One Person, One Identity, One Credential: Converging Logical-Physical Identity and Access Management

By Sharon J. Watson
Senior Producer, Security Squared
July 2009
www.securitysquared.com

This paper explores in depth the convergence of physical and logical identities—a nascent, but logical and likely outcome of the implementation of identity management tools and Internet Protocol-based security tools. It will offer examples of how synchronizing the creation and management of physical and logical identities creates business, regulatory and security benefits. Security, IT and executive readers will come away with a high level understanding of the technological and logistic challenges involved in converged IAM; current solutions for addressing these; and how IAM convergence is benefiting users.

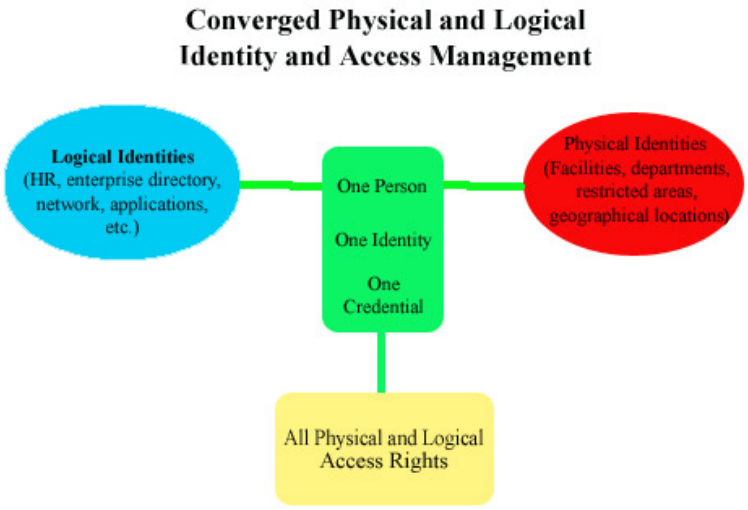
I. Introduction

What is converged physical-logical identity and access management (IAM)?

For Shape.Net, a health and fitness club management firm, it's a profit center: converged identity management has enabled Shape.Net to offer its health club clients 24/7 access to its facilities—which they in turn offer to their fitness customers. After hours, a customer swipes a proximity card tied to Brivo System's web-based access control service that in turn queries a Shape.Net database in real-time to verify the health club customer is current on her bill and should be allowed entry.

At Toronto Pearson International Airport, converged IAM means greater productivity, satisfied clients, reduced costs and improved security. Instead of waiting days or weeks for credentials, the airport's Pass/Permit Control Office can now provision new users, even to highly secure areas, within 20 minutes. Its system, the centerpiece of which is Quantum Secure's SAFE, ties together disparate physical access control systems and external identity databases and automates workflows to create a singular trusted identity and one credential to match.

One identity, one credential: that is the basic definition of converged IAM. Achieving it requires synchronizing an individual's physical and logical identities and access rights within and across the enterprise (see diagram).



"Identities," plural, is the key word. Virtual and physical identities tend to proliferate in most enterprises. On the logical side, a person may have one virtual identity within the enterprise human resource software, such as a PeopleSoft or SAP system. That identity typically consists of salary, benefits, insurance, social security number and other specific employee details.

Then there's a logical identity within the information technology department's directory software, such as those from Microsoft, Novell, CA, Sun Microsystems, or Oracle. This directory knows

which network, database and software applications the logical identity may access. Within those intranets, databases and applications, the user may have still more identities, in the form of different user IDs and passwords or PINs he uses to log into each one.

That user also will have at least one more identity: a physical credential of some sort used for access to parking garages, buildings, floors, warehouses, etc. In enterprises with more than one brand of physical access control system (PACS) and several facilities or areas users must enter, a user may have more than one physical access credential—and therefore, more than one physical identity.

The permutations seem endless—and the key goal for converged IAM is cleaning up or at least mapping all these logical identities to create a singular, authoritative identity. That is, IMA PERSON equals I MA. PERSON equals PERSON, Ima, etc.

Why converge identities?

A sensible reason for converging identities is that when disconnected logical and physical identities proliferate, it's time-consuming, expensive and inefficient to manage them. That's true for IT, for physical security, for risk managers and business units.

