State of the Market: Access Control

Smart cards, especially the new PIV-I card, managed access, and NFC all stand out in the 2012 access control market.

By Heather Klotz-Young, Senior Editor

For years, the physical security industry has predicted the "tipping point" in the video surveillance market as the point in time when Internet protocol (IP) video will outsell analog video. But are you paying attention to the other tipping point? Yes, access control has a tipping point of its own — the point when smart cards will outsell legacy cards.

ABI Research, New York, estimates that about 1.5 billion smart credentials will be issued through 2014. ABI Research analyst Phil Sealy predicts, "We expect smart card-based government and healthcare ID products to catch up with and surpass shipment volumes of legacy credentials by 2013."

Over the past several years, smart card adoption has grown in many sectors, but none more so than the federal government. Since the Homeland Security Presidential Directive 12 (HSPD-12) in 2004 mandated the Personal Identity Verification (PIV) card to establish a common, interoperable smart credential, more than five million PIV credentials have been issued to government employees.

As it has grown, the PIV initiative has attracted a great deal of interest from parties outside the federal government wanting to issue identity cards that are technically interoperable with federal government PIV systems and also can be trusted by the federal government. This interest has resulted in the "Personal Identity Verification Interoperability for Non-Federal Issuers" or PIV-I card, which allows those parties outside the federal government to be able to issue smart card credentials that are either interoperable or compatible with government-issued PIV credentials.

"One of the trends that we are seeing is organizations outside the federal government using the government standards and looking at PIV-I so they can have a more secure credential," says Geri Castaldo, chief executive officer of Codebench, Coconut Creek, Fla. "Organizations in the private sector are using the government standard so they don't have to start from scratch. We're really seeing it starting in the banking sector. Here is a market sector that doesn't have to comply with the standards but is

Accessing the 'Green' Side of Access Control

There is a natural connection between energy management and access control. A key area of energy management is the connection between energy consumption and occupancy. Access control systems provide the data that building automation systems need to manage energy usage.

"Access control itself, unless you power it with renewable energy like solar panels or wind energy, is not doing much with sustainability. But the richness of the information that an access control system contains can be vital for all the elements of building automation, energy management and conservation. An integrated access control system itself can be the trigger for energy management, providing data that can be used to optimize lighting, HVAC and energy usage," Vince Lupe, senior channel marketing manager, Honeywell Systems, explains.

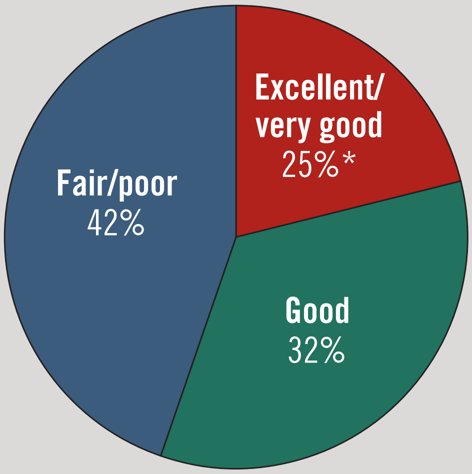
Access control can help with space occupancy and variations of occupancy during the day or throughout the day, helping HVAC systems run at the appropriate levels and making sure lights are dimmed or off on unoccupied floors.

"Organizations face intensifying pressure to reduce costs while improving environmental accountability. Corporations can improve their energy management and other 'green' initiatives with the proper selection of access control systems, secure printers and managed print services (MPS) programs," advises HID Global's Fenske.

The industry has a lot to say about the specific green potential of access control-related systems. Read the full article at www.sdmmag.com/green.

Reserved Expectations for 2012 Market

SDM asked dealers and integrators in 2011, “Considering the economic health of your business, how would you rate the potential for sales in 2012 in the **access control** market?”



SDM’s subscribers’ expectations remained muted for the 2012 market, with 4 in 10 dealers expecting a fair/ poor year.

