Orlando, FL

ASIS Intl European Security Conference
April 18 – 21, 2010
Lisbon Congress Center
Lisbon, Portugal

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

Expo Seguridad México
April 20 – 22, 2010
Banamex Center, Hall B & C
Mexico City, Mexico

MAY

IFSEC 2010
May 10 – 13, 2010
NEC Birmingham
Birmingham, UK

Near Field Communications World Europe
May 11 – 13, 2010
London, UK

MAY *(Continued)*

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

SEPTEMBER

2010 Biometric Consortium Conference
September 21 - 23, 2010
Tampa Convention Center
Tampa, FL

OCTOBER

ASIS International 2010
October 12 - 15, 2010
Dallas, Texas

NOVEMBER

Sixth Symposium and Exhibition on ICAO MRTDs, Biometrics and Security
November 1 - 4, 2010
ICAO Headquarters
Montréal, Canada

ISC East 2010
November 3 – 4, 2010
Jacob Javits Convention Center
New York, NY

DECEMBER

CARTES & IDentification
December 7 - 9, 2010
Paris-Nord Villepinte Exhibition Center
Paris, France

for physical access control might be new, the technology is not. That it's bee
and there are standards around it means not having to reinvent the wheel. But there
including how long it takes to process a transaction and how it will affect existing
infrastructures. In a PKI at the door implementation, as in traditional access control syst
happen is registration into the system. At this point in the FIPS 201 environment, the contact i
be used to check the PKI certificate, PIN and fingerprint biometric template stored on t
takes between 13 and 30 seconds and will have to be performed whenever the credential is to be
system. For example, a State Department employee going to a Homeland Security office will need
into the system before it can be used. After that initial registration the cardholder can use the contactle
authentication key, one of the four PKI certificate on the card, checked. This process, along with the usual challenge a
contactless smart card transactions, currently takes one to three seconds. First, however, the existing infrastructure for most ph
be upgraded. Typical access control systems use the Weigand protocol to communicate with controllers. Weigand is a one way communication. Bu
back and forth with the system. Current systems are designed to send an ID number and not much more. But if you want to do authentication you
you get with a network. PKI at the door will require Internet Protocol-based access control devices. Putting physical access control systems online
just because you IP-enable a system doesn't mean it's available via open networks. The physical access readers and controllers will also have to und

PKI AT THE DO

There will be two choices for the architecture of new physical access systems: do the processing of PKI certificates at the reader or do it at the co
the device that is chosen will need additional cryptographic certification. Most likely the choice will be to go with a smart controller instead of a
there's too much risk in putting the intelligence on the unsecure side of the wall. While upgrading the infrastructure for physical access control sy
costly, a bigger concern with PKI at the door is how long the transaction will take. Experts say it could take as long as a second and a half to
excessive but imagine trying to get through a turnstile with hundreds of other employees in the morning. Some fear that transaction duration c
environments. Others disagree. It's the difference between wave and go and touch and go. It does require some crowd behavior effort, but ju
on and off an escalator they'll learn how the system works. To deal with the time issue some are suggesting a switch from PKI, or asymm
scheme. People say that symmetric keys are faster than PKI at the door. But PKI is more secure and may actually be easier to deploy and m
With PKI the secret is stored on the card and it never leaves that card. There is a public certificate on the physical access control system bu
distributed and there is no security vulnerability. With symmetric keys the same certificate stored on the card also has to be stored on t
system. This leads to more complex key management than with PKI. Public keys don't need to be protected, but all these symmetric ke
to a reader on a door and must be protected in transit, in use and at the reader. This results in far more vulnerable situations and
system compromise. Symmetric key management can be expensive and complex, especially when dealing with something th
government. A fact of large scale use is that key management drives the cost. It's expensive. While symmetric keys may bring a sp
complexity of key management may be too much of a detractor. The General Services Administration has been pursing an exp
door solution. The agency contracted with Exostar, a provider of collaboration solutions for the aerospace and defense manu
their 40,000 supply chain partners and CertiPath, a credentialing authority for aviation, aerospace and defense organiz
concept demonstrates how a single-credential system can provide secure access for both physical and logical assets, w
providing interoperability for employees, customers and partners. The need for the system arose for the greater sec
needed for federal physical access control systems. The system demonstrates the ability to perform th
challenge response to the card authentication key on the contactless portion, but also how the system works with the contact portion including use of the biometrics and PIN. Additionally, it addresses ways to handle guests with and without PIV credentials. A visitor with a trusted credential can use it to pre-register via a Web site for a remote visit request. Upon arrival at the site the card has already been verified and after checking in the visitor can gain access to protected areas. Guests that do not have a trusted credential check in at an attended area and are issued a credential with an operational biometric and PKI certificate stored on the card. Now every defined population is using PKI for physical access control. HID Global is working to improve the speed of PKI at the door via caching. The company's caching status controller checks the certificate on the card once and then conducts

PHYSICAL SECURITY

periodic checks back to the revocation list to make sure the certificate is still valid. Initially the cardholder taps the badge on a reader and the PKI certificate on the card is checked against the Federal Bridge, a process that takes a couple seconds. From that point forward, the certificate is checked against the stored cache that is updated every hour against the Federal Bridge. In essence, at set time intervals the system validates the certificates from all cards commonly used in that specific access control environment. When a card is presented at an access reader, it need only be validated against the local cache, a process that is much quicker than validating against the remote system. You're extending the Federal Bridge right out to the door. Then you get virtually the same card performance as you do with a standard transparent reader and you're going with a smart, very secure edge appliance to do it. ID Technology Partners has created a solution for physical access control called Mutual Registration PIV, or MR-PIV, that speeds up transactions and potentially makes them more secure. The solution enables a credential holder to register the card in the local physical access control system and also register that system with the card. That way if anyone tries to sniff information off the card and the system doesn't have that

CRYPTOGRAPHY

mutual registration the card won't give up any information. Also, since it's a local identifier and not the global identifier the process is quicker. Rather than register the global identifier of the card we register the local identifier and a key to the physical access control system. This mutual registration speeds up the transaction to around half a second. The throughput is a five or six times performance increase. While it seems clear that PKI at the door is coming, not as clear is the role that biometrics will play with these new systems. Biometric authentication is the single best way to truly tie the credential to the holder. Biometrics are an intrinsic property of the owner. It adds to the high assurance and the non-transferability of the credential. This will become increasingly important as other weaknesses in physical access control systems are alleviated. In a PIV card system the contact interface of the card contains two fingerprint templates that can be used to confirm identity. These would be used to register into a new physical access control system. However, since the contactless interface doesn't have access to these templates, it would be difficult to use the biometric anywhere that high throughput is necessary. When a biometric authentication is required, would depend on the security policy of the particular agency. They wouldn't have to be used by credential holders on a daily basis. While general consensus seems to be that PKI at the door is the future for physical access control there are still challenges. One of the biggest maybe convincing those on the IT side and those on the physical security side to cooperate. But change is happening as the industry works to make it easier for the authorized to gain entry and make it more difficult for unauthorized

Is cryptography the future of physical access control?

PKI begins its migration from the desktop to the door

Zack Martin
Editor, AVISIAN Publications

n around for some time
are still serious questions,
physical access control
ems, the first thing that will
nterface of the credential will
he card. This process currently
used in another physical access
to have his credential registered
ess interface to have the PIV
and response that takes place with
ysical access systems would have to
ut for PKI to work there needs to be a
u need bi-directional protocols which
raises security concerns to some, but
ergo a makeover with PKI at the door.

OR

ntroller. Either way the processor on
smart reader. The argument is that
ystems will be time consuming and
open a door. This may not seem
ould be the deal breaker in many
st as people learned how to get
etric keys, to a symmetric key
manage than symmetric keys.
ut it's not a secret. It's widely
the physical access control
ys need to find their way
more opportunities for
e size of the federal
eed advantage the
edited PKI at the
ufacturers and
ations. The
hile also
urity
e

Most people don't think much about opening doors: insert key, turn knob and walk in. If your workplace issues ID badges there may be a bit more thought that goes into it as you tap the badge on a sensor, hear the click and pull open the door.

But physical access systems are undergoing the most radical transformation since the switch from keys to cards and tumblers to electronics. To the end user very little should change – there may be an increase in the use of biometrics – but most individuals will still simply tap the ID and go.

It's what happens behind the scenes that will be vastly different. Backend system will drastically change. Access control readers and controllers will become more sophisticated with cryptography and bi-directional communication. Because physical access control systems typically have a lifespan of 10 years, this won't happen overnight, but industry visionaries agree that it will happen.

Leading the charge for these next generation systems is the U.S. federal government. The FIPS 201 physical access control specification recommends public key infrastructure (PKI) at the door. The specification, Special Publication 800-116, does not mandate PKI, but recommends it. This, however, could change as a revision to the original FIPS 201 standards is due by the end of 2010 and some say it could include a PKI mandate (See *Predictions for FIPS 201-2*).

PKI is typically associated with logical access and digitally signing documents. When it was proposed for physical access it was something of a first. Making the leap wasn't that difficult though, says Bill MacGregor, a computer scientist at the National Institute of Standards and Technology. MacGregor, who was instrumental in writing Special Publication 800-116, says there were simply too many points of potential vulnerability with existing physical access systems.

"We knew there were a significant number of plausible threats against physical access control solutions dealing with authentication," MacGregor says. "There are devices available on eBay that would duplicate many of the common cards used for physical access control."

That's one of the reasons why the FIPS 201 spec released in 2005 limited the applications for the contactless interface and prohibited its use with biometrics and other sensitive data. It's also a reason many experts say that portion of the standard is incomplete and potentially even insecure.

The cardholder 's unique ID number is stored on the contactless portion of the card and it's possible for it to be read and copied. "This is more or less a step above a prox reader," says Rob Zivney, vice president of business development at Hirsch Electronics. "To get the real benefit of FIPS 201 you need to do better than a basic read of the cardholder unique ID, you need to go to PKI."

In order to properly secure systems and provide high-assurance authentication, the government needed to apply cryptography, MacGregor says. Since FIPS 201 was already using smart cards and PKI for logical access it seemed like a logical leap to use it on the physical

Predictions for FIPS 201-2

Every five years federal information processing standards (FIPS) are up for revision and since it's been half a decade since FIPS 201 was released discussion on what may be included in an update is underway.

It's difficult to say what may be included this early in the year, but experts are focused on five areas.

PKI at the door

Even though many vendors and government officials suggest PKI for physical access control is the next big thing, FIPS 201 doesn't mandate it. NIST Special Publication 800-116 recommends PKI at the door but many say it could be mandated in the revised FIPS 201 specification.

Contactless

The contactless capability was purposefully limited in the first standard and this has been an ongoing criticism of the first spec. Many from the physical security realm would like to access biometrics over the contactless interface, a practice that is currently prohibited. Perhaps an easing of these limitations is on the horizon.

Match on card

Officials posit that match-on-card fingerprint biometrics could be included in the revised spec. With match-on-card technology the fingerprint template never leaves the card and the match is conducted on the card itself, rather than a reader or controller.

Iris

Iris biometric standards have improved in the past five years and the proprietary nature of the technology has eased. Some predict it will be added as an additional biometric modality for FIPS 201.

Adding trusted applications

Another criticism of FIPS 201 is that it basically sealed off the card after issuance. Agencies that wanted to add another application, such as e-purse, haven't been able to do it. A revised FIPS 201-2 may include the ability to add trusted applications to the card to increase its usability. ID

Symmetric key cryptography

In a symmetric key system the same encryption key is used to both encrypt and decrypt a message. Thus both the sender and the recipient must be in possession of the shared, secret key. In the case of a physical access control system using symmetric keys, this key sharing leaves both the cards and the system as points of vulnerability. Examples of common symmetric key systems include AES and DES.

Asymmetric key cryptography

In an asymmetric system, a matched pair of encryption keys – one public and one private – is issued for each credential or user. Data encrypted using one key from a pair can only be decrypted using the pair's other key. The power of an asymmetric system is that a user's private key never leaves his possession. Unlike a symmetric system, there are no shared secrets in asymmetric cryptography and thus vulnerabilities are greatly reduced. Public key cryptography is synonymous with asymmetric cryptography.

Public Key Infrastructure (PKI)

PKI is a specific implementation of asymmetric cryptography. It relies on the use of digital certificates that are issued by certificate authorities as a means to bind a user to an assigned key pair. In other words, a trusted third party (the certificate authority) vets the identity of the individual owning the key pair and then issues a document (the digital certificate) asserting this fact. In use, others can have confidence in the identity of a key pair's owner by verifying the authenticity of the digital certificate.

side of things too. "PKI is a fully standardized, mature technology and it's deployed through the Federal Bridge," he says. "And it forms the core of the trust model for the PIV credential."

While using PKI for physical access control might be new, the technology is not, says Sal D'Agostino, CEO at IDmachines. That it's been around for some time and there are standards around it means not having to reinvent the wheel. "It's strong security, standards based, open and through a federation it enables trust and interoperability," he says.

But there are still serious questions, including how long it takes to process a transaction and how it will affect existing physical access control infrastructures.

How it will work

In a PKI at the door implementation, as in traditional access control systems, the first thing that will happen is registration into the system. At this point in the FIPS 201 environment, the contact interface of the credential will be used to check the PKI certificate, PIN and fingerprint biometric template stored on the card.

This process currently takes between 13 and 30 seconds and will have to be performed whenever the credential is to be used in another physical access system. For example, a State Department employee going to a Homeland Security office will need to have his credential registered into the system before it can be used.

After that initial registration the cardholder can use the contactless interface to have the PIV authentication key, one of the four PKI certificate on the card, checked. This process, along with the usual challenge and response that takes place with contactless smart card transactions, currently takes one to three seconds.

First, however, the existing infrastructure for most physical access systems would have to be upgraded. Typical access control systems use the Weigand protocol to communicate with controllers. Weigand is a one way communication, says David Auman, partner at ID Technology Partners. But for PKI to work there needs to be a back and forth with the system. "Current systems are designed to send an ID number and not much more," he says. "But if you want to do authentication you need bi-directional protocols which you get with a network."

PKI at the door will require Internet Protocol-based access control devices, Auman says. "When you bring session encryption and mutual authentication you need an IP-based device just to get the connection," he says.

Putting physical access control systems online raises security concerns to some, but just because you IP-enable a system doesn't mean it's available via open networks, Auman says.

The physical access readers and controllers will also have to undergo a makeover with PKI at the door, says Hirsch's Zivney. There will be two choices for the architecture of new physical access systems: do the processing of PKI certificates at the reader or do it at the controller. Either way the processor on the device that is chosen will need additional cryptographic certification.

Most likely the choice will be to go with a smart controller instead of a smart reader, Zivney says. "The argument is that there's too much risk in putting the intelligence on the unsecure side of the wall," he says.

Wave and go vs. hold and go

While upgrading the infrastructure for physical access control systems will be time consuming and costly, a bigger concern with PKI at the door is how long the transaction will take. Experts say it could take as long as a second and a half to open a door. This may not seem excessive but imagine trying to get through a turnstile with hundreds of other employees in the morning. Some fear that transaction duration could be the deal breaker in many environments.

METROPOLITAIN
What do the Cannes Film Festival and the Paris Metro have in common?

evolis
Pebble

Others disagree. "It's the difference between wave and go and touch and go," says D'Agostino. "It does require some crowd behavior effort, but just as people learned how to get on and off an escalator they'll learn how the system works."

Symmetric vs. asymmetric keys

To deal with the time issue some are suggesting a switch from PKI, or asymmetric keys, to a symmetric key scheme, says MacGregor. "People say that symmetric keys are faster than PKI at the door," he says.

But PKI is more secure and may actually be easier to deploy and manage than symmetric keys, MacGregor says. With PKI the secret is stored on the card and it never leaves that card. There is a public certificate on the physical access control system but it's not a secret. "It's widely distributed and there is no security vulnerability," he says.

With symmetric keys the same certificate stored on the card also has to be stored on the physical access control system. This leads to more complex key management than with PKI. "Public keys don't need to be protected," MacGregor says, "but all these symmetric keys need to find their way to a reader on a door and must be protected in transit, in use and at the reader." This results in far more vulnerable situations and more opportunities for system compromise.

Symmetric key management can be expensive and complex, especially when dealing with something the size of the federal government, says MacGregor. "A fact of large scale use is that key management drives the cost," he says. "It's expensive."

While symmetric keys may bring a speed advantage the complexity of key management may be too much of a detractor.