These inefficiencies are most apparent in regulatory compliance, the big driver behind many identity management projects. Meeting regulatory compliance standards is more difficult when identities multiply, because correlating the actions of disconnected physical and logical identities across systems, assets and facilities is usually a manual, labor-intensive process.

Another issue is that security can be more easily compromised when physical and logical identities are separate. A physical identity may appear legitimate to a standalone PACS, but what if that identity is no longer trusted by the enterprise network? That's what happens when an employee is terminated in the logical systems, but that information isn't immediately relayed to a PACS. If the enterprise has more than one PACs, and they are not integrated with each other, it may take several more steps to ensure all PACs refuse the ex-employee's credentials.

Physical or logical credentials that stay live long after an employee has left an enterprise are always a compliance gap and, at worst, can leave the virtual or physical door open for mischief and attack.

One identity, one credential

Converging logical and physical IAM within the enterprise is designed to solve these problems. In its ideal form, converged IAM creates one identity assigned to one credential that encompasses all of an identity's logical and physical access privileges. When one set of privileges changes, whether physical or logical, that alteration triggers automatic, complementary revisions in the other set. The most common example: an employee termination on the logical side being instantly—and thoroughly—reflected on the physical side.

The technology exists to accomplish converged IAM. Mature identity management systems and provisioning tools exist at the IT level. More security systems and devices are now Internet Protocol-based and can more easily share data with IT systems. Older systems can be integrated

through third party bridge software so that both IT and PACS can draw data from a central, authoritative identity database.

Therein lays the rub: creating authoritative identity stores requires enterprises to figure out how many identities they have, how and by whom these are created, managed and terminated.

Determining these processes, or creating them anew, cuts across every functional enterprise boundary: IT identity management specialists, IT security experts, human resources personnel, business unit end users, physical security experts. Additional identities can include enterprise trading partners, contractors, temporary employees, and vendors.

Finally, there's the question of how much IAM convergence is truly required for a given entity. Vertical industries rife with regulatory requirements to govern privacy, security, hazardous or controlled materials benefit from more granular degrees of convergence—such as limiting access to specific areas or applications based on logical/physical data. Other entities may be content with ensuring physical access is automatically revoked when HR declares an account inactive.

That said, converged IAM initiatives are under way. They are most likely to be found in heavily regulated or critical infrastructure industries, such as finance and power. Lessons learned here are likely to influence how a broader range of Fortune 5000 level enterprises and even smaller entities manage identities.

II. The Building Blocks of Converged IAM

Recently, a California Water Service Co. auditor resigned his post in the morning. That evening, he returned to a company building, accessed a former co-worker's computer—and the applications necessary to arrange to wire himself $9 million.

Converged IAM, which ties together a person's logical and physical identities and access rights within an enterprise and assigns them one credential, can help prevent such incidents. First, a converged IAM solution would have ensured the auditor's building access card was deactivated. It might also have noted that the co-worker was not physically present in the building and refused to accept the normal system login data while also automatically alerting security.

Engineering such solutions is not inexpensive or easy. Yet illicit funds transfers, data theft or destruction, sabotage and other malicious acts by current or former insiders are also expensive—and increasing. In a recent survey conducted by McAfee, Inc., 68 percent of respondents said the greatest threat to their data was from inside sources.