*percentage of respondents to *SDM*’s 2012 Industry Forecast Study, conducted October 2011 among *SDM*’s Subscribers; exceeds 100% due to rounding.

still choosing to use PIV-I because it provides a more secure credential.”

The key is making sure your physical access control system (PACS) can read the credentials. For more on PIV-I and how it differs from PIV, see “Understanding PIV-I Versus PIV Identifiers,” on page 64.

John Fenske, vice president, product marketing, HID Global, Irvine, Calif., explains that the current architecture is not optimized to handle this new authentication. “However, new capabilities for secure identity information processing will enable the authentication without requiring a complete replacement of the existing infrastructure. Installing PIV-capable readers with bidirectional communication capabilities as well as an authentication module and software to ensure that credentials are validated by the correct federal authority make it possible for government agencies and their contractors to comply with the mandates in the most cost-effective manner.”

The Security Industry Association (SIA) is reviewing Open Supervised Device Protocol (OSDP) possible adoption and codification as a SIA standard, which will further drive interoperability among industry devices.

“OSDP is an open standard for communication between access control devices and their associated controllers that provides flexibility and scalability in an open standard that is also cost effective and more secure. OSDP is a bidirectional communications protocol that enables information to be shared about the status of an access control reader or other device and it allows for more information to be transmitted to the reader for control, credential updates and display purposes,” Fenske describes.

All of the changes are designed to offer a migration path from legacy to PIV credentials and provide a modular hardware approach that makes it easier for agencies to respond to regulatory changes.

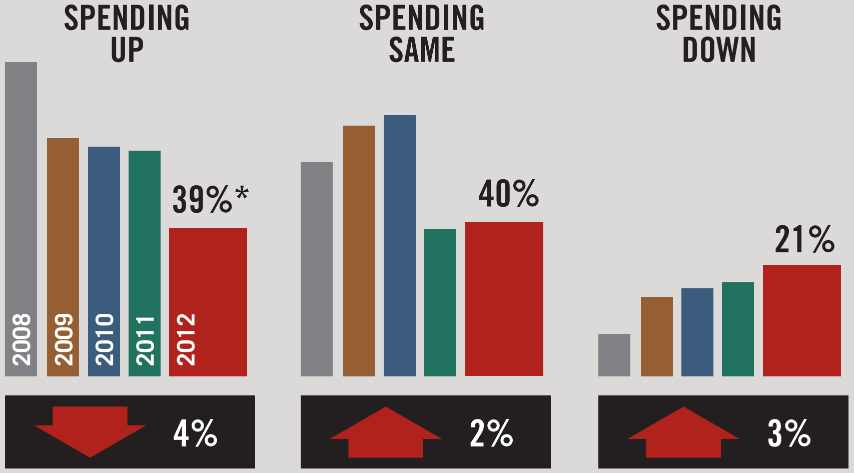
HSPD-12 also included a focus on combined physical and logical access, which hasn’t been fully implemented yet. For example, the Energy Department’s inspector general said in a Feb. 28 report that while the DOE has spent more than $15 million throughout the last seven years, most of the money was to issue and maintain badges, and was not for implementing physical and logical access controls.

Donald Woody, ADT Security Services, Federal Systems Division, Alexandria, Va., confirms that in addition to a “noticeable amount of activity in government and the associated commercial space to get compliant with HSPD-12 through PIV or PIV-I credentials, we’re also finally seeing that intersection of the physical and logical; people using the PIV card to log into systems and then also using it to get in and out of the door.” He points out that in order to take advantage of the growth in the federal sector, companies have to be knowledgeable in the area and on the GSA’s approved product list (APL), whether as an integrator or a manufacturer.

“Those are the folks that are helping lead the charge, but if you are not on the APL, you are not able to play in the space. The window is certainly not closed, though. Every day someone is coming up

Access Control Spending in 2012

SDM asked dealers and integrators to indicate how they expect their level of spending on **access control** in 2012 will compare with the prior year.