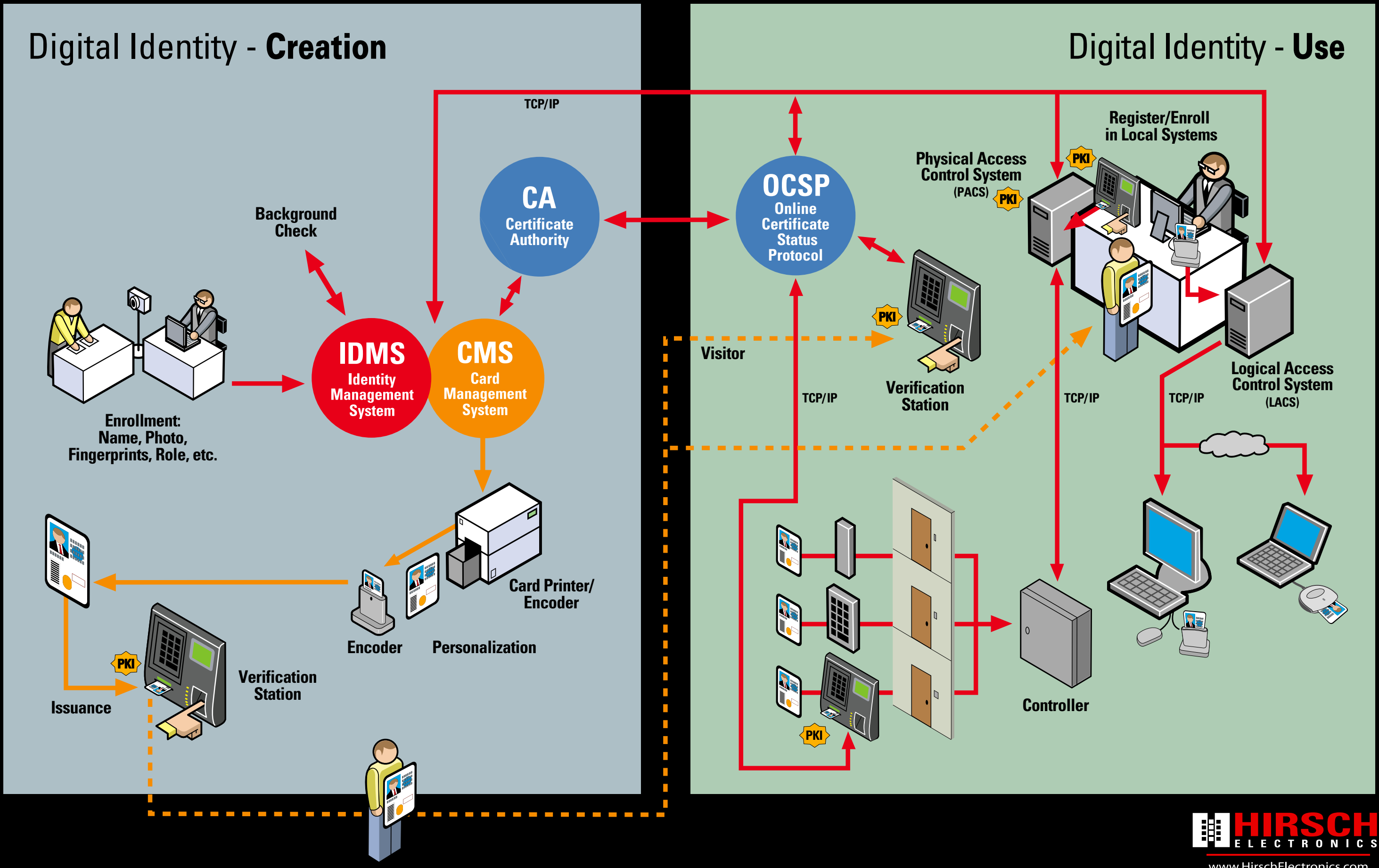
Making PKI work at the door without the wait

The General Services Administration has been pursing an expedited PKI at the door solution. The agency contracted with Exostar, a provider of collaboration solutions for the aerospace and defense manufacturers and their 40,000 supply chain partners and CertiPath, a credentialing authority for aviation, aerospace and defense organizations.

The concept demonstrates how a single-credential system can provide secure access for both physical and logical assets, while also providing interoperability for employees, customers and partners. The need for the system arose for the greater security needed for federal physical access control systems, says Steve Howard, vice president of operation at CertiPath.

The system demonstrates the ability to perform the challenge response to the card authentication key on the contactless portion, but also how the system works with the contact portion including use of the biometrics and PIN, Howard says.

Additionally, it addresses ways to handle guests with and without PIV credentials, How-



Digital Identity - **Creation**
Digital Identity - **Use**
TCP/IP
Background Check
CA Certificate Authority
OCSP Online Certificate Status Protocol
Register/Enroll in Local Systems
Physical Access Control System (PACS)
PKI
Enrollment: Name, Photo, Fingerprints, Role, etc.
IDMS Identity Management System
CMS Card Management System
Visitor
Verification Station
TCP/IP
Logical Access Control System (LACS)
Card Printer/ Encoder
Encoder
Personalization
Issuance
Verification Station
Controller

ard says. A visitor with a trusted credential can use it to pre-register via a Web site for a remote visit request. Upon arrival at the site the card has already been verified and after checking in the visitor can gain access to protected areas.

Guests that do not have a trusted credential check in at an attended area and are issued a credential with an operational biometric and PKI certificate stored on the card, Howard says. "Now every defined population is using PKI for physical access control," he says.

CertiPath's architecture conforms to the principles of NIST Special Publication 800-116 and also:

- Leverages PIV, PIV-I, the Department of Defense Common Access Card and the Transportation Worker Identity Credential
- Utilizes FIPS 201-certified, or in process, components
- Enables customers to upgrade without replacing existing systems
- Leverages commercially available products to minimize custom solutions
- Uses the U.S. Federal Bridge to validate interagency trust
- Delivers cost-effective options to operate at one or multiple assurance levels

'Caching' in on PKI

HID Global is working to improve the speed of PKI at the door via caching, says David Adams, senior product marketing manager at the company. The company's caching status controller checks the certificate on the card once and then conducts periodic checks back to the revocation list to make sure the certificate is still valid.

Initially the cardholder taps the badge on a reader, Adams says, and the PKI certificate on the card is checked against the Federal Bridge, a process that takes a couple seconds. From that point forward, the certificate is checked against the stored cache that is updated every hour against the Federal Bridge.

Federal Bridge

The Federal Bridge Certification Authority is a system that facilitates acceptance of PKI certifications for transactions. Since its initial concept and operations, it since evolved into the Federal Public Key Infrastructure Architecture (FPKIA) that encompasses Certification Authorities from multiple vendors supporting different Federal PKI policy and function.

In essence, at set time intervals the system validates the certificates from all cards commonly used in that specific access control environment. When a card is presented at an access reader, it need only be validated against the local cache, a process that is much quicker than validating against the remote system.

"You're extending the Federal Bridge right out to the door," Adams says. "Then you get virtually the same card performance as you do with a standard transparent reader and you're going with a smart, very secure edge appliance to do it."

Meet MR-PIV

ID Technology Partners has created a solution for physical access control called Mutual Registration PIV, or MR-PIV, that speeds up transactions and potentially makes them more secure, says Auman.

The solution enables a credential holder to register the card in the local physical access control system and also register that system with the card, Auman says. That way if anyone tries to sniff information off the card and the system doesn't have that mutual registration the card won't give up any information. Also, since it's a local identifier and not the global identifier the process is quicker.

Beyond convergence and PKI: Fusion

PKI at the door may be coming and most have heard about the convergence of physical access and access to computer networks using one credential, but beyond that is what some are calling fusion.

Fusion may be the ultimate end game of PKI at the door and convergence. Once physical access control readers and IT networks are wired together it will enable the systems to do things never before possible and have far greater intelligence, says Bill MacGregor, a computer scientist at the National Institute of Standards and Technology. "Information can be shared across the physical and logical worlds," MacGregor says.

"A parallel would be with fraud detection in retail practices," MacGregor says. "We are all used to the idea that if we travel somewhere and use a payment card there might be questions."

Similarly, fusion would enable a system to question why someone is using a badge for physical access in San Francisco when they are logged on to a computer in Chicago or even using the phone in another location. Such a system could also track when an employee walks in the front door, only then enabling him to login to secure computer networks.

ID

“Rather than register the global identifier of the card we register the local identifier and a key to the physical access control system,” Auman says.

This mutual registration speeds up the transaction to around half a second, Auman says. “The throughput is a five or six times performance increase,” he says.

The role of biometrics in physical access

While it seems clear that PKI at the door is coming, not as clear is the role that biometrics will play with these new systems. Biometric authentication is the single best way to truly tie the credential to the holder.

“Biometrics are an intrinsic property of the owner,” says NIST’s MacGregor. “It adds to the high assurance and the non-transferability of the credential.” This will become increasingly important as other weaknesses in physical access control systems are alleviated.

In a PIV card system the contact interface of the card contains two fingerprint templates that can be used to confirm identity. These would be used to register into a new physical access control system. However, since the contactless interface doesn’t have access to these templates, it would be difficult to use the biometric anywhere that high throughput is necessary.

When a biometric authentication is required, would depend on the security policy of the particular agency. They wouldn’t have to be used by credential holders on a daily basis.

D’Agostino says biometrics must begin to play more of a role in physical access control. “PINS are a pain,” he says. “Biometrics is much easier than PIN and it’s the preferred second factor.”

Turf war

While general consensus seems to be that PKI at the door is the future for physical access control there are still challenges. One of the biggest maybe convincing those on the IT side and those on the physical security side to co-operate, says MacGregor. “It does require governance to talk about change management,” he says.

But change is happening as the industry works to make it easier for the authorized to gain entry while making it more difficult for the unauthorized to circumvent systems. The changes won’t happen overnight and won’t come without pain, but in the end security will be improved.

The biometric problem

Any discussion of physical access control should also include the role of biometrics. Fingerprint scanners have been used for some time with these systems and iris biometrics are becoming more popular too.

Biometrics may be the only way to truly tie a credential to its holder. But the identification technologies are still not without problems, says Bill MacGregor, a computer scientist at the National Institute of Standards and Technology.

The infamous use of gummy bears to copy fingerprints is almost ten-years old, but making sure an actual finger is placed on a scanner is still a concern. Many scanners are very good at liveness detection while others are not.

“The system has to know that the sample is coming from a person and not some simulated object,” he says. “Some sensors are very good at this and some are very poor and we know the differences because they have been reported but what we don’t have is a systematic basis for evaluating the resistance to a false or simulated object.”

Five-years ago the FIPS 201 specification actually took liveness into account, MacGregor says. The card has two biometric authentication methods, one called Bio and another called Bio A. Depending on the security level of the particular agency one or the other can be used.

Bio is a lower assurance level that uses the biometric to authenticate identity and it relies on the liveness capture of the scanner. Bio A is high assurance and requires that an individual watch the finger be placed on the scanner to make sure that the credential holder’s actual finger is presented.

While the use of biometrics may be limited with federal projects for now, some predict that won’t be the case for long. (See *Predictions for FIPS 201-2*, page 21).

Photos: HID Global

Next generation PACS

Stephen P. Howard, *VP Operations, CertiPath LLC*
Salvatore D'Agostino, *CEO, ID Machines*

It's here: next generation physical access control. The key drivers of physical access control systems are interoperability, security, scale and convergence of the logical and physical – people and things. These features come when leveraging the benefits of smart card credentials. Moreover, the standards behind next generation PACS provide a basis and building blocks that enable cost-effective and secure solutions.

The next generation systems are a new class of enterprise identity application that promises tremendous value. However, one critical consideration to bear in mind: these solutions must support integration with enterprise identity infrastructure – in particular, the emerging Personal Identity Verification credentials (PIV) issued by federal agencies, and the new Personal Identity Verification-Interoperable credentials (PIV-I) from non-federal issuers.

Navigating the Threat Landscape

Today's cyber environment is full of threats and security risks. A next-gen system gains resiliency from its use of strong authentication, ensuring it cannot be fooled by clones and copies. A resilient physical access control system must take advantage of public and enterprise IT infrastructure, providing the provisioning and integrity of the credential within the system.

Identity and financial fraud runs into the tens of billions per year. Physical access control cannot be the weak link in solving this problem. To combat fraud, the next generation system upgrades credentials and hardware. The traditional lifespan of most physical access control systems exceeds 10 years. In some cases, technology refresh can take decades. As an example, look at physical keys, keyways and locksets. More than 100 vendors recognize this, and have made substantial investment in next generation products and people.

PKI: The Next Step

Throughout industry and government, public key infrastructure is widely used to enable cloud infrastructure, platforms and applications. Standards developers claim that using PKI to bring strong authentication to physical access systems is the next logical step.

Next generation solutions are at the forefront of strong authentication technology that supports the ubiquitous use of identity credentials and devices. These physical access control systems leverage PKI and biometrics for contact and contactless solutions, as appropriate to users' needs.

The type and number of authentication factors adapt to the resource being accessed:

- What you have: e.g., digital certificates with challenge response protocols
- What you know: Fortunately, this can be a single PIN
- What you are: Typically a fingerprint and facial image, although increasingly iris and vein patterns.

PKI use has always been driven by the scale and key management asymmetric cryptography can provide. However, its implementation at scale presents challenges. At the U.S. Department of Defense, PKI lumbered under the load of revocation list data required to handle millions of users and high credential turnover.

Today, distributed validation products have been specified and deployed to support the growing population of more than 5 million PIV and PIV-I credentials. The next generation PACS makes use of this identity infrastructure and follows its expansion into critical infrastructure and other enterprises.

The Rise of PIV and PIV-I

PIV and PIV-I break open traditionally proprietary systems. Complying with these standards enables end-users and system integrators to gain flexibility with the system components used. This occurs in credentials, readers, panels, servers, sensors, alarms, video and networking gear. Complete interoperability enabling mix-and-match service providers isn't yet a reality, but standards have paved the way for customer options.

Physical access isn't the only reason enterprises should use interoperable credentials that deliver strong authentication and interoperability. PIV and PIV-I provide the scope and flexibility to address enterprise information application needs with authentication, encryption, signing and multiple form factors – and are particularly well-adapted to mobile form factors. Replacing a dual interface smart card with a mobile phone using its SIM and/or wireless capabilities already exist in "version 0.1" demos.

PACS environments are ideal for deploying strong authentication of both users and devices. PACS devices and controllers will make use of mutual strong authentication and encryption in accordance with the National Institute of Standards and Technology guidance on information security. These standards include FIPS 140, 199, 187 and 201. In fact, next generation physical access control deployments leveraging these standards are a pre-cursor to its use by supervisory control and data acquisition systems for critical infrastructures, manufacturing and process control.

Protecting Against Attack

In this continuum physical access control systems are no longer isolated. Deployed systems often run on their own dedicated IT network – rather than just a dedicated subnet – and their own dedicated servers. This isolation leads to a false sense of security.

Systems isolated from the internet are not immune to cyber and direct attack, especially given the expanding use of internet protocol devices by vendors. IP cameras deployed in the last decade without strong authentication or encryption are everywhere. Case in point: the United States government drone cameras that were sending video in the clear.

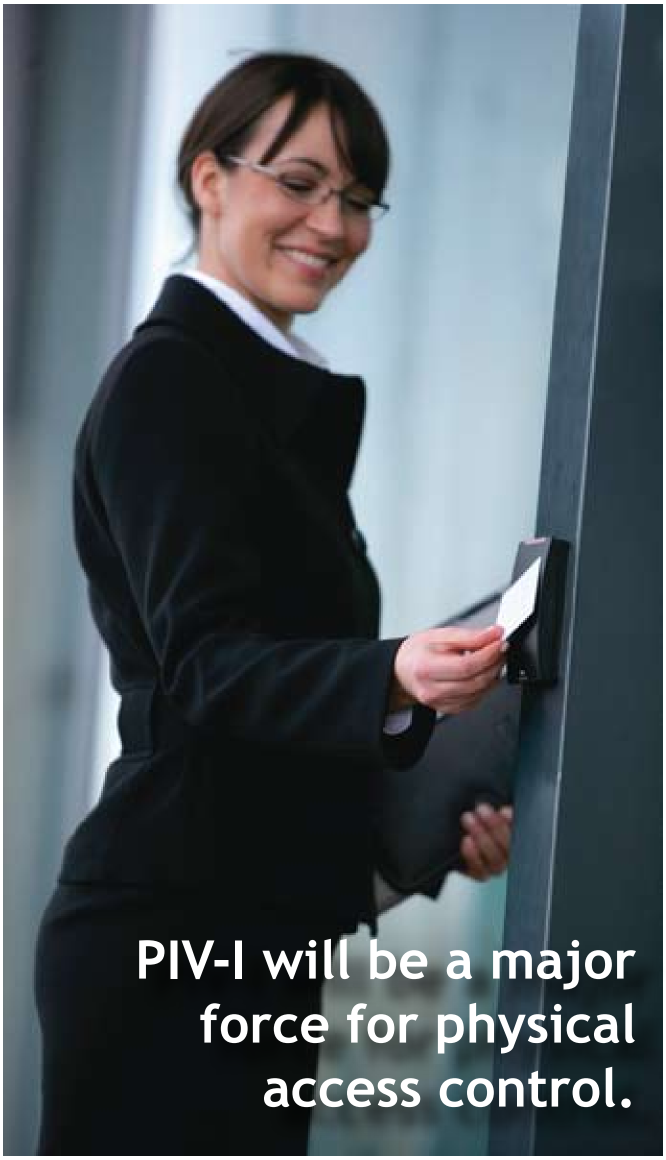
Next generation systems, along with PIV and PIV-I credentials and devices use strong authentication to address these challenges in two ways:

- Via the enterprise databases that exchange data with the PACS
- At the door, to mitigate attacks against individuals and assets.

With these new operational models in place, physical access moves away from just something that opens doors to a system that is part of a building. It is now a key application that must be built on the same architecture as IT networks and other corporate assets – such as the identity management and credential issuance system (IdM-CIS), for issuance of PIV and PIV-I credentials. They participate in high-assurance provisioning of the credentials and applications with individual access roles, rules and attributes.