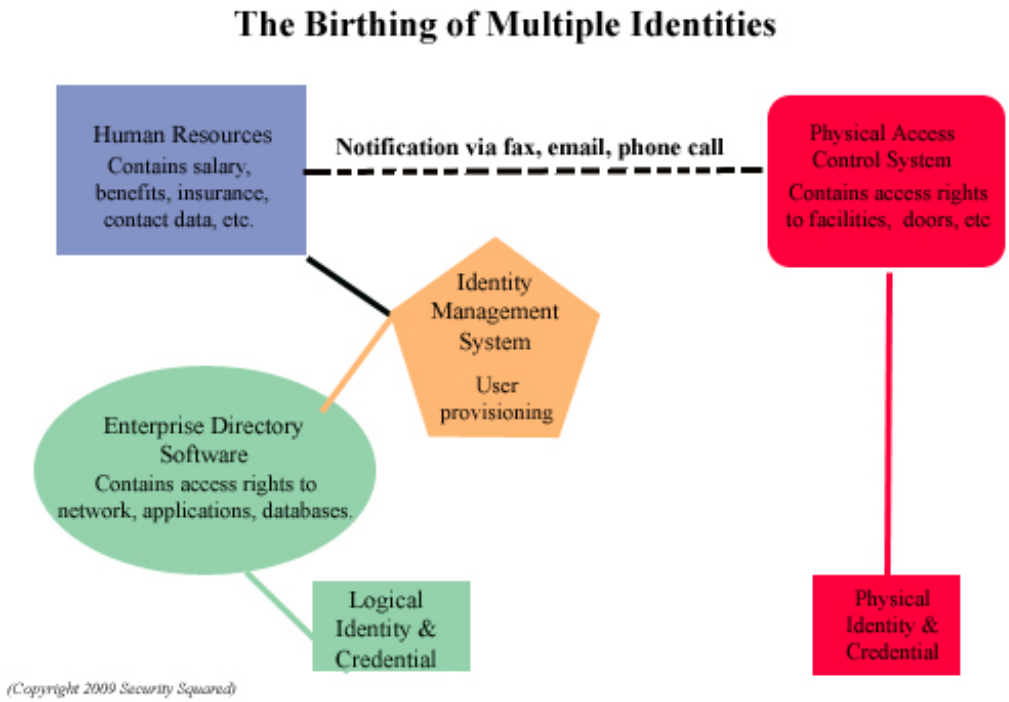
Statistics like those are one driver behind converged IAM—which need not be a green-field deployment. Many larger enterprises already have several key pieces of technology in place on which to build converged identities. These include human resource systems, directory software, and identity management provisioning tools on the IT side, plus PACS on the security or facilities side of the enterprise.

The birthing of multiple identities

Converged IAM can't exist without connections, preferably automatic, software-driven ones, between these logical and physical identity systems. These ties usually begin with links between human resources systems and a critical IT network component, the enterprise directory. HR systems, such as those from PeopleSoft and SAP, essentially ensure the employee receives proper salary and benefits. The directory software, such as Microsoft's Active Directory or others based on the Lightweight Directory Access Protocol (LDAP), ensures the employee has the network, software and database access—the virtual provisions--she'll require to do her work.

Many large enterprises already use identity management tools from vendors like CA, IBM Tivoli, Novell, Oracle and Sun, to provision users from the HR system into the enterprise directory.

That process is fairly well automated. The disconnection between logical and physical identity usually appears when it's time to provision a user's physical access rights—at the most basic, where and when that person is allowed to be within the enterprise. In many enterprises, this task is typically still manual: a phone call, email or fax from HR alerts the physical security department to put the new employee into the PACS and create an access badge for him.



That's more than a logistical gap. Typically, very little information about the user's logical access rights is transferred to the PACS. The PACS tells the identity management tool very little about the user's physical access permissions. In essence, two identities are born and are free to move about the enterprise without correlation—and that's a security risk.

"If there are role changes up there on the digital side, that must change down in the physical; if last name changes in digital, last name must change in physical; something happens in digital, the

same thing has to take effect in physical," said Ajay Jain, CEO of Quantum Secure. "If you cannot keep those personas concomitant with each other all the time, security can be compromised—it will be very easy to compromise."

Jain

Integrating the PACS with the enterprise directory enables enterprises to address the issue of disconnected physical-logical identities, said Erik Larsen, product manager of identity solutions for Lenel Systems International. "We see the value to the customer is that [integration] allows them to have a better understanding of who has rights to their network and their physical facilities. It allows them to manage access rights and people's responsibilities within the organization more efficiently," he said.