*percentage of respondents to *SDM*'s 2012 Industry Forecast Study, conducted October 2011 among *SDM*'s subscribers. Results do not equal 100 percent due to rounding.

There may be several factors at work in the growing percentage of integrators who indicate their spending on access control products will be down; including more competition for fewer projects as well as the prices of products themselves decreasing, resulting in a smaller amount spent.

with a new product that should be on that list. Also, keep in mind that the government likes to have participation by smaller enterprises, and it wants multiple solutions and integrators on the list," Woody advises.

Woody also spotlights a continued focus on managed access in 2012, especially after The Federal Cloud Computing Strategy in February of 2011 implemented its "cloud first" strategy.

"In 2012 the industry shouldn't lose focus on the cloud and managed service. ADT is consciously positioned very well for managed access, as this is something the government is highly promoting. Rather than own or buy, the instructions to federal organizations are to go ahead and rent because the responsibility for maintaining and keeping that platform current falls on the integrator. Moving forward, the CIO Council continues to emphasize to move to the cloud as much as possible," Woody says.

Steve Van Till, Brivo Systems LLC, Bethesda, Md., concurs that, "The 2012 access control market continues to show increasing emphasis on cloud adoption. More so than 2011, however, we are seeing this trend moving further up the enterprise scale into many Fortune 500 companies, including compliance-minded industries like pharmaceuticals and those with PCI requirements."

When *SDM* asked dealers and integrators if they offered managed access control to subscribers, 52 percent answered "yes."

"Small integrators want out of the box Web-based solutions with recurring monthly revenue (RMR) capabilities and monitoring, good report generating to support monthly fees, and simple integrations with video," says Paul DiPeso, vice president of Sales, United States and Canada, Lenel Systems Int'l, Rochester, N.Y. This will drive managed access in 2012.

In addition to integrators' RMR demands, the cloud answers an increasing demand for access

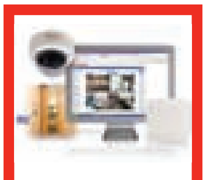
SDM Asked: "Which Vertical Markets Do You Think Will Hold the Most Potential for Growth in 2012?

"Education and healthcare continue to be drivers in the access control market. The small- to medium-sized business market is a growing vertical, as a large number of access control projects are six doors or less." — *Tony Sorrentino, president, ScanSource Security, Greenville, S.C.*

"The healthcare, government and utilities sectors all offer opportunity in 2012. In the utilities segment, the heightened demand to protect water facilities, power plants and transmission centers is fueling access control." — *Paul DiPeso, Lenel Systems Int'l*

"One area for growth involves the higher education market. Premium optical turnstiles help add a layer of security without making students feel like they're on lock down. In fact, one of Smarter Security's recent university clients reported that the peace of mind provided by the turnstiles has been such an important addition that the university even highlights the turnstiles during campus tours." — *Jeff Brown, CEO, Smarter Security, Austin, Texas*

"The banking sector will be huge in 2012 as the world attempts to cut back on the problems of ID theft and reduce waste, fraud and abuse. In transportation applications, the control of assets via RFID tagging coupled with biometrics allows carriers to not only track merchandise and goods but also maintain a proper chain of custody — who's loading / unloading containers, transporting these goods, etc." — *Phil Scarfo, vice president, Worldwide Sales and Marketing, Lumidigm, Albuquerque, N.M.*



Understanding PIV-I Versus PIV Identifiers

Legacy physical access control systems (PACS) designed for proximity cards (or even PIV cards) are unlikely to support PIV-I cards without specific upgrades for handling 128-bit identifiers. And, just because a PACS supports PIV cards doesn't mean it supports PIV-I cards. In a plug-and-play world, it may be your job to ensure that each component in your PACS is capable of PIV-I. The main difference is in the PIV card identifiers and the PIV-I card identifiers.

PIV Card Identifiers

The identifier on a PIV card is the 32-digit Federal Agency Smart Credential Number (or FASC-N). The FASC-N, found in the card's cardholder unique identifier (CHUID) container, is a "smart number," consisting of 9 fields.