Increasing sensors and resolution, a need for security in depth, increased use of analytics – all create the need for more data assigned to and consumed by access control systems.

By their very nature these systems deal with personally identifiable information, and the next generation will necessarily have to deal with the security of data at rest and in motion. Access control systems may contain biometric identifiers, emergency contact information, name, address, and related personal information. To minimize this information, next generation systems will take advantage of the mutual registration capabilities of PIV and PIV-I credentials. The ability to write to the card and also to anonymize or encrypt these identifiers represents an easy way to address the overhead associated with using "real" personal information.



PIV-I will be a major force for physical access control.

Compliance Best Practices

PACS distributed databases need to be protected like any other IT system on the network – such as HR, ADFS, or payroll records. Consequently, administration and management of the security of these systems must involve traditional controls. In the Federal enterprise, this is FISMA certification. For corporations, it is often industry-specific, with an alphabet soup of compliance mandates, including CFATS, HIPAA, PCI, and SOX.

Proper implementation of the four A's of access is key to establishing and maintaining compliance:

- Administration
- Authentication
- Authorization
- Audit.

Together, these form a best practice checklist to ensure next generation PACS align with compliance goals.

A Shifting Market

Who are the vendors in the next generation marketplace?

Interestingly, it is fairly dynamic. Over time, different companies become market leaders and then go to pasture. Consolidation among building controls companies – SCM/Hirsch, Honeywell, Tyco, United Technologies, Johnson Controls, Siemens and Schneider – continues while the technology shift presents opportunities for new and innovative solutions. All of IT, TCP/IP and smart cards bring new technologies and partnerships – as well as a healthy dose of technology infusion.

However, access control systems are delivered by installers and system integrators – the overwhelming percentage of which are small to medium-sized businesses. These installers have extensive experience providing service – access, life/safety, burglar and fire alarms – and growing recurring monthly revenue. An important step in the transition of next generation systems will involve partnership between these businesses, as well as adoption of by global integrators and, increasingly, by global services organizations.

Large IT product and services companies have a foot in the door. Examples include Cisco, Verizon, HP, Unisys, CSC, Booz Allen, and others. As physical access control systems become an enterprise application and funding overlaps with IT, these organizations will be forced into the arena – and will look to grow their businesses supporting early use cases. Some already have involvement in the issuance of the credential and the supporting infrastructure.

In this transition, the access control perspective offers an alternative viewpoint. Specifically, the integration of PIV and PIV-I into deployed PACS, as well as emerging architectures for PACS going forward. There must be a value proposition to vendors. How exactly do they make money as a result of these changes in the marketplace?

Good customer communications with regard to single sign-on and strong authentication should blaze the trail of discovery. Convergence, single sign-on and strong authentication are driving forces in corporate and agency IT strategies.

The Road Ahead

Certainly, questions remain. How does a physical access control vendor differentiate itself in the market if the credentials and issuance systems for those credentials are now standardized? How do these vendors deal with separate identity infrastructure and enterprise identity management solutions? How do access control vendors issue temporary or replacement credentials? Is it possible to do local PIV-I electronic personalization?

Consider the ease of badging with a traditional prox card versus issuance of a PIV-I credential. Next generation systems need capabilities to deploy, register, enroll, issue and activate PIV-I credentials approaching the same, easily personalized solutions of prox cards.

One way to differentiate is in the means of integration. "How" becomes more important than "what" particularly when standards-based components are involved. This is true whether it is green field deployment or upgrading deployed systems: The ability to offer services for migration and management of change will be critical to success.

When it comes to standardized credentials and their impact on the credentialing ecosystem, PIV-I will have a larger overall influence than PIV. Why? Consider the potential volumes. The government – Executive Branch only – represents the PIV community, supporting about 6 million credentials today, expected to grow to about 10 million.

PIV-I represents the supply chain into the federal agencies. The Defense Department alone has a supply chain that numbers in excess of 20 million. First responders, utility providers, telecommunications, state and local government, legislative and judicial branch, are *all* PIV-I communities. There is an opportunity for PIV-I to dwarf PIV, as it represents well over 150 million individuals with a relationship to the federal government.

With a footprint this large, it is not reasonable to be an ostrich and stick our heads in the sand. PIV-I will be a major force for physical access control.

The market has seen a dramatic shift away from physical access control as a building asset to seeing it as an IT asset. This helps breaks down the stovepipes separating the chief information officer, the chief information security officer and the chief security officer's organizations.

Identity is a common tool that spans these organizations. Provisioning, and more importantly, de-provisioning, is critical to any cyber security and PACS strategy. Next generation access control leveraging PKI and PIV-I will become a hallmark of the successful enterprise.

ICAM: A roadmap for FIPS 201 applications

Mission of new initiative is to help agencies, others put PIV credentials to use

The presidential directive ordering a standard, interoperable identification credential for federal employees is coming up on its sixth birthday. The deadline to have these Personal Identification Verification (PIV) credentials issued is more than a year old.

And while every federal employee may not yet be carrying around a PIV there have been more than 4 million credentials issued. So it just makes sense that the next step should be creating use cases for the IDs.

"No two agencies are in the same place and no two agencies have the same need," says Judith Spencer, chair of the Federal Public Key Infrastructure Steering Committee for the GSA. "So they need to figure out what they need to do and what needs to be applied."

Enter ICAM or Identity, Credential and Access Management, a group of government officials co-chaired by the General Services Administration and Department of Defense and charged with aligning the identity management activities of the federal government.

ICAM key target initiatives

1. ***Augment policy and implementation guidance to agencies***
2. ***Establish federated identity framework for the federal government***
3. ***Enhance performance measurement and accountability within ICAM initiatives***
4. ***Provide government-wide services for common ICAM requirements***
5. ***Streamline collection and sharing of digital identity data***
6. ***Fully leverage PIV and PIV-I credentials***
7. ***Modernize physical and logical access infrastructures***
8. ***Implement federated identity capabilities***

The organization released a "Roadmap and Implementation Guidance" document for officials late in 2009. Now ICAM is working on a more robust version of the implementation guidance, tentatively called Part B, which it hopes to complete by the end of September. "The Federal Government is operating in a constantly shifting threat environment – data breaches are all too common, identity theft is on the rise, and trust relationships are enforced in an inconsistent and hard-to understand manner," states the Roadmap.

The hope is that ICAM work will extend outside the federal space. "The resulting framework can be leveraged in other areas as well – promoting data security, privacy and the high-assurance authentication needed to support improvements in health care and immigration and to promote collaboration through secure information sharing and transparency in government," the document states.

The PIV is an essential component to ICAM. Some 4.1 million federal employees, or 71%, have been issued credentials, according to the Fiscal Year 2011 Federal Budget. The ICAM Roadmap is also cited in the budget, a fact that highlights just how ingrained the PIV credentials are with federal employees.

"The ICAM roadmap, issued in November 2009, outlines a number of transition activities for agencies to complete," the document states. "It also serves as an important tool for providing awareness to external mission partners and driving the development and implementation of interoperable solutions. ICAM solutions will leverage the existing investments in the federal government while promoting efficient use of tax dollars when designing, deploying and operating ICAM systems."

In preparation for the September issuance of the implementation guidance Part B, six different ICAM working groups have been created:

- The Federation Interoperability Working Group is looking at business rules and requirements for how agencies will establish reciprocal trust agreements so credentials can be used at other agencies, Spencer says.
- The Architecture Working Group is developing "how to's" and expanding the new technical architecture of the credentials. The group is also working on 11 use cases for the credential, Spencer says.

- The Federal PKI Authority Working Group is looking at strong-assurance technology and administering the federal PKI policies.
- The Roadmap Development Team is reviewing the development and content of the ICAM Roadmap and Implementation Guidance.
- The Citizen Outreach Focus Group is working on recommendations concerning solutions for government-to-citizen interaction and how ID technology may play a role in the future.
- The Logical Access Working Group is developing guidance and best practices to assist agencies in implementing log on/authentication capabilities using PIV cards.

The ICAM roadmap also details some of the benefits agencies will experience via the implementation of ICAM systems and technology:

- Increased security, which correlates to reduction in identity theft, data breaches, and trust violations.
- Compliance with laws, regulations, and standards as well as resolution of issues highlighted in GAO reports of agency progress.
- Improved interoperability, specifically between agencies using their PIV credentials along with other partners carrying PIV-Interoperable or third-party credentials that meet the requirements of the federal trust framework.
- Enhanced customer service, both within agencies and with their business partners and constituents.
- Elimination of redundancy, both through agency consolidation of processes and workflow and the provision of government-wide services to support ICAM processes.
- Increased protection of personally identifiable information by consolidating and securing identity data.

Where does PIV-I fit?

ICAM is also considering how the PIV-I will interact with government credentialing, says Steve Howard, vice president of operations at CertiPath. The architecture group is working with a PIV-I subgroup to figure out use cases for how the two credentials will work together. "Their goal is to come up with the governing requirements that will translate to certificate policy," he says.

While PIV-I has been looked at as a standard for first responders and state officials, federal contractors will also be using it, Howard says. This makes interaction unavoidable.

Strategic Vision

The ICAM Roadmap outlines a strategic vision for identity, credential, and access management efforts with the Executive Branch of the Federal Government and demonstrates the importance of implementing the ICAM segment architecture in support of five goals and their related objectives.

Goal One 1 ***Comply with federal laws relevant to ICAM***	**Goal Two** 2 ***Facilitate government by streamlining access to services***	**Goal Three** 3 ***Improve security posture throughout the federal enterprise***	**Goal Four** 4 ***Enable trust and interoperability***	**Goal Five** 5 ***Reduce costs and increase efficiency***
• Align and coordinate federal policies and key ICAM initiatives • Establish and enforce accountability to governing bodies	• Expand secure electronic access to government data and systems • Promote public confidence through transparent practices	• Support cybersecurity programs • Integrate electronic verification procedures into physical security • Drive the use of risk-based framework for access control • Improve electronic audit capabilities	• Support information sharing communities of interest • Align processes with external partners • Establish and maintain trust relationships • Leverage standards and commercially available products	• Reduce administrative burden associated with ICAM • Align existing and reduce redundant programs • Increase interoperability and reuse of programs and systems

2010: When ideas become reality?

Last year saw the groundwork for ID projects but this year they could become reality

E-Verify™
U.S. Department of Homeland Security
Social Security Administration USA

The first year of the Obama administration saw many credentialing and security project take shape, but in 2010 some of these projects may become a reality, says Kelli Emerick, executive director of the Secure ID Coalition.

"The recognition that identity manage is critical to the Obama administration agenda is starting to come through," Emerick says. "2010 is the year you will see some of those areas bear fruit," she explains citing specific examples including immigration, health care and e-government and authentication.

Immigration reform

Sen. Chuck Schumer (D-N.Y.) is pushing for better employment verification. He held hearings on the subject in 2009, pushing for additions to the U.S. Department of Homeland Security's E-Verify system.

E-Verify checks an employee's Social Security number and gives the employer a red light or green light response to indicate whether the number is valid. But it makes no attempt to tie the number to the individual.

Schumer called for a "non-forgeable identification system to completely and accurately identify workers." Biometrics were the primary system talked about last year but some industry insiders also suggest a smart card could become part of the plan.

Health care

The health care industry received $19 billion in funding in 2009 to use advanced technologies to deploy electronic medical records for patients. But one of the concerns is making sure patients are properly identified in electronic records and making sure only those with authorization can access them.

The U.S. Department of Health and Human Services (HHS) is working to develop standards and recommendations on how these records should be secured and what types of technologies could be used, Emerick says. HHS also has established a privacy and security working group.

Some high-level recommendations have been made to the Office of the National Coordinator for Health Information Technology, the group heading the administration's health IT efforts. These include building on existing standards for authentication and identity proofing, determining the level of assurance appropriate for different exchange scenarios and permitting innovation and local autonomy in the method of authentication. The recommendation, however, states that no single infrastructure should be put in place nationally.

These efforts have also been recognized in the Cybersecurity bill passed by the U.S. House of Representatives. The bill calls for officials to: "improve privacy protection in identity management systems, including health information technology systems, through authentication and security protocols." As of press time the Senate had not voted on the bill. (See *House passes cybersecurity bill*)

The federal budget also mentioned health care, identifying privacy for electronic health records and the personal information stored within them as a priority. "This is a huge step in the right direction in the implementation of electronic health records," Emerick says. "With sufficient privacy and security controls, EHRs can be adopted for patients and ensure personal heath information will be kept private."

Government authentication efforts

There are also the internal efforts to use more electronic authentication technology within the federal government, Emerick says. The proposed budget discusses identity management for the Federal government in a broader sense by addressing various levels necessary in all computing environments, especially when dealing with national infrastructure. The budget slightly increases IT spending to $79.4 billion.

"You'll start to see many of the policies for these programs develop in the next year and the implementation will happen over the next couple of years," says Emerick. "The good news is the Obama 2010 budget recognizes that using information technology solutions to improve government requires security and privacy protection for everyone." ID

House passes cybersecurity bill

The U.S. House of Representatives passed the "Cybersecurity Enhancement Act of 2010" aimed at improving cybersecurity research, development and technical standards.

The proposed law would establish a position for a national coordinator for the program to develop standards around identity management, with a particular focus on health care.

Goals for the new director include:

- Improve interoperability among identity management technologies;
- Strengthen authentication methods of identity management systems;
- Improve privacy protection in identity management systems, including health information technology systems, through authentication and security protocols; and
- Improve the usability of identity management systems.

The house passed the bill 422-5. As of press time the Senate had not voted on the proposed legislation. ID

Miami-Dade makes launching a contactless fare collection system EASY

Miami's new smart card-based transit system rolls out in record time

Ed McKinley
Contributing Editor, AVISIAN Publications

A new $42 million contactless smart card fare-collection system is helping Miami-Dade County Transit (MDT) boost ridership, streamline routes, combat fraud and make its service more convenient. Miami's transit system is the nation's 14th largest with a thousand buses, a 23.5-mile Metrorail system and a free 8.5-mile downtown Metromover system.

To smooth the transition to tapping the new plastic EASY Cards and paper EASY Tickets on contactless smart card scanners, MDT looked inward to draw upon the experience of its own transit chief and went outside itself to seek help of an experienced vendor.

The in-house font of experience was Harpal S. Kapoor, MDT director. Kapoor had worked his way up during 15 years in Miami but had not pursued a straight career trajectory. He left MDT for a while, spending six years with the Washington Metropolitan Area Transit Authority. It was while working in the nation's capital that he gained experience in the installation of new fare systems.

The system Kapoor helped set up in Washington resembles the new one in Miami. Both are based on the Nextfare Solution Suite from San Diego-based Cubic Transportation Systems Inc. Cubic has been selling the system for about seven years, says Steve Brunner, the vendor's senior program director.

Nextfare is operating in cities and regions that include Atlanta, Baltimore, Los Angeles, San Diego, Minneapolis, Philadelphia and New York-New Jersey, says Brunner. "Among cities that have systems," he adds, "I can only think of one major city in the U.S. we don't have."

MDT and the county commissioners chose Cubic in a competitive process designed to find "the most responsive and responsible vendor," says Kapoor. MDT awarded grades to bidders for low cost, technical savvy and tight scheduling – with Cubic emerging victorious. Coincidentally, Cubic had also supplied the 26-year-old system MDT wanted to replace.

In a hurry

When considering vendors, MDT was motivated partly by a desire to convert to the new fare-collection system as quickly as possible. MDT was in a hurry to staunch losses from fraud, provide convenient features for riders and begin collecting data more efficiently to improve the transit system's operations, says Kapoor.

Photos: Miami-Dade Transit

The official launch came Oct. 1, about 15 months after MDT signed the contract. The quickest previous project required more than 18 months to implement, says Richard Wunderle, Cubic senior vice president and general manager.

Cubic managed to expedite the process because it has deployed the Nextfare system 11 times, Wunderle says. "While each customer has specific and unique requirements that we incorporate into the design," he says. "The basic software platform and much of the infrastructure is the same so we don't reinvent the wheel each time."

Still all parties agree that getting the wheel to roll straight and quickly required cooperation. MDT retained control of the parts of the project its leaders believed they could do better and gave Cubic authority where it could operate more efficiently, Kapoor says. "Then we came together as a team to see how we could deliver it faster," he says.

The sooner the new fare system came online, the sooner MDT could thwart the thieves who were counterfeiting paper bus transfers and monthly magnetic-stripe rail passes, says Kapoor. Fare beaters also found it easy to walk through gates intended for the handicapped.

Now all gates are kept closed, and no one enters without tapping a card or ticket on a reader. If someone does succeed in sneaking into the system, he or she is required to "tap out" to leave, thus creating another opportunity to apprehend the fare beater.

The power of data

The new fare system also furnishes MDT with much richer data than the old system. Transit officials learned soon after installing the new system that riders seldom used 1,500 of the 10,000 bus stops scattered around the county, Kapoor says. That knowledge enabled MDT to eliminate stops or relocate them to higher-traffic areas.

MDT expects to discontinue some bus routes and plan schedules more effectively saving millions of dollars per year, all because of the ridership data provided by the new system, Kapoor says. He could not calculate the exact savings because the system had been in place only a short period as of press time.

The new data also indicates where to place stops to shorten walks for senior citizens. Seniors who live in the county full time qualify for free public transportation with their Gold Passport cards. Now, officials can track the timing, distance and locations of their travel to make sure the system meets their needs.