Integration issues

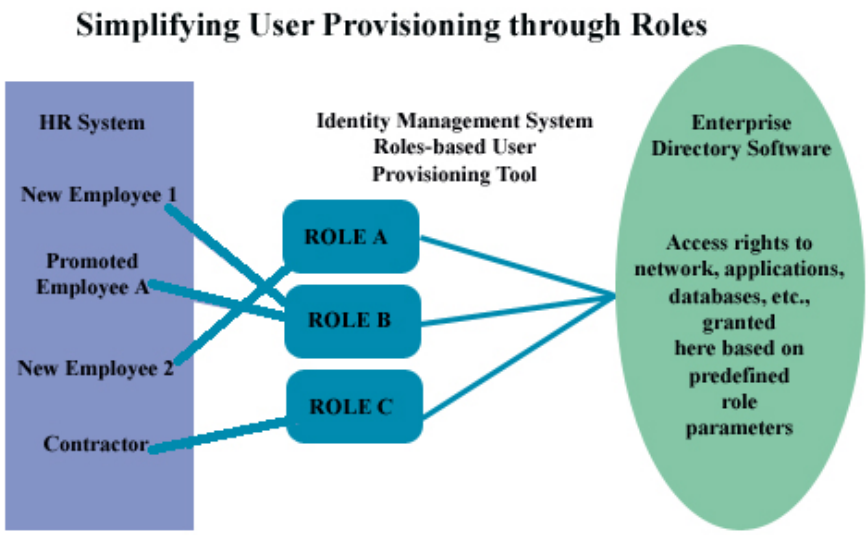
One challenge to integrating the IT and PACS identity systems is technological: many older PACS are based on closed, proprietary platforms, making it difficult to seamlessly transfer data between them and IT identity and directory systems, which are based on standard languages and platforms.

Standardizing multiple existing identities is no small process, either. In his webinar "Enhanced Identity & Compliance Management Delivered Through Systems Integration," Brandon Arcement, manager, global security technology for Johnson Controls, explained that one client assumed it could create common user IDs in its various databases and applications in a long afternoon; on further investigation, it determined it would need six months to tackle the task.

The value of standardizing logical identities is rising to meet the work involved to do so, as logical identity management tools become increasingly sophisticated. In particular, they are beginning to streamline how enterprises provision logical access rights. Most identity management tools today enable enterprises to define roles and associate logical rights to those roles. Then, instead of individually assigning applications or network portals to new or promoted employees, the new user can simply be assigned a role in which those permissions are already embedded.

These roles-based permissions can be extremely granular: for example, a role might detail not just an application, but also which functions within the application a user may access. This capability helps ensure regulatory compliance.

Such roles-based provisioning could also help with identity maintenance. An employee may accumulate many permissions over time as her job titles and responsibilities change; roles-based changes could help ensure access to special projects or files are deactivated.



Roles can also speed deployment and security of single sign-on (SSO) solutions, in which a user signs onto the network only once to access all her permitted applications. Many SSO solutions incorporate devices that generate one-time-only passwords, so users don't need to remember them. That reduces the administrative costs of password management—still a big productivity cost center for IT help desks.

Physical roles managed by logical systems?

Physical access rights can also be embedded in those identity management system-defined roles. Integration between IT's identity management system and a PACS could enable those rights to be embedded on a smart physical credential. Further, as more security tools, such as card readers, doors, surveillance cameras and sensors become IP-based and attached to the enterprise network, they too could be linked to identity management systems. That would help tie together physical movements with activities in logical systems.

It's not a theoretical capability: Daniel Raskin, chief identity strategist at Sun, noted that the badge he uses to enter Sun's facilities integrates with two IT-based Sun products, Sun Access Manager and OpenSSO, to give him physical/logical access. But he adds: "I haven't seen a lot of demand or queries for that."

Some identity management vendors flat out say they'd rather let someone else integrate the physical security components. "It's very customized work you're talking about because the standards are minimal in the [physical security] industry," said Dave Hansen, corporate senior vice president and general manager, CA Security Management. "There's definitely a role there for a middle person."

Not surprisingly, some of these players in the middle point out their systems have abilities not necessarily shared by logical IAM vendors. "What we control from our SSO is what privileges

for application level access you can get from a given location," said David Ting, CTO, Imprivata. "[Identity management platforms] can do certain levels of application and web resource authorization, but they can't tie into location. So we supplement what they can't do."

Others see their role as complementary. "We're just leveraging what [identity management systems] are doing to manage identities across the IT space to provision access control privileges as well," said Arcement at Johnson Controls.

"We're kind of the ecosystem," agreed Hansen, noting that the identity management systems can propagate the authentication from the PACS and its security devices across the logical world. "We have the hooks into all the operating systems to do the authentication," he said.