The first 5 FASC-N fields (16 binary coded digits) are sufficient to uniquely identify every federally issued credential. That means that PACS may safely use the first 16 digits of the FASC-N as the card identifier without concern for duplicates. The largest possible 16-digit identifier would therefore be 9,999,999,999,999,999, which happens to require 54 bits. Most access control panels cannot store a value as large as this as a single number. Instead, they employ schemes that split the value into two or three logical parts. A common method is to concatenate the Agency Code, System Code, and Credential Number (14 digits), forming one number and the Credential Series Code and Individual Credential Issue (2 digits), forming another number. Another method is to combine the Agency Code and System Code into a number represented as the traditional "facility code" and store the Credential Number as the traditional "card number." This is often done to avoid updating panel firmware and head-end software to support larger identifiers.

PIV-I Card Identifiers

PIV-I cards are intended for non-federal issuers. The number of organizations that could potentially deploy it is so large that the Agency Code, System Code, Credential Number method used by PIV cards would not work. Therefore, with PIV-I, the FASC-N can no longer be used as the card identifier. In fact, the first 14 digits of the FASC-N on a PIV-I card is all 9s. Therefore, if a system can only read a partial FASC-N, all PIV-I cards would appear the same.

PIV-I credentials must use a different numbering system called the global unique identifier (GUID), which is also found in the CHUID container. The construction of the GUID has some important properties that impact physical access control systems.

A GUID is generated in a way that assures uniqueness across the planet, even if the machine generating it is "off the grid." The GUID is always 128 bits, which is more than double the size of the 16-digit truncated FASC-N.

The Reader

The reader must be able to recognize that the credential is a PIV-I card. The correct way for the reader to do this is to read the CHUID and check the first 14 digits of the FASC-N. If it is not all 9s, it then outputs the FASC-N. If it is all 9s, it outputs the GUID. The panel must be able to accept cards of both formats — FASC-N or GUID.

For more on how panels and head-end computers address PIC-I credentials, read the expanded sidebar online at www.sdmmag.com.

— Contributed by Bob Fontana, president and chief technical officer of Codebench.

control-related services from end users, says Jacky Grimm, vice president, Security Solutions and Business Development, Diebold Inc., North Canton, Ohio, *SDM*'s 2011 Systems Integrator of the Year and No. 4 on the Top Systems Integrators Report.

Grimm told *SDM*, "When it comes to access, we're absolutely seeing a movement toward services. End users are looking to save costs and shift responsibilities for the administrative tasks related to access control. So we're seeing a lot more activity around the outsourcing of things like badge printing and other program essentials that may not be the best use of internal staff resources," she describes.

Technology integration also is key in 2012.

"We are seeing access control systems crossing over into video surveillance, intruder detection, alarm systems, and more. Products that combine the power of access control, digital video and intrusion into one solution are becoming more common. These solutions allow dealers to provide a single user interface to control and manage a complete security system. These types of integrated systems soon will be a standard across the market. PSIA and ONVIF have recognized that enhancing their standards to include access control integration will bring them new adopters and streamline the approach to open source integration," says Andy Morra, vice president, Marketing, ADI, Melville, N.Y.

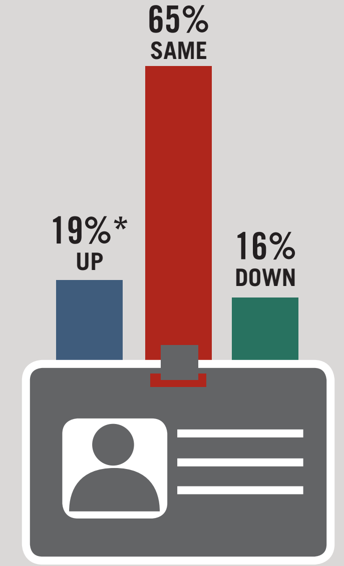
"ONVIF is developing interfaces for both video and physical access control systems. These interfaces will aid integration between the two systems, further facilitating the development of more integrated systems, which will influence the market," confirms Jonas Andersson, chairman, ONVIF Steering Committee.