Public outreach

In addition to wanting to take advantage of the system's benefits as quickly as possible, MDT sought a smooth transition to the new way of paying fares. "We took the customer support in-house," says Kapoor. "We used our staff. Outreach was done by our marketing department in connection with Cubic."

MDT took responsibility for teaching customers how to use the new cards, tickets, fare boxes, turnstiles and readers, and the effort succeeded, Kapoor says. For starters, users can call for help by dialing a phone number printed on the back of tickets and passes. The staff compiles a list of the top five concerns and takes action in response, he says.

Web traffic reveals that few riders are reporting problems. Of 92 million hits on the MDT site where riders can load value onto the cards and tickets, only 3,700 visits involved inquiries or complaints, Kapoor says. “Basically it’s less than .04%,” he says of the hits that indicated problems.

“I give credit to my marketing staff,” Kapoor says of the customer-training effort. “They led the whole outreach effort passionately and took every complaint seriously. When we had issues, we adjusted right away.”

The 65,000 passengers who take the MDT trains each day are regular customers who adapt quickly to fare-collection changes. They do not represent as big an outreach challenge as the 250,000 who catch the buses each day and may be the occasional rider, Kapoor says.

To reach both types of passengers before the launch and during the early days of the new system, MDT positioned staff members at the gates and at machines to assist with the new cards, says Clinton B. Forbes, senior executive assistant at MDT. A “soft launch” on Sept. 18, with the new cards and tickets, gave the staff time to deal with glitches and helped riders get used to the new system.

MDT gave away half a million plastic EASY cards before the launch, Forbes says, to help acclimate customers to the new system in advance.

The cards cost $2 each and last three years, while paper EASY tickets have no extra fee and have an expected life of 30 days or less. The cards and tickets all contain microchips and antennas, says Cubic’s Brunner. Cubic typically charges transit authorities $2.49 each for the cards he says.

Online passengers can buy or reload cards and tickets, check the balances on their cards or sign up for a service that automatically deducts fares from another payment card, Brunner says. Employers can use another site to manage the transit benefits they provide their workers, he adds.

MDT buses have new fare boxes that accept cards, tickets, coins and bills, says Brunner. In the rail system, the gates accept only cards and tickets. Vending machines at the rail stations accept coins, bills, credit cards and debit cards and more than a hundred convenience and grocery stores sell and reload cards and tickets.

Going live

Finally, the sun rose on Oct. 1. Early that morning Forbes stood on a platform at Dadeland South Metrorail Station, one of the busiest points in the transit system, prepared to witness the new fare-collection system in action.

“We have buses that come into that station and unload 60 to 70 passengers at a time,” Forbes says. “This is the first time folks are going to have to use the new fare media in order to get to the gates. Is the system going to work?”

He watched anxiously as a busload of passengers “seamlessly” disembarked, walked into the station, tapped their cards and entered. “It was a beautiful thing to see,” he recalls.

MDT gave away half a million EASY cards before the launch to help riders learn about the new fare collection system.

Have you gained access to
Biometrics Certification?

Fingerprint scanners on handsets enable apps

Can biometrics help launch mobile payment in U.S.?

For the first time, a mobile phone with a fingerprint biometric scanner is arriving on U.S. shores.

The LG eXpo is being offered in the U.S. by AT&T and in Canada by TELUS, says Art Stewart, vice president of mobile systems products at Authentec, a Melbourne, Fla.-based provider of fingerprint scanners.

While this may be revolutionary in the U.S., fingerprint scanners on mobile devices aren't new in many countries. Authentec has provided more than 10 million scanners for 20 different mobile phones since 2003, says Stewart.

The LG eXpo features an Authentec fingerprint scanner that can be used for authentication, replacing PINS and passwords with a fingerprint swipe. The fingerprint recognition also complements the touch screen user interface providing precise cursor control for text editing and rapid browsing.

Initially the fingerprint scanner enables user authentication and can be used to protect specific files, explains Stewart, but other applications are in the works. Eventually users will swipe and have a login and password entered for access to specific Web sites, he adds.

This model of device security first and other applications second, has worked in the past. In Japan, for example, the fingerprint scanners were first used to secure mobile devices and later payment functionality was added.

Sony's FeliCa contactless technology is widespread in Japan with millions of individuals using mobile devices and contactless cards to enter subways and make purchases, Stewart says. On mobile devices, individuals swipe a finger over the scanner to authorize the payment or fare collection application on the phone.

It seems that the launch of applications beyond device security is key.

There are 8 million phones in circulation that can use biometrics for payments, Stewart says, adding that outside of Japan mobile payment has yet to really take off. Using fingerprint scanners for security or convenience hasn't been enough to drive wide-scale deployment.

But Stewart is optimistic. He cites that mobile payment is growing in the U.S. and so is the need for easier navigation of screens on mobile devices. The need for fingerprint scanners, too, he predicts will continue to grow. ID

Mexico deploying multi-modal biometric ID

Mexico plans to start enrolling 110 million citizens into its national ID card program this summer. The program will be among the first to capture iris, fingerprint and facial biometrics for identification, says Terry Hartmann, vice president of identity solutions at Unisys.

Unisys' Mexican subsidiary was awarded a contract by the Mexican Ministry of Internal Affairs and National Citizen Registry to create and manage the biometric-based citizen identification solution.

The agency will issue another tender for companies to compete for the ID card issuance portion of the project. The country expects to issue cards to citizens over the course of three to four years.

Unisys is charged with setting up 3,000 enrollment centers as well as adding enrollment capabilities to existing government facilities, Hartmann says. Some of these enrollment systems will be portable, suit case style systems.

The multi-modal nature is what makes Mexico's program different from others out there, Hartmann says. "It's essentially the first national identity system that will capture iris and use it," he says.

Mexico hasn't had a national ID system before, though the country's voter ID card has used to identify citizens.

While the card technology to be used for the national ID has not been determined, Hartmann says, "there is a very good chance it will be a smart card because they will want to use biometrics for identity verification."

Exactly how the card will be used has yet to be worked out either, Hartmann says. Similar programs around the world use biometrics for voter registration and even financial transactions. "The card isn't only for identification, it could be a driver licenses, used for collection of tolls, a travel card and even an ATM card," he says.

Unisys is seeing a lot of interest in Latin American and Asia in new national ID projects or upgrading existing projects, Hartmann says. "It's mainly in the countries that don't have a national ID or don't use biometrics with that ID … they recognize the problems with identity fraud," he says.

ID

SARGENT®

ASSA ABLOY

Come Face to Face with the Future of Security

SARGENT introduces Access Control Solutions that you'll want to take notice of: the Profile Series v.S1 and v.S2 IP-enabled locks. Both provide connection to your existing network using non-proprietary and industry-standard equipment, reducing cost and easing installation.

The v.S1 lock communicates to the access control system on your LAN using Power over Ethernet technology, requiring only an Ethernet cable for data and power. The v.S2 WiFi lock talks to your access control system using an existing 802.11b/g wireless network, dramatically reducing installation time, and providing security in remote locations.

For more information, visit us at www.sargentlock.com or contact your local ASSA ABLOY Door Security Solutions representative.

ASSA ABLOY, the global leader
in door opening solutions

Breaking down business cases for NFC

Banks, telcos, TSMs ...
Who will get paid
in the NFC ecosystem?

Autumn C. Giusti
Contributing Editor, AVISIAN Publications

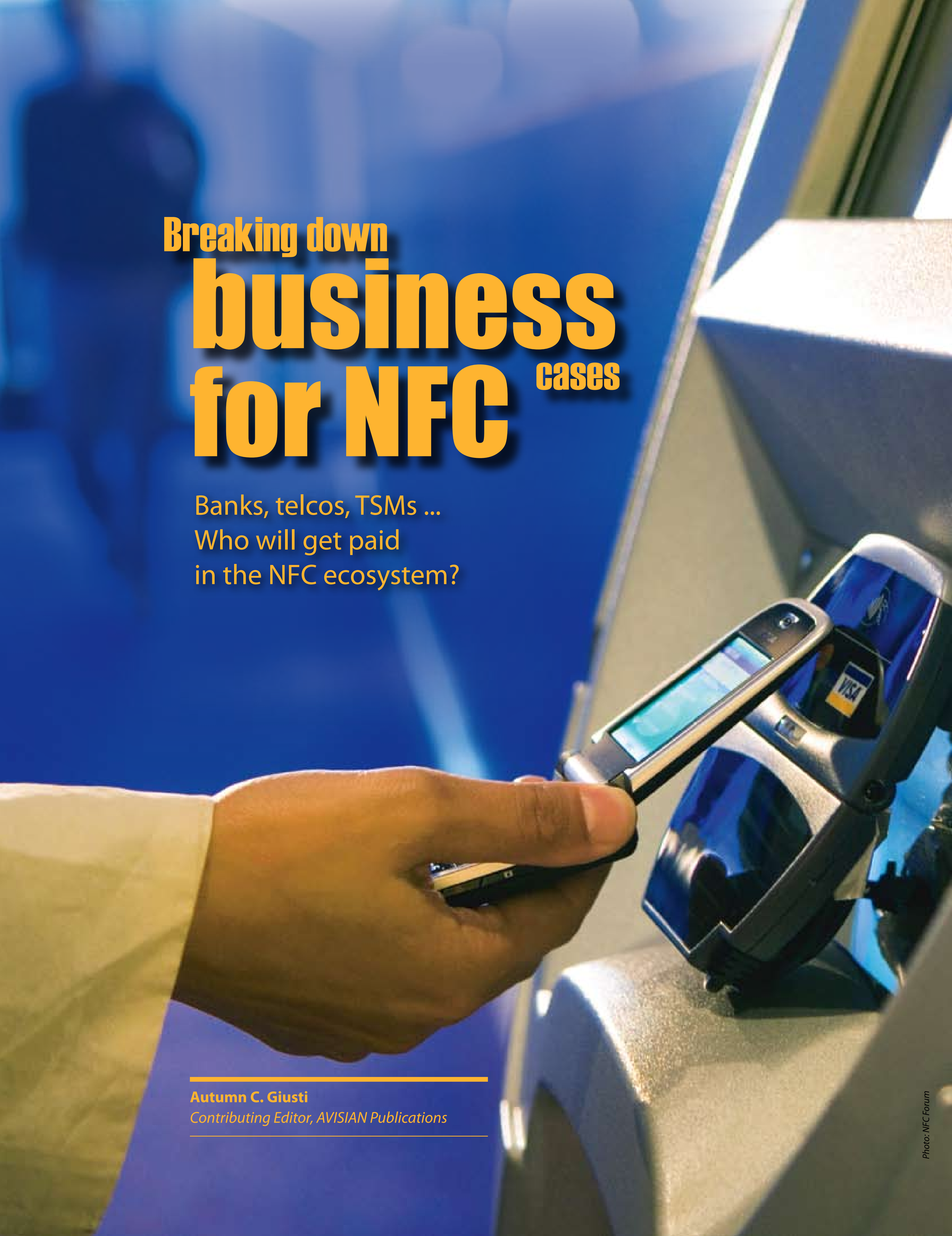


Photo: NFC Forum

Will that be Visa, MasterCard or iPhone?

That's the question banks and cell phone companies are hoping to hear more of in the next few years as the contactless payment world prepares to make the leap to near field communication (NFC).

Near field communication is a technology that would enable people to make purchases or ride the subway with a wave of their mobile phones. The technology is beginning to take hold in Japan and South Korea, and trials have taken place around the globe. Analysts believe NFC could start appearing in U.S. markets before the end of 2010 and could reach critical mass in the next two to three years.

But as with anything else hitting the market, someone needs to make money off it for it to be viable. Unlike most new forms of technology that require only a single company to apply it, there are multiple players involved with NFC – financial institutions, mobile operators, merchants and other stakeholders. Thus its business model is a bit more complicated.

The question comes down to who will make the first move. "I see a lot of opportunity … it's a matter of who wants to pick this up and go for it," says Stephen Ezell senior analyst with the Information Technology and Innovation Foundation in Washington, D.C.

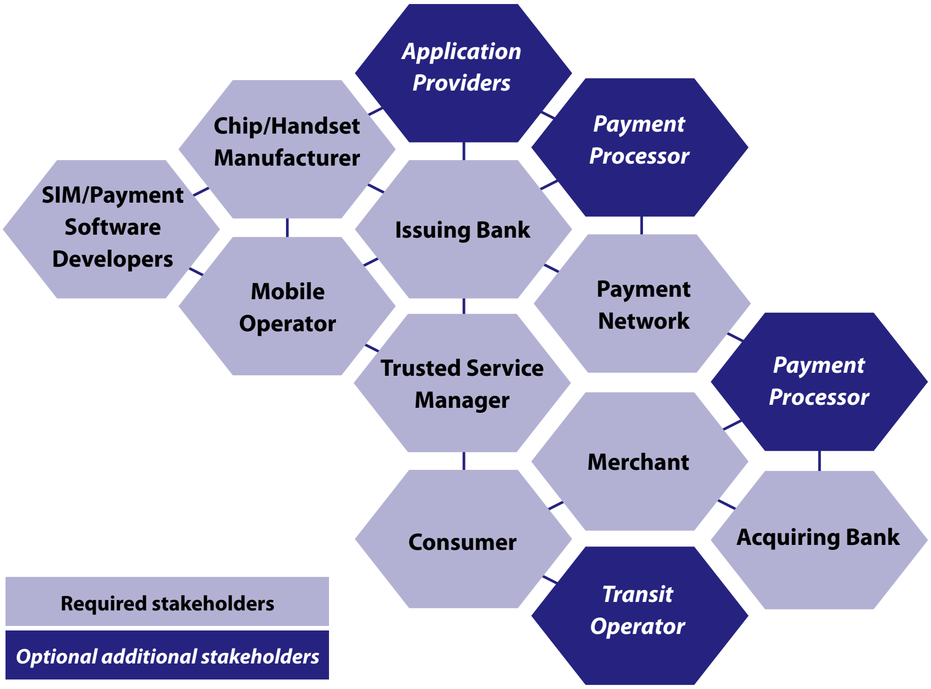
How it works

One of the main selling points of NFC is that it could eliminate the need for banking customers to carry around a stack of credit cards. Loading a payment application, customers would have all the capabilities of a contactless payment card on their mobile phones.

"We know from our primary research that consumers are more likely to leave home without their wallet than without their phone. So it's more convenient to have a payment device built into the phone," says James Anderson, vice president for mobile product development at MasterCard. Anderson also sits on the board of the NFC Forum, an organization developing standards for near field communication.

In 2008 ABI Research forecasted that there would be 100 million mobile phones with NFC by the end of 2010 and 292 million by 2012. "This is a technology that is available glob-

At least nine stakeholders may cooperate in the mobile payments ecosystem



Charts: Smart Card Alliance

ally, but because there are substantial differences between markets in the United States versus Japan and Europe, how it gets implemented is going to vary region to region," says Randy Vanderhoof, executive director of the Smart Card Alliance.

Business models explored

There are multiple parties looking to make money off NFC technology, primarily mobile companies and financial institutions. "Figuring out who's going to bear the freight and who's going to be a free rider is one of those classic geekonomic problems," Anderson says.

A report by the Smart Card Alliance explores four possible business cases: one where the mobile companies take the lead, one led by the banks, a peer-to-peer model – using a third party such as PayPal – and a collaborative model.

In the survey 86% of participants supported collaboration, meaning all of the stakeholders would need to work together and figure out how to share the revenue. "There's a big banking ecosystem, a big payments ecosystem and a big mobile ecosystem. Those parties historically haven't worked together, so we've got a lot of learning to do about each other," Anderson says.

Through the collaborative model, the merchant fees would most likely be split between banks, mobile operators and possibly third-party stakeholders.

Vanderhoof says one way for the mobile operators to make money is by renting out their phones to financial institutions and charging them a fee to post a Visa, MasterCard or other payment application on the phone. The mobile companies could also charge customers a fee for every purchase made with the phone.

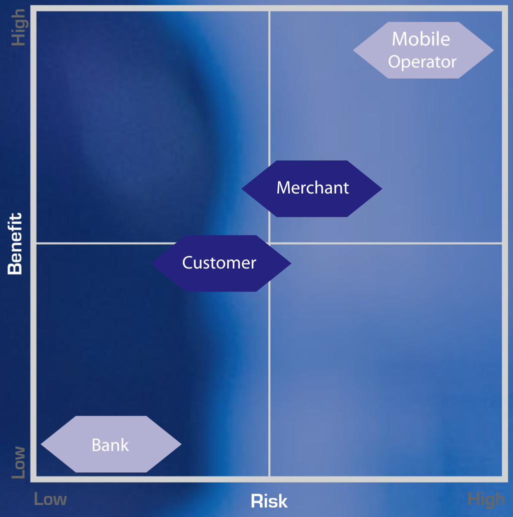
Another potential revenue source for the mobile companies involves charging customers higher fees for the amount of data they use on their phones. Mobile handsets would also be able to receive promotions, coupons and other marketing messages, either from a retailer or from a mobile company.

Once phones are outfitted with NFC capabilities, the question remains as to who pays for the hardware. In the U.S., mobile companies typically subsidize some of the cost of the handset under their service contract. But that could change with NFC. Analysts say it's uncertain as to whether mobile operators will continue to pay the full subsidy, or if customers or other stakeholders will have to ante up for NFC capability.