III. Physical, Meet Logical

IT-based identity management systems have the ability to manage physical identities and assets as well as virtual identities and assets. Yet given the complexity of the physical security ecosystem in many enterprises, most sources expect PACS to be a key to converged IAM.

Huntington

PACS do bring strengths to the job. PACS architectures are built for authenticating many users in a short time, such as at a busy door. "IT systems are built to support confidentiality first," said Guy Huntington, an identity management consultant who has worked with Boeing, Capital One and Toronto Hydro.

In addition, PACS interact with many complex systems of their own, such as door and card readers, video surveillance systems and physical perimeter defenses.

Then there's the fact that many PACS wind up being the unofficial yet central identity management system for all the non-employees who visit the enterprise: cleaning crews, maintenance workers, repairpersons, temporary employees, contractors and visitors.

Yet PACS also pose challenges to converged identities. Many enterprises operate more than one PACS because they acquired another firm or bought a physical facility or space. Further, many PACS still operate on networks independent of the enterprise network. In addition, most are based on proprietary technologies, each with their own application programming interface (API).

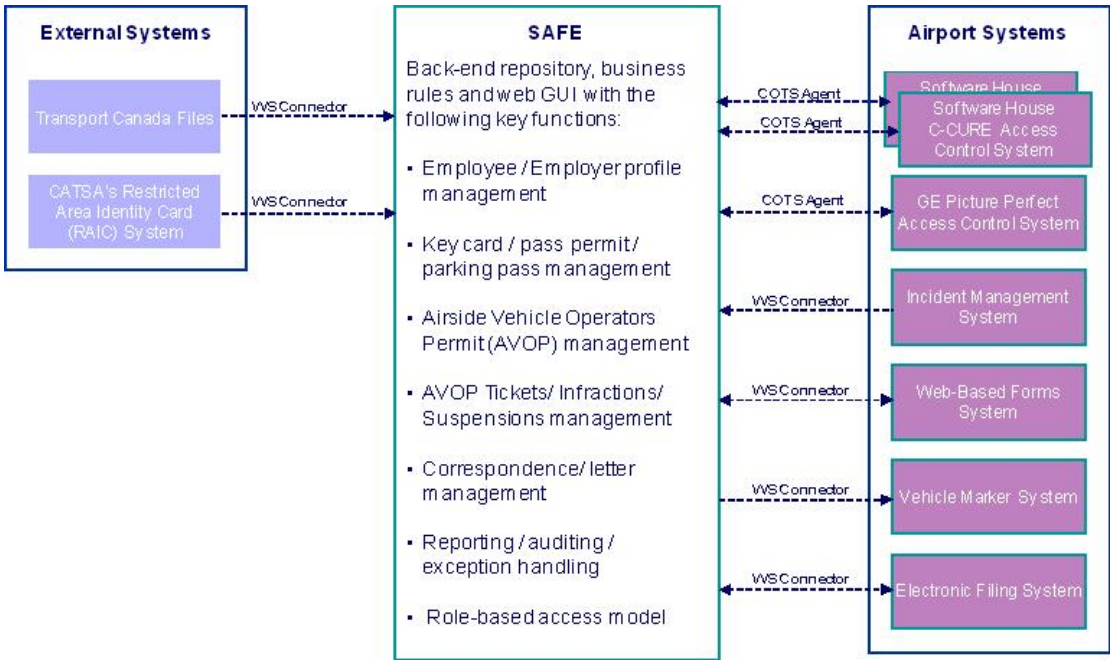
Different PACS with different APIs mean the IT department or its identity management vendor must write separate interfaces to each PACS—some older versions of which may not even have APIs—to ensure logical-physical integration. And most don't want to do that.
"For us, we have a hard enough time managing all the potential types of things we have to provision and deprovision to," said Hansen. "If we had to go to every very unique, rudimentary badging system, it doesn't scale. We don't want to be experts in HID cards and smart cards and all that. There are a lot of people who do that."

Enter the bridge-builders

Those "people" include vendors building businesses on their ability to connect disparate PACs and then integrate those to enterprise directory software and other enterprise applications. These include AlertEnterprise, Imprivata, and Quantum Secure.

Each of these companies brings a comprehensive library of PACS and identity management systems interfaces to its installations. Imprivata boasts of an appliance-based approach that permits integration with practically a menu selection.