"The integration of access control with other systems — most notably with video — is an important area of growth in 2012," says Dan Rinehart, strategic marketing manager, Honeywell Systems, Louisville, Ky. "Dealers and integrators, whether they serve small, mid-size or enterprise markets, are embracing integrated video and access control because they see value in a combined offering. An integrated offering allows end users to get greater detail behind access

DVR
NVR
RS2
POE
CCTV
IP
WIFI
WWW
GUI

Expected Spending on ID Cards/Printers

SDM asked dealers and integrators to indicate how they expect their level of spending on **ID Cards/Printers** in 2012 will compare with the prior year.



*percentage of respondents to *SDM*'s 2012 Industry Forecast Study, conducted October 2011among *SDM*'s subscribers.

A majority, 65 percent, of SDM's subscribers expect their spending on ID cards and printers to stay the same.

control events. Video provides context to events that happen at the door, exposes and documents issues like piggy-backing or unauthorized access and much more.

"Furthermore, the addition of power over Ethernet (PoE) at the door has taken the per-door cost and dropped it dramatically, expanding the opportunity set for our customers. NetAXS-123, a Web-based access control solution, hits a sweet spot in the small-market, entry-level application and gives dealers the ability to take one-, two-, or three-door customers and grow with them into a larger system. It is a very nice migration path, and it is much easier on customers' wallets as well," Rinehart says.

Wireless is also saving money for installers, according to Cindy English, director of Marketing, Ingersoll Rand Security Technologies, Davidson, N.C.

"Almost 70 percent of electronic locking systems now incorporate wireless. As a rule of thumb, implementing wireless access control reduces installation time by up to 50 percent, system costs by up to 25 percent or more, and disruption to the facility during installation," English estimates.

Wireless continues to increase the solutions for end users, as well.

"We just recently completed a project of integrating into the ASSA ABLOY series of wireless locks," says Steve Lewis, C•CURE 9000 product manager for, Tyco Security Products, Westford, Mass. "There are so many markets that need that technology. Think about health care and education. In those environments, the physical environment is changing constantly. Wireless allows them to move doors at will without pulling cable and in hospitals it allows them to keep the environment clean."

As more and more products are developed to take access control out to "the edge," it will take less and less cable to connect things together and make them work, predicts David Barnard, director of dealer development, RS2 Technologies LLC, Munster, Ind. "This means a significant reduction in the use of a wide variety of raw materials and the energy used to produced the finished cable, etc. When taking full advantage of the new wireless access control products, I can visualize that someday we might be able to completely eliminate the need for any wire at all," Barnard says.

Near Field Communications (NFC) continues to grow in 2012. NFC-enabled phones shipped in 2011 totaled 35 million globally, but IMS Research forecasts the number to reach nearly 80 million by the end of 2012.

"We believe you will see NFC technologies be deployed in much the same way Wi-Fi was, starting with limited penetration but growing quickly. It has been estimated that between 10 and 15 percent of all phones will have NFC in 2012, up from only 1 percent during 2011," says Fenske.

NFC-enabled phones shipped in 2012 will reach nearly **80 million.**

Source: IMS Research

Tyco Security Products' Lewis adds, "It is a technology that is very close and it is exciting for the industry. There are companies racing to release solutions. In 2012 companies are showing the possibilities for NFC. You can 'send' keys to contractors working at your home or to your daughter who forgot her keys. It allows you to pass keys around but you don't have to worry about a badge. Tyco Security Products has a new touch screen reader in development that is NFC-ready that we're excited about," he says.

NFC, like smart cards, is yet another access control technology speeding toward new levels of adoption, and possibly toward an eventual tipping point of its own. These technologies along with the flexible options of managed access and wireless' low entry point help with the overall outlook for 2012. ■