Risks & Benefits for NFC business case options

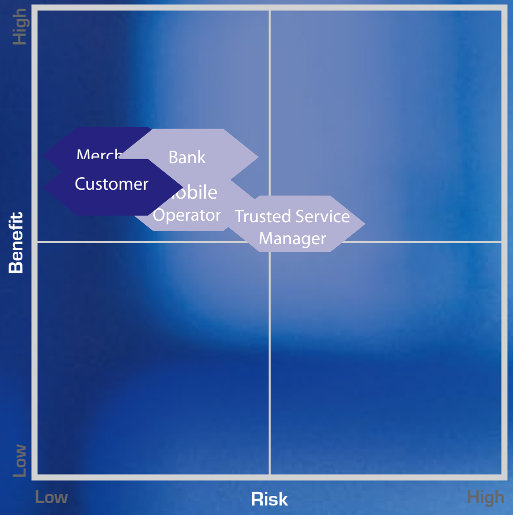
Operator-centric model

The mobile operator acts independently, taking on the responsibility of financial institutions either by providing merchants with a wireless POS system or by signing people up for credit card accounts on their phones.



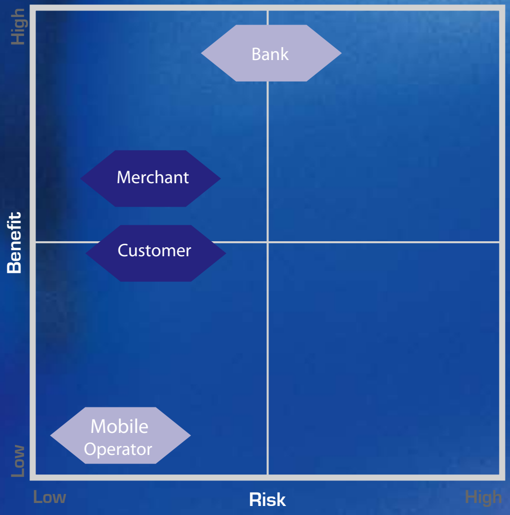
Collaboration model

This involves collaboration among banks, mobile operators and other stakeholders. A mobile operator would either partner with a bank to offer a payment service, or industry associations representing these two parties would negotiate and set standards for mobile payments apps.



Bank-centric model

The bank is responsible for getting NFC-enabled phones to customers. Essentially, instead of distributing payment cards to customers, they would be distributing mobile devices and apps. The bank's role in this model can range from giving customers a phone fully outfitted with NFC to simply adding a payment application to the customer's current phone.



Charts: Smart Card Alliance

A third party to secure the transaction

Linking NFC-enabled phones to payment networks opens a new door for potential security breaches, and thus, some analysts suggest a third entity may need to come into the picture – the trusted service manager (TSM).

A TSM would serve as an intermediary that secures financial data transmitted between the banks, the merchants and the mobile device, says Ray Wizbowski, director of marketing and communications for Gemalto, a digital security company that has participated in several NFC pilot programs worldwide.

Wizbowski says most of the pilots that have succeeded involved a TSM. One such pilot took place in Paris, involving eight banks and three mobile operators. Gemalto was the TSM for seven of the eight banks.

The benefit of putting payments on secure mobile devices is that banks would save money on acquisition fees, which run from $25 to $250 per account. When banks mail credit cards to customers, 64% of those cards are never activated, Wizbowski says.

But if a TSM secures a mobile phone, the bank could virtually eliminate acquisition fees by issuing a payment card application directly to the customer's phone over the air. Instead of having to call an 800 number to activate a card, the customer would enter an activation code directly into his phone.

"You go from having a 36% to a 100% activation rate," Wizbowski says. "You're suddenly seeing a larger cost savings because you don't have as many calls going through a call center."

Testing the market

While about 50 NFC pilot programs have taken place worldwide, few have been able to implement a full NFC ecosystem.

Japan has had widespread success with its NTT DoCoMo and FeliCa program, as has Spain with its MobiPay trial. Both of these NFC projects involve mobile companies essentially operating as banks. But these pilots operate under an economic infrastructure and circumstances that are very different from North America.

In the United Kingdom, credit card company Barclaycard and mobile operator Orange UK announced plans in the first quarter of 2009 to launch a fully-integrated NFC platform with the goal of having widespread adoption in 2012.

Sprint and AT&T have been the most active mobile operators in terms of U.S. pilots. In one pilot program in Atlanta, audience members at an Atlanta Hawks basketball game were provided handsets they could use to make purchases and download promotions within the stadium.

MasterCard has also been working on trials worldwide. "Trials are very good about testing out technology, but you can't get real numbers until consumers start changing their behavior," Anderson says.

Building an ecosystem

For NFC to succeed widespread, the infrastructure must be in place for its use. That means merchants will need to have contactless card readers in place. "The problem in the U.S. is that customers have few places where they can go

The same readers that accept current contactless payments can also accept NFC, so the merchant infrastructure is already being deployed.

to use an NFC-enabled phone so they're not going to use it, and retailers aren't going to sell it," Ezell says. "The question is how do you resolve that paradox and bring the market closer to fruition?"

Helping to address the need, the payment industry has been deploying contactless terminals across the U.S. and around the globe. Because the same reader that accepts current contactless payments can also accept NFC, this portion of the hardware infrastructure is experiencing a significant boost.

MasterCard has been rolling out contactless payments in more than 30 countries and has 174,000 merchants with contactless readers, Anderson says. "We're ready on the acceptance front to have a merchant be ready to accept contactless payments on the phone," he says.

The bigger hurdle is that mobile phones enabled with NFC also need to be ready and widely available.

One way to get the ball rolling could be through use of a sticker or tag, a contactless payment card that can be physically adhered to a phone. "It's essentially taping a credit card to a handset," Wizbowski says.

Analysts acknowledge this would be a transitional form of the technology but could help change people's purchasing habits. They also offer the potential to put a relatively large number of NFC cards into the hands of customers and see how they're put to use.

"One of the very important things for a business model discussion is that the parties in those discussions have to have numbers they feel confident about to justify their investment. And I think that's where things like tags can be helpful," Anderson says.

Where NFC is headed

While analysts expect NFC technology to hit U.S. markets later this year, they don't expect widespread use overnight.

"There's going to be some lag between seeing how well those devices work and how well consumers respond to them," Vanderhoof says. "Then you'll see the rest of the market start to move at the same pace and probably make incremental improvements over what the early adopters delivered. From a timing standpoint, that's going to take 18 to 24 months from when we see the first solution being tested in the market."

Another challenge comes from the fickle nature of mobile customers, who have unique features they like about their phones. "To reach a mass market it's going to take mobile operators making NFC available across multiple platforms to satisfy all of their different customers," Vanderhoof says.

And fine-tuning the business model for NFC will factor into how quickly the technology takes hold.

Photo: MasterCard

NFCNews @ GSMA MOBILE WORLD CONGRESS

EnStream launches Zoompass mobile wallet for Android phones

Canadian mobile commerce company EnStream LP launched the Zoompass mobile application for Android powered phones, enabling users to send money securely to friends and family via the smart phone.

Zoompass users can also import existing contacts directly from their address book, load and transfer money directly from their bank account or credit card, and check account balances and view transaction history.

EnStream launched the Zoompass mobile application in Canada in 2009, but up until now it has only been available for Blackberry and iPhone smart phones.

Common Zoompass uses include splitting a lunch bill, requesting sports team fees, or collecting money for a group gift or to pay a housekeeper, babysitter, etc.

Gemalto, HighCo partner for NFC-based mobile coupons

Gemalto announced a partnership with HighCo, a marketing solutions provider for mass-market retailers and consumer goods manufacturers, to launch mobile coupon services using NFC technology.

According to Gemalto, the goal of the partnership is to provide a more convenient way of collecting and redeeming coupons from NFC phones.

Using an application in the mobile phone, users can connect to HighCo's server, then select and download mobile coupons onto their handset, where they are stored locally in the SIM card.

The coupons are automatically redeemed at the point of sale, where the contactless terminal communicates directly with the application stored in the SIM to find the right coupon used for the purchase. All the user has to do is wave their phone at the reader.

NFC payments trialed at Mobile World Congress

At this year's Mobile World Congress in Barcelona, GSMA, Samsung, Telefonica and Visa, with Giesecke & Devrient, Ingenico, ITN International and La Caixa, collaborated across industries to give Congress attendees an opportunity to experience SIM-based NFC mobile payment.

The participating companies provided more than 400 NFC handsets to guests for use at the Congress. The Samsung Star NFC handsets contain Telefonica SIM cards from O2 pre-loaded with 60 euros of airtime credit as well as a La Caixa Visa Mobile Payment Application.

Participants used their NFC phones to pay for food and drink at more than 30 merchant locations around the Congress. Purchases in excess of 10 euros require a pass code, which the participant keys into the handset before presenting it to the terminal. The transactions are authorized online with funds deducted from a La Caixa Visa account.

According to GSMA, the goal of the pilot was to raise awareness of NFC technology in anticipation of the commercial launch of SIM-based NFC handsets.

MicroSD phones become payment devi

A new payment solution combines Visa's contactless payWave technology and DeviceFidelity's In2Pay technology. It transforms mobile phones with microSD memory slots into mobile contactless payment devices, enabling consumers to make transactions at any retail location accepting contactless payments.

Visa's global transactions processing network, VisaNet, and its contactless payment technology are designed to securely process transactions initiated with the In2Pay solution, providing real-time fraud monitoring and encryption technology that work together to prevent counterfeit fraud.

The In2Pay solution conforms to the industry standard for microSD cards and integrates with multiple mobile phone operating systems, according to Visa. In2Pay uses an onboard software controlled antenna and an industry standard dual interface contactless smart card chip t Visa payWave, as other contactless app such as transit, identi and access control.

In addition to DeviceFide ity, Visa is also working with technology providers and alliance partners, including CPI Card Group, Inside Contactless, Monitise plc, and NXP Semiconductors. Trials are scheduled to begin in the second quarter of 2010.

Colorado town leading the way with contactless payments, rewards

Ed McKinley
Contributing Editor, AVISIAN Publications

Los Angeles dazzles, New York overwhelms and Chicago gets the job done on broad shoulders. But don't look to America's urban behemoths for the latest in payments technology. Tiny La Junta, Colo. – until now known mainly for melons, corn and cattle – is becoming one of the nation's first hotbeds of open-loop, community-oriented, rewards-based wireless debit payments.

Some 500 customers of The State Bank of La Junta automatically debit their checking accounts when they tap their cell phones on dedicated readers at more than 50 participating businesses in and around La Junta. Their town, a county seat of 8,000 residents far from the ski slopes and in the middle of relatively flat southeastern Colorado, could become a model for the nation, observers say.

A contactless chip in a Bling Nation sticker attached to their cell phones exchanges radio signals with the reader to pay for anything from a steak at Boss Hogg's Saloon, a trim at the I Need Fabulous salon or a fill-up at any of the area's five Tank N Tummy C-Stores.

Bling Nation authenticates the transactions over cell phone networks, eliminating steps that accompany more usual debit card purchases. No major card brands get involved in the authentication, so more money stays in the pockets of La Junta shoppers and merchants instead of electronically flying off into the coffers of Visa USA in San Francisco or MasterCard Worldwide in Purchase, N.Y.

But don't get the idea the State Bank's Redi-Pay Bling is just another pilot. The bank, merchants and townspeople are committed to the convenience, consumer rewards, low merchant fees, tight security and community spirit of wireless debit payments, says Brad Rose, a State Bank of La Junta vice president and IT security officer. The bank's rivals are getting ready to offer the tags, too, Rose says, helping to make La Junta ground zero for the spread of wireless debit payments.

The birth of Bling in LaJunta

State Bank heard about Bling Tags in December 2008 from Rose's brother, who was operating a micropayments company for digital media. That prompted discussions with Wenceslao Casares, a founder, director and co-CEO of Palo Alto, Calif.-based Bling Nation. State Bank began the Bling Tag project in earnest in February 2009 and began offering the tags to the public three months later, Rose says.

Casares explains that State Bank became the first paying customer for Bling Nation, which began pitching the system to bankers in 2007. Before the bank signed on, the vendor had tested the scheme in Palo Alto with Facebook employees serving as customers and several local restaurants accepting the tags.

E-mail alerts and anti-fraud procedures built into the Bling Nation system captured Rose's imagination. "When I heard about the security features on the Bling tag, I just fell in love with the product," Rose says. Any time a transaction breaches security parameters set by the bank, the system rings the account holder's cell phone. When that call comes, the user enters a PIN number to complete the purchase. If the correct PIN isn't entered, the transaction is not allowed.

La Junta, Colo. – until now known mainly for melons, corn and cattle – is becoming one of the nation's hotbeds of open-loop, wireless debit.

Triggers include exceeding a set dollar amount in a single transaction, which State Bank established at $1,000; making more than a specified number of purchases in a defined time period; making total purchases of more than a set amount during a designated period; and making the 20th purchase at a single business, says Rose. Fewer than 5% of transactions require customers to enter their PINs, says Casares. In the first 25 days of November 2009, for example, State Bank's 500 Bling Nation accounts set off triggers just 32 times, Rose says.

Convincing those 500 customers, nearly half of the bank's 1,100 checking account holders, to attach the self-adhesive, postage-stamp-sized Bling Tags to their phones represented a victory for the bank, Rose says. To start that effort he himself photographed and narrated a video of a trip to the town's Fox Theater to show how the tags worked. The theater shows the video before feature films, and it's available for viewing on the bank Web site.

Postcards and statement stuffers meant to explain the tags failed to make much of an impression with account holders, according to Rose. From what he could determine, recipients simply glanced at the printed materials and tossed them into the trash or the recycling bin.

However, word-of-mouth brought success. First, State Bank executives briefed the tellers on the tags. Then, the tellers urged merchants to encourage shoppers to convert to the tags. Soon the bank began reaching its goals, he notes. "We went from 50 to 500 consumers very quickly," he says.

Generous rewards drive usage

To help motivate townspeople, the bank and participating merchants are cooperating to underwrite rewards points valued at 3% of the purchases made with the tags. So a carpenter who buys a $100 miter saw at Ranchers Supply Co. earns enough points that he can then walk into the Barista coffee shop and buy a latte for points alone.

To help motivate townspeople, the bank and participating merchants are cooperating to underwrite rewards points valued at 3% of the purchases made with the tags.

The tags, about the size as a quarter, may serve as a predecessor to phones with built-in near field communication capabilities.

Merchants can add to the 3% rewards built into the system and they might do well to consider that option because the current system is proving too generous to last indefinitely, Rose says. For every $50 spent with a tag at one local bar, for example, the customer receives a $5 discount on the next visit. "More and more merchants are looking at rewards on top of the 3%," he notes.

Bling Nation helps consumers keep track of the of the points flowing in and out by sending an electronic receipt to their cell phones for every transaction, Rose says. The receipts come as SMS text messages that note the number of points accumulated, where the points were obtained and the cash balance available in the checking account, he says.

Consumers also notice the quickness of the Bling Nation transactions, says Rose. Visa and MasterCard purchases can take 20 to 30 seconds when they require signatures, he claims, adding that the Bling procedure does not even require a paper receipt because it includes the electronic record on the shopper's cell phone.

The look of the tags can heighten their popularity, too, and the State Bank tags come in "several flavors," says Rose. Customers can state their politics by choosing a tag configured as a peace sign, demonstrate their loyalty to the local community by carrying one that says "Shop La Junta," or promote the bank by using one with the financial institution's mascot, a caricature of a railroader named "Redi," that bears the slogan, "Redi to Make a Difference."

State Bank still hopes to win over another couple of hundred tag converts at the main bank in La Junta and its branch about 15 miles away in Rocky Ford. The bank intends to extend the project this year to its other branch in the town of Falcon. The bank has determined the tags do not bring in new accounts, however, and thus decided to drop its claim to geographic exclusivity for the payment system.

One competing bank plans to introduce the tags in the first quarter and another is in talks with Bling Nation and intends to enter the field when the technology matures, Rose says. "There has been somewhat of a halo effect," observes Casares. Merchants and then bankers have started to notice in towns near La Junta, and Rose has introduced it to bankers who have approached him, he says.

Merchant fees and terminal deployment

Before consumers can use the tags frequently enough to make them worthwhile, however, the State Bank had to achieve critical mass among local merchants willing to accept the payments. The bank began with a test at the Copper Kitchen and Wallace Oil Co. Both businesses were included in discussions with Bling Nation and quickly embraced the system, Rose says, noting that, "merchants don't have anything to lose by going on it."

In fact, merchants pay lower fees to Bling Nation than to the major card brands. At the 2% to 3% rate that Visa and MasterCard typically charge merchants, the merchant's fee would come to $2 to $3 on a $100 transaction. The same transaction costs shopkeepers $1.33 with Bling Nation, Rose says. For a $1,000 purchase, the major card brands might assess a fee of $20 to $30, while Bling would charge the same $1.33, he continues. Bling Nation fees typically amount to 15 cents on purchases of $5 to $25, 30 cents on those of $25 to $75, 50 cents on purchases of more than $75 and a top rate of $1.33, Rose says.

Bling Nation fees vary for different types of merchants but all fall within four tiers, Casares says. A written explanation of the pricing system requires just half a page and is much simpler than the Visa and MasterCard pricing schedules, he says. Bling Nation often posts payments to merchants' accounts on the day of the transaction, according to Rose.

The Bling process requires its own terminals, which Bling Nation provides to merchants free of charge, says Casares. The only wiring the terminals, or "Blingers," need is a power cord to an electrical outlet. Batteries keep the terminals working during power outages and also empower the wait staff at La Junta restaurants, such as the Gold Panner Café and Thyme Square, to take payments tableside, says Rose.

The tags may serve as a predecessor to phones with built-in near field communication capabilities that perform a host of functions, says Casares. "It may just happen sooner than people expect with some open architecture phone just throwing a contactless chip in there and letting developers do whatever they want with it," he adds.

This year, however, Bling Nation is limiting its growth by adding just one bank a month to its network despite increasing interest, Casares says. By starting small, the company can choose only banks that will benefit greatly from the tags, he says. Moreover, slow growth will give Bling Nation time to learn the intricacies of differing financial institutions, divergent local cultures in small towns and big cities, and changes in seasonality and geography that can affect marketing.

Through it all, State Bank has led the way, Casares says. "We have calls from banks on both coasts now, but it's because they called this community bank in La Junta first," he says. Bling Nation foresees a growth path with increasingly larger banks in ever-larger cities. In Colorado, for example, the company could work its way up to Denver by signing up more banks, merchants and consumers ever closer to the region's big city. The growth would continue until, "you have a blanket of merchants around the Denver area that makes it compelling for a large bank to launch there," he says. ID

3D photo technology for secure driver licenses

Cindy Alexander
Identity Solutions Manager, MorphoTrak

Three-dimensional photo technology strikes the delicate balance necessary for driver licenses between ownership, privacy, ease of enrollment and cost. This technology provides a first-line security feature that is obvious at a glance and simple to validate.

Laser-engraved 3D portrait technology is difficult to counterfeit and inherently establishes ownership between the ID and its rightful owner. The method used to validate the 3D photo security feature is clear and performed intuitively by examining the image. It is intrinsic to the person being identified and integral to the card structure.

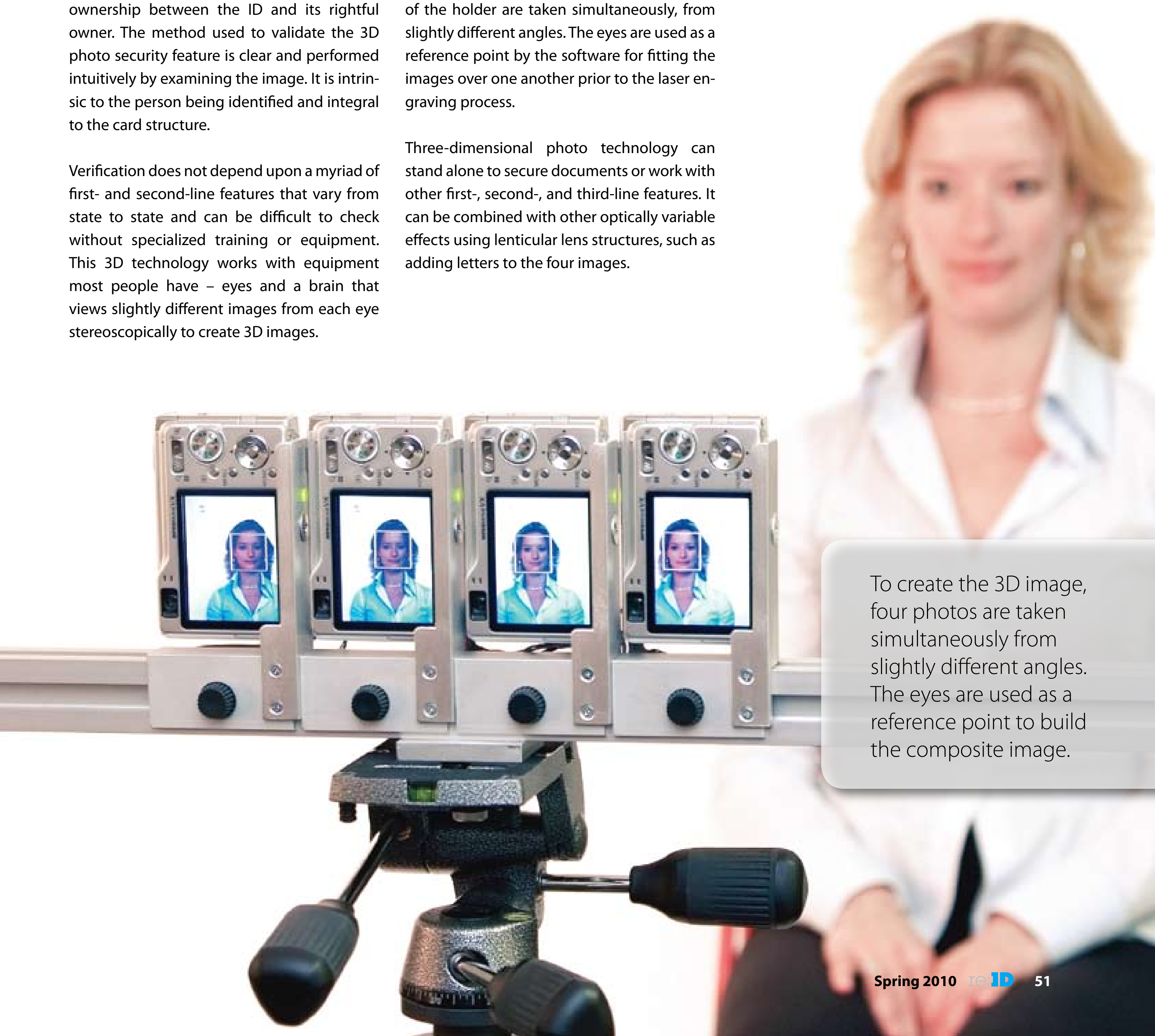
Verification does not depend upon a myriad of first- and second-line features that vary from state to state and can be difficult to check without specialized training or equipment. This 3D technology works with equipment most people have – eyes and a brain that views slightly different images from each eye stereoscopically to create 3D images.

Cardholder privacy rights are enhanced with a known and obvious feature – photos – available on all driver licenses. 3D photo enrollment is as simple, fast and non-invasive as typical photo capture and offers the advantage of using low-cost, off-the-shelf components.

To create a high quality three-dimensional image of the license holder, four photographs of the holder are taken simultaneously, from slightly different angles. The eyes are used as a reference point by the software for fitting the images over one another prior to the laser engraving process.

Three-dimensional photo technology can stand alone to secure documents or work with other first-, second-, and third-line features. It can be combined with other optically variable effects using lenticular lens structures, such as adding letters to the four images. The letters appear to “float above” the card surface while the photograph “sits beneath” the surface. Since both these first-line features are easily recognized, they add further ID security while staying consistent with established industry practice.

Read the full article at *SecureIDNews.com*, search term “3D photo”



To create the 3D image, four photos are taken simultaneously from slightly different angles. The eyes are used as a reference point to build the composite image.

Trojans have found vulnerabilities to one-time password tokens and could also be used against biometric and smart card technology.

— Avivah Litan, VP & Analyst at Gartner Research

Report: Problems with some two-factor authentication

Most agree that using two-factor authentication for access to secure networks is better than simple user names and passwords, but a report from Gartner Research states that hackers have found ways to compromise these more advanced systems as well.

Trojan-based, man-in-the-browser attacks have found vulnerabilities to one-time password tokens and could also be used against biometric and smart card technology, says Avivah Litan, vice president and analyst at Gartner Research. A layered security approach can help protect individuals from these kinds of attacks.

The attack occurs when a user unknowingly downloads a malware program. The application sits in a user's browser until they log into a banking Web site. At that point the user name, password and one-time password information is transmitted to the criminal and the legitimate user receives an error message stating that the system cannot be accessed. Meanwhile the fraudster is using the information, complete with a valid OTP, to drain the individual's bank account.

Other malware will overwrite transactions sent by a user to the banking Web site with the criminal's own transactions. "This overwrite happens behind the scenes so that the user does not see the revised transaction values," the report states. "Similarly, many online banks will then communicate back to the user's browser the transaction details that need to be confirmed by the user with an OTP entry, but the malware will change the values seen by the user back to what the user originally entered. This way, neither the user nor the bank realizes that the data sent to the bank has been altered."

The criminals have also figured out a way to defeat out-of-band authentication methods such as phone calls. The fraudster simply asks the carrier to forward calls to another number citing issues with the line. Phone carriers do not always properly verify an identity before forwarding calls, the report states.

In order to prevent fraudsters from gaining access to the account information there are a number of steps financial institutions and individuals can take.

Banks should use fraud detection systems that monitor a user's behavior. These systems can review a user's Web history and navigation to determine if the user is a person or a piece of malware. One European bank had success with this method. "The bank found that once inside the account, the Trojans generate transactions much faster than a legitimate human user does. For example, it takes a normal human user 10 to 20 seconds to enter a money transfer amount and press 'okay' to confirm it, but the Trojan entered the same type of data and confirmation in under one second."

Banks should also use fraud systems that monitor for odd transaction behavior, the report states. The issue here is that some transfer activity, such as ACH withdrawal, is structured, while other activity, like wire transfer is unstructured. "A fraud prevention application can determine the payment and payment beneficiary data in an ACH money transfer request so that it can spot that the amount or beneficiary is 'unusual' and suspect. In contrast, wire transfer instructions are unstructured in part, and transfer instructions can be documented in textual comments. In order for a fraud prevention application to work in this case, it must be able to parse textual comments and isolate the important data."

Litan notes that out-of-band authentication requests can also be used to protect transactions, but they need to be used properly. This channel should only be used for verification of high-risk transactions.

"Enterprises also need to use out-of-band communication providers that can prevent the enterprise's calls from being forwarded to phone numbers that the enterprise has not registered and vetted for a legitimate user account," the report states. "Alternatively, the enterprise can simply terminate any calls that are being forwarded to another number (as a cautionary measure), and ask the user to call the bank instead."

ID

2005 2006 2007 2008 2009

re:ID
Authentication
the chain of trust
FIPS 201
NFC
THE COMING STORM
SECURING IDENTITY in an online world
Airport IDs: Grounded ... or ready for take off?
ID industry fights Big Brother image
HACKING IDENTITY
Next generation access cards do more than access
CONVERGENCE!
IDENTITY and the ELECTION
DIGITAL IDENTITY The forces are aligning but is America READY
Identity takes on GLOBAL SIGNIFICANCE
BEYOND ISSUANCE... e-passports struggle to achieve usage
Changing Perspectives? NATIONAL IDs
AVISIAN

OWN THE ENTIRE COLLECTION

1000+ pages of ID technology insight just $200

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

For the first time, AVISIAN is offering all back issues of their industry-leading *re:ID magazine* in a packaged set. You receive three year's worth of top-notch news and insight – 15 issues of *re:ID* and 6 issues of *CR80News magazine*. Plus you get password-protected access to our online library with more than 1000 feature articles.

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

AVISIAN

Tokens becoming more popular on mobile devices

Separate hardware no longer needed for two-factor authentication

Meredith Gonsalves
Contributing Editor, AVISIAN Publications

In a digital age where more people are succumbing to the smart phone phenomenon and the desktop computer has become a thing of the past, the online world is literally at our fingertips. Technology has revolutionized the way the online market place conducts business and in turn enabled consumers to operate within this marketplace with ease and convenience.

Never again will an individual have to wait to access a computer to manage their bank account, access an office file or make a purchase on EBay. These functions are available on a variety of smart phones sweeping the nation including the popular iPhones and Blackberries. However consumers and enterprises have found that this convenience comes with a price. Security breach and identity theft pose even more of a threat now with increased accessibility to online networks.

Individuals no longer have to carry around a separate token because the software is embedded in the smart phone.

User names and passwords, as well as other forms of single-factor authentication, are fraught with issues but security companies have struggled to deploy easy ways for consumers to achieve higher security. Two-factor security – something you have in addition to something you know – has commonly been used by corporations to protect network access.

The second factor has traditionally been a one-time password (OTP) token that generates a random key to be entered along with user name and password. Today these separate hardware tokens are being replaced by software loaded on to mobile devices like iPhones and Blackberries. The software works the same as the hardware token with the device generating the random number or OTP.

Companies – such as RSA, Verisign and Vasco – that traditionally sold the hardware tokens are beginning to offer the software for mobile devices.

The infrastructure that would enable a consumer to use these two-factor authentication for access to bank accounts or retailers isn't in place. A study by Javelin Strategy showed weak customer satisfaction with the hardware token. "We consistently found hardware tokens ranked at the bottom of the list. From a customer standpoint, they simply found it ineffective," said Robert Vamosi, fraud and security analyst at Javelin.

The new software token is said to eliminate some of the cost and convenience concerns. Individuals no longer have to carry around a separate token because the software is embedded in the smart phone. Vasco, VeriSign Technologies and RSA have each released a software-based technology for mobile phones. Javelin Strategy recently rated VeriSign's VIP Access and RSA's SecureID systems "Best in Class" for authentication technology. Both companies have claimed that this development has changed the way consumers use two-factor authentication security.

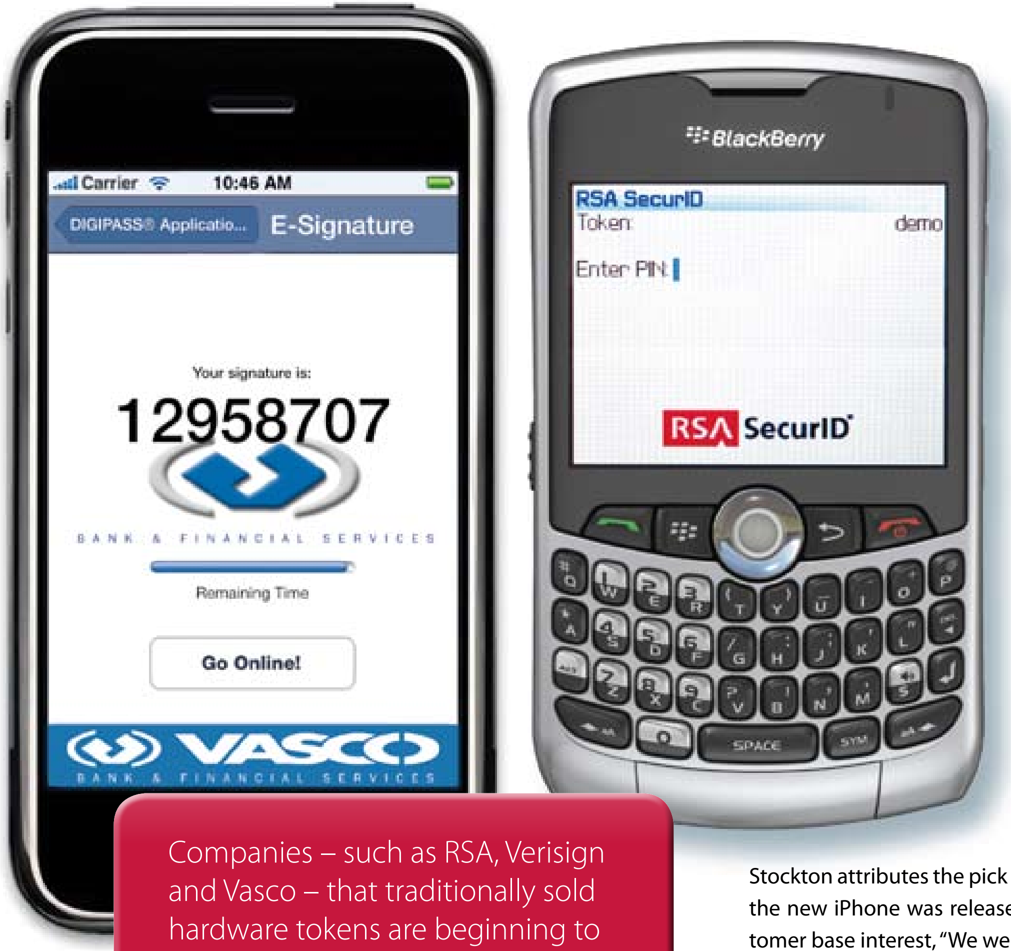
"People love the merging of the two devices. The great thing about [the software token] is that it is connected to something you have every day, your phone," said Rachael Stockton, principle product manager at RSA.

How it works

OTP systems require two components: the credential that consists of either the hardware token or an application stored on the phone and the back end system that validates the credential.

The end user registers the credential with their username and password within the enterprise. When the end user accesses an application, he or she provides the username and password along with the one-time passcode from the credential.

USER:
PASSWORD:
OK
User name:
Password:
System Log In



Companies – such as RSA, Verisign and Vasco – that traditionally sold hardware tokens are beginning to offer software for mobile devices.

After entering the passcode into a site, it's checked against the back end system to determine if access should be granted or a transaction approved. The back end systems need only validate the second factor – thus it can be an anonymous service that has no personal information or username/passwords.

The mobile software token consists of two parts: the physical application that is downloaded to the smart phone, and the "seed" or power behind the application. The seed generates a new pass-code every 60 seconds without worry or bother to the user. "You can have a case where a user isn't even aware that the software is working for them because there is no typing involved, " said Kerry Loftus, vice president of authentication at VeriSign.

In addition, the seed enables the software to be re-accessed in the event that the phone is lost or broken. Compare this to the hardware token where if lost, a user would have to purchase a new one. This software token requires a one-time purchase upon downloading along with a yearly service fee, however RSA and VeriSign claim overall cost will decrease because there is no cost of hardware replacement.

The seed in both the VIP Access from VeriSign and SecureID from RSA has embedded all the functionalities of the hardware token, so the level of security is the same. The added convenience of software however, has mainstreamed the product. Enterprises that originally used the hardware token now see the value in migrating to the software tokens, according to VeriSign. Alternatively both VeriSign and RSA have experienced companies who were initially turned off by the cost of the hardware token but are now interested in utilizing the software token.

"Originally we saw popularity among the service industries: consulting, accounting, law and financial institutions. Then the health care and pharmaceutical industry showed interest. Now we find it to be horizontal, where everyone is beginning to use the software," said Stockton.

An increasing number of enterprises are using blackberries and iPhones as business tools and are therefore looking to accommodate these newer devices while maintaining the security of their existing systems.

Stockton attributes the pick up in sales to the smart phone craze. When the new iPhone was released RSA saw an immediate reaction of customer base interest, "We were getting calls from existing and potential customers asking if the iPhone would support SecureID," said Stockton.

This expansion has made it easier to apply these tokens to a variety of mobile systems, and therefore reach a much larger consumer demographic.

When it comes to reaching the general consumers, a study by Javelin Strategy found that customers rated the two-factor authentication technology the most effective security solution, 14% saying it would increase their online shopping. Javelin Analyst Vamosi said, however, that in order for the system to take off validation from a big player like Amazon for instance, would be necessary to mainstream the software token.

Stockton agreed saying that the mobile token will really increase Web purchases if given the option by more and more retailers.

Vamosi says it may take sometime for widespread adoption of the product, "it is kind of like PayPal where it existed for a while and then took off after big players implemented it."

It is the usability and convenience of the mobile token that has attracted the positive response, and the popularity of the smart phones that have broadened the interest among new industries and consumers. The deployment of tokens on mobile phones enables users to passively protect their secure information when banking, shopping or conducting business online, on a device that no one leaves home without. ID

What POWERS Your Campus?

Contactless technology from Blackboard Transact™ is ready to power faster, safer and more convenient transactions at forward-thinking institutions everywhere. Around the clock, our clients manage transactions in dining halls, bookstores, vending machines, and more. They use our technology for privilege verification, door access, video surveillance, and even managing the crowd at the big game. Now, they can do it faster and more securely than ever before.

Let us show you how you can achieve the system performance you expect and the user experience your students demand from a name you can trust.

www.blackboard.com/contactless

Blackboard transact™

Your campus. Connected.

Will your next card include a display, battery, or button?

John Elliott
Head of Public Sector Practice & A Principal Consultant, Consult Hyperion

We at Consult Hyperion have spent a lot of time considering the technology developments that will allow chip cards to realize their full potential in the next few years.

The most obvious differences in this area will be in the card displays, which are hardly used at all on smart cards at the moment. Broadly speaking, this change will fall into two categories: Emissive technologies and Reflective technologies. Thanks to developments in both of these areas, we expect that color "e-paper" will be available within the next two to three years and that video-capable reflective displays will be available within the next five years.

As technology continues to evolve in the area of power consumption, batteries will also become a lot thinner, with the only real barrier being the trade-off between battery size and capacity. Suppliers are already targeting the ID1 card form factor market, since battery capacity is increasing so as to enable better support for emissive display technologies.

For greater security, biometrics will also begin to feature more in the next wave of card technology. By using a smart card chip to perform on-card biometric matching, terminals will be able trust both the card and the cardholder – without the need to access an online biometric database. To support this technology, cards could soon feature a flexible display interface that includes a fingerprint swipe reader.

Another key area for change will relate to energy-harvesting technology and rechargeables, with breakthroughs expected in areas such as the ability to recharge wirelessly, or by using movement, light or temperature effects. Recharging via USB may also be an option. This kind of energy-harvesting technology, especially when combined with printable batteries, will in turn lead to a variety of efficient charging mechanisms for the consumer. At the same time, environmental issues will increasingly play more of a role in product choice for a growing proportion of customers.

Organics will also begin to make the headlines in the next few years. Organic electronics have a number of advantages over silicon, including printable connections and more flexibility. They are also thinner, lighter, more environmentally friendly, and offer a long-term price advantage. For all of these reasons, we predict that organics will soon be passing silicon as the method of choice for producing low-cost electronics.

Means of data input will also see some new options in the coming years, including printed buttons or areas that use resistive or conductive touch. Although some may wonder about the costs associated with this kind of technology, the incremental cost of a single printed button will be insignificant with regards to long-term production costs, especially in comparison with processing, display and power components.

'Wait a minute!" I hear you cry, 'A smart card with a display and buttons? Isn't that what I call a cell phone?' It will be interesting to see whether smart applications shift inside the handset before these new card technologies gain a foothold.

Clearly, there are potential barriers to many of these developments. Cost is always an issue, as is size, since the technology will need to physically fit into the envisaged payment form factors. And what about durability? Will the technology survive everyday customer use? Are the power consumption requirements realistic for a three-year lifetime product? And to what extent can the technology be exploited using existing standards and infrastructure?

All of these are valid questions, and will need to be addressed, but in the meantime we need to maintain a "watching brief" on these developing technologies, and to conduct deeper research into tactical opportunities to gain a better understanding of the target markets and likely costs. At the same time, companies who don't want to be left behind will need to start organizing their business models to ensure that they are best positioned to exploit the strategic opportunities made available by these new and exciting technologies.

Emissive displays
As the name suggests, they emit their own light and thus can be viewed in dark conditions. Examples include televisions and computer monitors.

Reflective displays
They do not produce their own light, but rather reflect external light to illuminate the display. Like paper they rely on ambient light and thus cannot be viewed easily in dark conditions. Examples include many wristwatches, e-readers and the original Nintendo Game Boy.

Photo: Display card with Aveso display

Biometrics and payment card security

These and more top 2010 list of security trends

Ross Mathis
Contributing Editor, AVISIAN Publications

In predicting the security forecast for 2010, there will be a noticeable increase in the utilization of biometrics and cloud computing environments, says Terry Hartmann, vice president of identity solutions at Unisys. Increasing the security of credit card information and mobile transactions will also be a major issue.

Led by the Asia-Pacific region and Europe, more than sixty countries have invested in the electronic passport infrastructure, issuing passports containing a chip to store an individual's biometric data, typically a photo and a fingerprint. However, Hartmann points out only five countries are actually reading the information from the biometric chip to verify that the person who the passport is issued to actually matches the traveler crossing the border.

"In 2010, a lot more countries will pilot, investigate, and look at verifying electronic passports," says Hartmann.

More countries are also issuing biometric-enabled identity cards. Taking these cards into the streets and other remote locations, will in turn, increase the demand for mobile biometric devices. These mobile devices permit a country to take biometric-based critical services directly to citizens, rather than requiring citizens to come to the technology.

Police forces in Australia are already using mobile fingerprint scanners to access the national fingerprint database from the field. Officers cross reference with the criminal database and search for a match. In the future, these devices will also aid in the identification of individuals in disaster situations when time is critical.

Taking it to the clouds

Organizations will begin to reduce the tendency to protect everything, instead prioritizing security controls based on whether the data presents low, moderate or high levels of risk.

"Cloud computing can allow customers to make a number of cost savings as they run their operations," Hartmann says. "2009 was the year of people becoming aware of cloud computing."

In 2010, organizations will begin moving less sensitive public data into cloud environments. They will attain these cost savings and follow with migrating more sensitive data into the cloud, as new security models are tailored to address the increasing levels of data sensitivity.

Securing card and mobile transactions

Hartmann predicts there will be tougher standards and policies to combat credit card fraud in coming year. "At the moment, in the U.S., we are pretty lax in regards to how we handle credit cards."

On the back of a credit card is supposed to be a handwritten signature of the owner – a biometric linking the owner to the card itself. "However, nobody actually checks that," says Hartmann.

He predicts more implementation of EMV to ensure that both online and face-to-face transactions are performed by the actual owner of the credit card.

Hartmann states this system will be primarily pushed by consumer demand. "People travel to Europe and Asia-Pacific where these extra levels of security are already established, they are surprised that these types of controls are not already set into place in the United States."

The demand for security platforms and anti-fraud applications need to be strengthened and updated regularly, to ensure the protection of mobile transactions. As more employees and consumers use smart phones to conduct business dealings online, organizations will look for new ways to protect its data beyond simple PINs and passwords.

"For a lot of people, your cell phone is a biometric – you're uncomfortable if it's not around. It's a part of you. You'll notice you've lost your cell phone before you've lost your credit card."

Sesames winners announced

Annual competition is among the most prestigious recognitions for excellence in the identity and security industry

Hardware: F@CIL

The winner for best hardware was awarded to Gemalto, Leti and Raisonance for their contactless smart card reader called F@CIL. Building on existing standards for data rates up to 848 Kbps, the new reader promises 10 Mbps secure transfer for contactless smart cards. F@CIL encompasses all levels of implementation including physical, protocol and tools for test and verification.

For the best Software the Sesames was awarded to Sagem Orga for its T2TIT (Things to Things in the Internet of Things). The project defines and standardizes an architecture that enables communications between a Web portal and other objects. This project focuses on the treatment of the mobility and the privacy of these objects.

The architecture offers a secure way to have RFID tags authenticated by a server while maintaining full privacy. Sagem Orga worked together with Telecom, Paris Tech, LIP6 and CNAM to develop the communication protocol HIP-TAG, which uses cryptography to secure connections and guarantees anonymity and non-traceability.

Mobile: MASSIM

For the best mobile application the winner is Gemalto for Massim. The MASSIM project targets a new field of application where the M2M/UICC is plugged into electrical/gas metering equipment enabling the service to identify the subscriber through network access. MASSIM, which stands for M2M Anti-Stealing SIM, is a machine-to-machine SIM card that detects theft or removal.

Once installed, the card automatically detects and registers its location. If removed and inserted into a mobile phone, it will immediately alert the service provider of the change in location via SMS. At that point the service provider is then able to take all necessary actions, such as blocking the card.

Transit: eO

ERG Transit System's eO was awarded the Sesames for best transit application. eO is an open account-based fare collection system. Developed with the Utah Transit Authority, eO enables transit agencies to focus on moving people rather than managing cards. Readers accept contactless bank cards as well as ISO 14443 and ISO 15693 cards managed by third parties like local ski resorts, universities and employers.

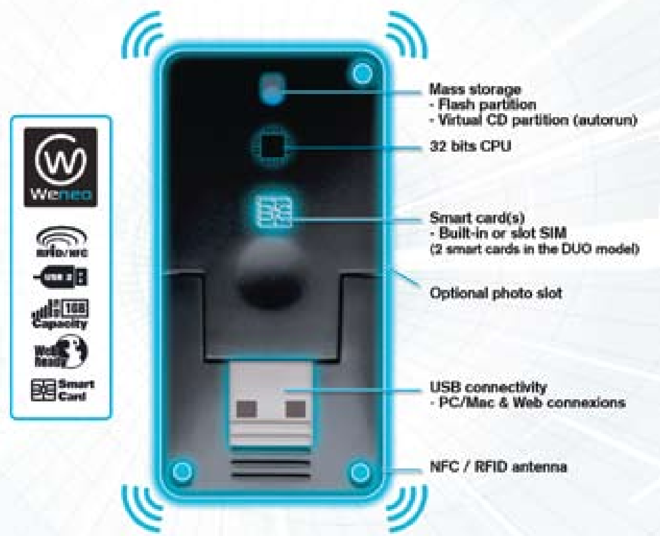
An on-bus router communicates through WiFi, 3G or GPRS with a real time validation server, seeking rider authorization or denial. If communications are delayed, lists of registered cards and bad payment cards are created and later updated to a database, reducing the opportunity of fraud.

The eO system handles on-the-spot authorization and settlement. Device status can be monitored remotely along with maintenance records and updates.

IT Security: Weneo ID

For the best IT Security application the award went to Neowave for its Weneo ID Corporate Bundle. The Weneo ID is a smart object for the corporate enterprise offering logical access control, physical access control, payment and ticketing.

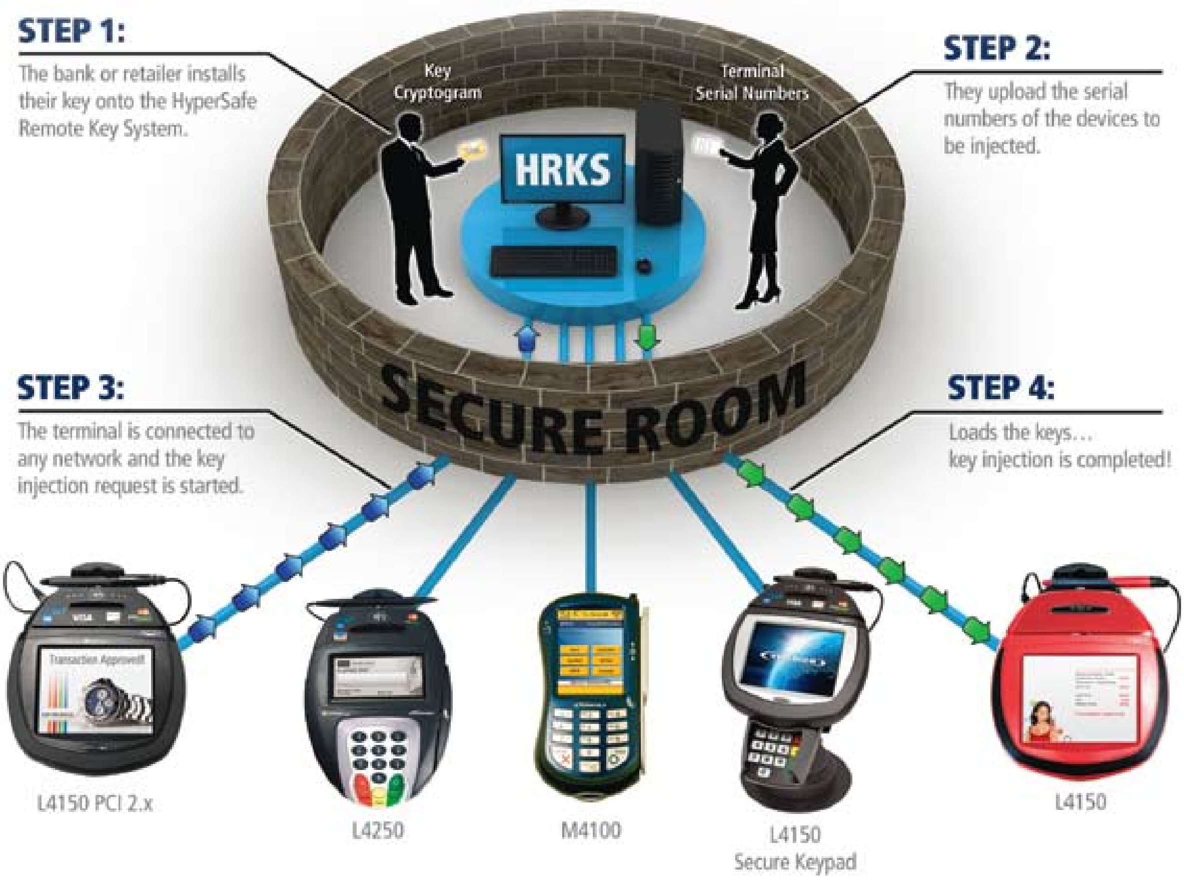
Neowave's Weneo smart objects blend the security provided by smart cards with he benefits of USB keys and NFC/RFID contactless connectivity. Each token combines a contact and contactless JCOP smart card chip with up to 1 GB of flash memory for personal productivity. As an additional safeguard, each can have a photo or company logo added.



Banking, Finance, Retail: HyperSafe Remote Key System

The winner for the best Banking/Finance/Retail application is Hypercom for its HyperSafe Remote Key System. HyperSafe is a standards-based solution for "injecting" acquirers' symmetric keys into point-of-sale terminals in non-secure, remote environments. With this system, PIN encryption keys can be remotely downloaded to the POS terminal at the merchant location.

Offering a fast and secure alternative to the industry's traditional secure room key injection process, the system eliminates the need for off-site secure room key injections by incorporating Public Key Infrastructure to securely distribute symmetric 3DES keys. This means retailers no longer have to ship their terminals to third party secure facilities for time-consuming key injections.


STEP 1:
The bank or retailer installs their key onto the HyperSafe Remote Key System.
Key Cryptogram
Terminal Serial Numbers
HRKS
STEP 2:
They upload the serial numbers of the devices to be injected.
SECURE ROOM
STEP 3:
The terminal is connected to any network and the key injection request is started.
STEP 4:
Loads the keys… key injection is completed!
L4150 PCI 2.x
L4250
M4100
L4150 Secure Keypad
L4150

Loyalty: Smart Lumière

The best Loyalty application Sesames was awarded to Oberthur Technologies for its Smart Lumière. Smart Lumière is Oberthur's light-card technology. Available in either dual interface or pure contactless configuration, Smart Lumière emits light when in the field of a contactless reader to tell the cardholder when the transaction is processing.

Smart Lumière is composed of a translucent plastic core, antenna and illuminating light apparatus to offer applications in the payment, loyalty, prepaid and transport markets.

For the card issuer, the color and sequence of the light sources, including the design of the card itself is customizable. Smart Lumière's illuminated visual cue helps industries reinforce trust in contactless as a secure, convenient and rapid way to pay.

Health care: eHealth-Portal

Gematik took home the award for the best health care application. The company's eHealth-Portal authenticates patients for access to online Web health-records including health data, medical history, prescriptions, and insurance status. It uses smart cards on the client side, without requiring plug-ins, drivers or other support generating tools.

Smart cards maintain basic patient data, insurance status, and a photograph. A set of emergency health data is also included if the patient agrees to have it added to the card.

e-Transaction: Sign4Pay

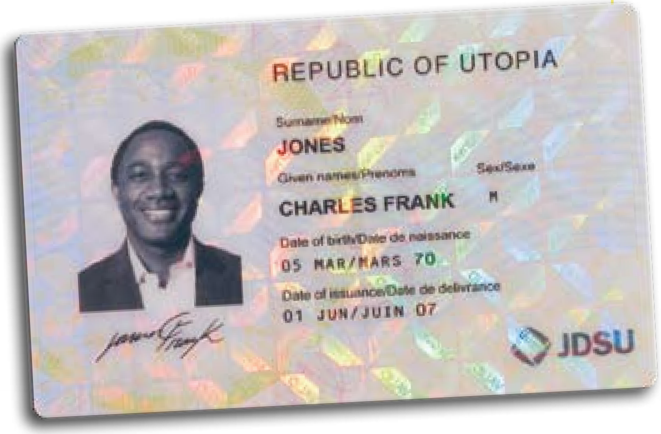
The Sesames for best e-transactions application was awarded to Monext for Sign4Pay. Sign4Pay is a new payment method using WPKI services and infrastructure enabling a user to conduct secure online transactions. This product turns a SIM card associated with an electronic ID into a secure payment tool and makes payment easier by eliminating complicated 3D-Secure payment steps.

A message is sent to the user's mobile phone asking for validation of the transaction by entering the user's secret SIGN-4PAY code. Once the transaction has been validated by mobile phone, the payment is completed in total security.

Identification: HoloFuse

The best identification application was awarded to JDSU for HoloFuse. HoloFuse integrates high-security demetalized holography with clear polycarbonate eliminating the need for adhesives when applying holograms to ID documents. The partially transparent and customized hologram within the polycarbonate film includes overt, covert and forensic security features that make it difficult to reproduce.

Without the need for adhesives or hot stamping, HoloFuse integrates the hologram, into the polycarbonate film itself. This in turn becomes the clear outer layer of identity documents. This reduces the ability of counterfeiters to separate card layers and tamper with security, and also simplifies the manufacturing process for card and identity document makers.



Applications being added to ID cards demand more from printing software and hardware

Jonathan Bowen
Product Manager, Digital Identification Solutions

The vast majority of ID cards in circulation a decade ago were used primarily for access control and time and attendance. Most had encoded magnetic stripes or printed barcodes that referenced a record in a database. The advent of proximity cards and contactless cards gave administrators an option to move to a touch-less interface resulting in greater security and eliminating mechanical card readers in favor of solid-state readers.

Today contactless smart cards such as MIFARE, iCLASS, DESFire, LEGIC, and FeliCa are gaining greater acceptance because they offer higher levels of card security and the ability to support multiple applications. Some can even store digital certificates to replace your user name and password for network logon.

Growing pressure from governance, risk management and compliance (GRC) is causing organizations to rely on the card for more than just access. But using cards in this way places new demands on administrative and security departments as well as their systems.

To meet these demands, administrators are looking for solutions that do more than issue a card that provides access to doors. Products that integrate with the HR system to make enrollment easy and provide tools to manage the lifecycle of the credential are growing in popularity. To reduce the high costs and security risks associated with managing IDs, administrators are drawn to products that provision a user's rights or access to other systems, and just as importantly can be used to remove a user from multiple systems.

Web-based systems that provide simple interfaces for users and administrators make deployment easy and provide global access to the system. By tying the ID management system into other systems like access control, parking, vending and even an organization's directory service provide administrators with the maximum control from one single interface.

Options like automatically encoding contactless cards and loading digital certificates are becoming central to the card issuance process as administrators rely on the card to do more. Web portals for user self-services are reducing the administrative manpower required to manage cards and the systems they access. They accomplish this by enabling cardholders to request updated credentials or access privileges.

As advanced technology cards become more prolific, administrators are increasingly motivated to upgrade their printing technology. Contactless cards and cards with contact chips have surfaces that are more difficult to print than yesterday's magnetic stripe cards. Additionally, the higher cost of these cards encourages issuers to look for solutions that minimize damage to cards during printing. Less waste means more money.

Added to this is the desire to encode cards during the print process so that the card is ready to issue once it ejects from the printer.

A key solution to these challenges can be found in modern retransfer card printers. Retransfer printers print the card's images and text on clear polyester film, and then bond this film with the card body. This all but eliminates the challenge when printing on technology cards.

Many of the new generation of retransfer printers also offer inline encoding easing the workload and streamlining the issuance process. Offering inline encoding while protecting the card from damage is the best of both worlds.

With advances in manufacturing technology and a growing demand in the commercial sector, the entry price to retransfer technology is becoming more attractive, making it an attainable option for even low to mid volume issuers. This "perfect storm" of benefits is driving the interest in retransfer technology higher than ever before. ID

ETHERNET
DS
EDIsecure
ILU
XID
590ie
digital identification solutions
digital identification solutions

Retransfer printers print the card's images and text on clear polyester film, and then bond this film with the card body. This all but eliminates the challenge when printing on technology cards.

Newly approved FIPS 201 products

Research detailed product listings and compare different vendor offerings online at FIPS201.com, the most robust source for FIPS201, HSPD-12, ISO 24727 and PIV products and services.

Caching Status Proxy
PIVCheck Plus Desktop Edition
PIVCheck Plus Mobile Edition • *Codebench*

Card Electronic Personalization Device
ActivID CMS for PIV • *ActivIdentity*

CHUID Authentication System
PIVCheck Desktop Edition • *Codebench*

CHUID Card Reader (Contact)
IDL MAX • *MaxID Corp.*

CHUID Card Reader (Contactless
IDL MAX • *MaxID Corp.*

Electromagnetically Opaque Sleeve
Rigid Shielded Badge Holder
Vinyl Shielded 2-Card Holder
Shielded sleeve • *Brady People ID / JAM*

Cryptographic Module
nShield F2 1500e
nShield F2 500e
nShield F2 6000e
nShield F3 1500e
nShield F3 500e
nShield F3 6000e • *Thales e-Security, Inc.*

PIV Authentication System
PIVCheck Desktop Edition • *Codebench*

PIV Card Printer Station
ZXP Retransfer Card Printer • *Zebra*

PIV Middleware
Smart Security Interface • *Charismathics*

SCVP Client
PIVCheck Desktop Edition • *Codebench*

Template Generator
BioMatch 378 Generator v2.1 • *Precise*

Template Matcher
BioMatch 378 Matcher v2.1 • *Precise*

Transparent Card Reader
Multi-Tech Wallmount Reader
Multi-Tech Wallmount RS485 Reader
Single-Freq Mid-Range Keypad Reader
Single-FreqMid-Range Readee • *XceedID*
SCR3500 USB Smart Card Reader • *SCM*
ACR3801 Smart Card Reader • *ACS*
LifeBook T5010 w/ integrated O2Micro SmartCard Reader • *Fujitsu America, Inc.*

CardProtectors™

Brady People ID

Visit us at ISC West Booth 23101

The new Made in the USA CardProtectors from Brady People ID protect personal information on contactless ID cards, credit cards, or debit cards. A layer of shielded material protects a card against unauthorized or unknown access to valuable information. There are 3 types of CardProtectors: Rigid Shielded Vertical, Vinyl Shielded Vertical and Shielded Paper. For more information about these products, visit www.bradypeopleid.com, email bradypeopleid_sales@ bradypeopleid.com or call 800-528-8005.

E-Plex 5800 Series

Kaba Access Control

The E-Plex 5800 Series FIPS 201 Locks and Stand-Alone Access Controllers (SAC) are the only stand-alone products listed on the FIPS 201 APL. The E5800 series works with TWIC, PIV, CAC NG, FRAC and other FIPS 201 interoperable credentials. Like all other Kaba E-Plex card-based products, the E5800 Series Locks and SACs offer the convenience of Kaba's new LearnLok™ feature allowing up to 300 FIPS 201 cards to be enrolled at the lock's reader without the use of software for basic access control. For management of up to 3,000 users per door and more advanced security features, optional software may be used.

VISIT FIPS201.COM TO RESEARCH AND COMPARE APPROVED PRODUCTS

Smart Card Alliance

Highlights of the 2010 Smart Card Alliance Annual Conference

- Standalone event – a return to the independent smart card industry conference prior to CTST co-event partnership
- Targeted content – focused on core identity management and authentication across payments and security markets
- Great networking – meet with other industry leaders in a social setting to share cutting edge information
- Informal breakout sessions – smart card implementers discuss the challenges they overcame and how they succeeded
- Expanded exhibits – leading companies showcase the latest smart card-related identity management solutions

May 17 – 20, 2010 • Marriott Camelback Inn Resort & Spa • Scottsdale, AZ

The **2010 Smart Card Alliance Annual Conference** is back again, returning to the original successful format as an independent, standalone conference after two years partnering with the CTST Conference. The Annual Conference returns to one of its most popular locations from past years – the **Camelback Marriott Resort and Spa in sunny Scottsdale, AZ, May 17 - 20, 2010**.

Join us for what the **Smart Card Alliance** does best – bringing experienced smart card practitioners and suppliers together with innovative solutions developers and end users. Network and share information on smart card-based identity management and authentication for the payments and security markets. Come and enjoy the best that the smart card industry has to offer.

www.SmartCardAlliance.org • 1-800-556-6828

NFC enables communication from beyond the grave

Visiting gravesites to remember loved ones after they have passed away is a tradition for many families. But as the years go by remembering those individuals can be difficult. But no longer with RosettaStone.

The product from Phoenix-based Objecs LLC places a near field communication (NFC) chip into a granite or travertine stone that can be used to launch text about or images of the deceased. If a visitor doesn't have an NFC-enabled phone, Web-enabled devices can be used to display the information by entering a unique ID. The company is limiting the information to pictures and text, with no plans to add video.

The chip in the stone doesn't actually store the information but instead acts as a pointer, says John Bottorff, owner of Objecs. The idea came out of a project Objecs did for a Portuguese tourist attraction that communicated information about military graves to visitors.

Research into the memorial market in the U.S. showed bar codes being used, but these required a user to download specific software to a mobile device, Bottorff says. While RosettaStone requires an NFC-enabled device, it doesn't require any additional software.

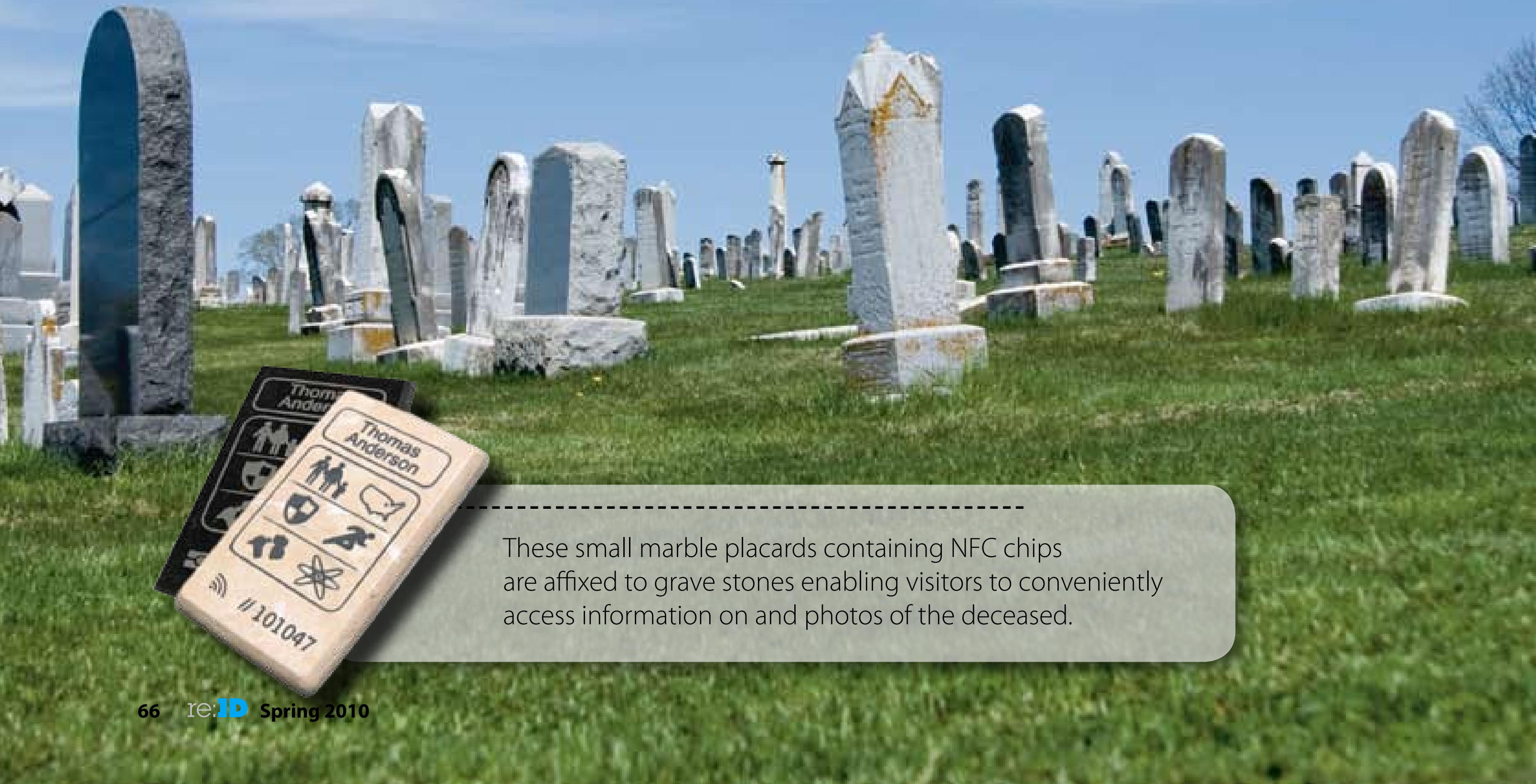
The front face of a RosettaStone has engraved hieroglyphic symbols, called Life Symbols, that an individual selects during the order process from a list of options that best represents your key life associations. Symbols represent being family status, career path and hobbies.

Setting RosettaStone apart from other memorial tributes is its long-term data archive strategy, says Bottorff. The company's solution is to mitigate this risk by sharing master copies of data file elements within a business-to-business data archive network. If one network business fails the data survives in another master copy. Some sites act as a single custodian, which may put the data at risk if the site goes out of business.

Green burials

The RosettaStone also fills a market niche for those wanting a green burial. These ceremonies consist of an ash spreading service or the individual being buried in a pine box with no headstone. The travertine marker can be used as a memorial gift for loved ones to remember the departed. The granite marker is designed to be attached to a headstone and could last as long as 3,200 years.

ID



These small marble placards containing NFC chips are affixed to grave stones enabling visitors to conveniently access information on and photos of the deceased.

Smart Guardian

The most secure device to protect your data on the go

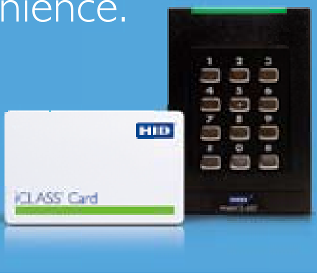
Use your device with any pc or mac • Zero footprint plug and play • Centralized deployment and administration • Eliminate data leakage through unauthorized portable media Zero footprint plug and play • Secure your files on the go • Centralized deployment and administration • 2GB and 4GB configurations • Zero footprint plug and play Up to 4GB of personal flash storage • Smart card based alwa [illegible] tion • Centralized deployment and administration • 2GB and 4G [illegible] Secure remote ac [illegible] of corporate resources • Smart ca [illegible] tion Eliminate da [illegible] rough unauthorized port [illegible] ase ROI • Sec [illegible] f corporate r [illegible] gh unauthorize [illegible] igital signat [illegible] te access of corporat [illegible] ate data le [illegible] able media • Digital signatures t [illegible] • Sma [illegible] tion • Zero footprint plug and play • Centra [illegible] eployment [illegible] ons • Smart card based always on encryption • Zero footprint plug [illegible] zed deployment and administration Zero footprint plug and play • Smart card based always on encryption • Secure remote access of corporate resources • Eliminate data leakage through unauthorized portable media • Work from where you are with secure remote access Secure remote access of corporate resources • 2GB and 4GB configurations Data locked by smart card encryption • Digital signatures to increase ROI • Secure remote access of corporate resources • Eliminate data leakage through unauthorized portable media • Secure remote access of corporate resourc [illegible] Digitally sign files for convenience Eliminate data leakage through unauthorized portable media • Smart card based

Protect what's yours

Secured by
smart card

www.gemalto.com/enterprise/smartguardian

gemalto
security to be free


HID
iCLASS Card