When searching for vendors to streamline identity management at Toronto Pearson International Airport, Deloitte found Quantum Secure to have the widest array of off-the-shelf PACS interfaces, according to Andre Romanovskiy, senior manager, security and privacy services, for Deloitte, during a webinar hosted by Quantum Secure.



At Toronto Pearson International Airport, Quantum Secure's SAFE acts as the authoritative identity source, connecting to three PACS as well as external databases owned by Canadian regulatory bodies. SAFE contains the rules, policies and workflows for credentialing and managing identities of 45,000 employees, vendors and contractors, serving an average of 175 customers a day.

(Image copyrighted by Deloitte. Used with permission)

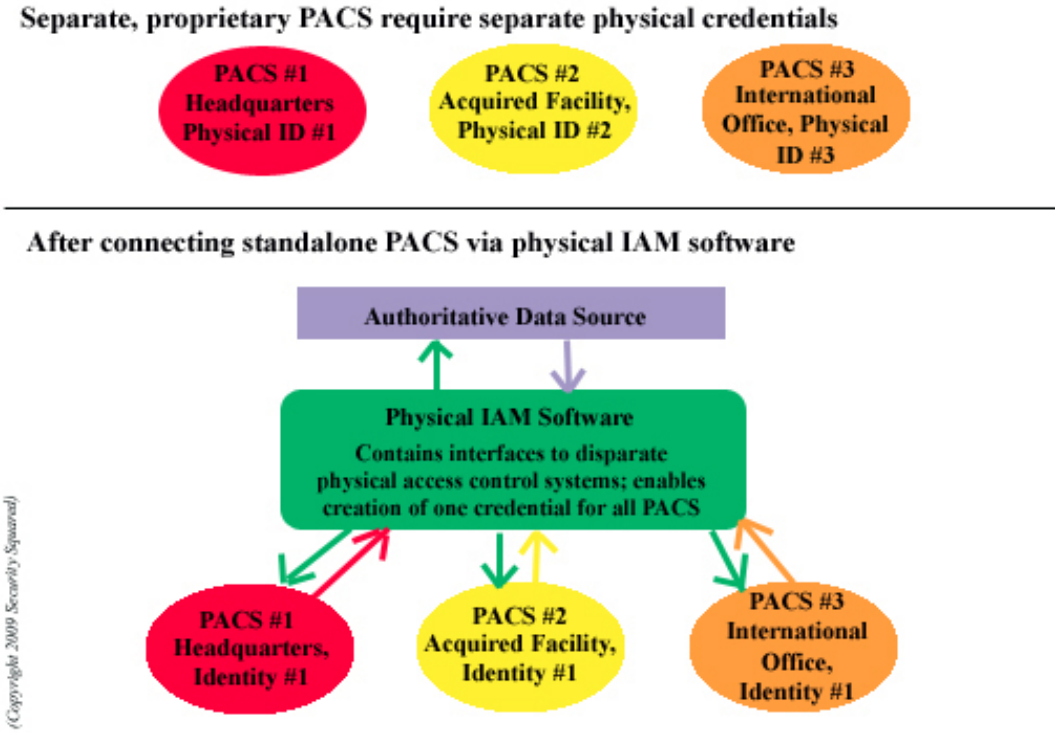
In the Toronto Pearson implementation, Quantum Secure's SAFE essentially acts as the authoritative identity source, sitting between the HR systems of dozens of airport tenants and three PACS. Automated workflows handle queries among these systems, reducing initial credentialing time from an average of 10-plus hours to 20 minutes.

Some leading access control vendors also say they are prepared to integrate with other databases. OnGuard, from Lenel, can be integrated with LDAP-based enterprise directories, the reigning standard, said Lenel's Larsen. (AMAG/G4Tec and Software House claim integration capabilities in their marketing materials.)

Brivo Systems, which delivers video and access control solutions via software as a service (SaaS), bases its solutions on extensible markup language (XML), an open language that enables it to easily integrate with other systems and databases.

Streamlined identities and security

Integration of disparate PACS with each other makes it more likely a user will need to carry only one card to enter all the enterprise facilities to which he's entitled, even those that are geographically dispersed.



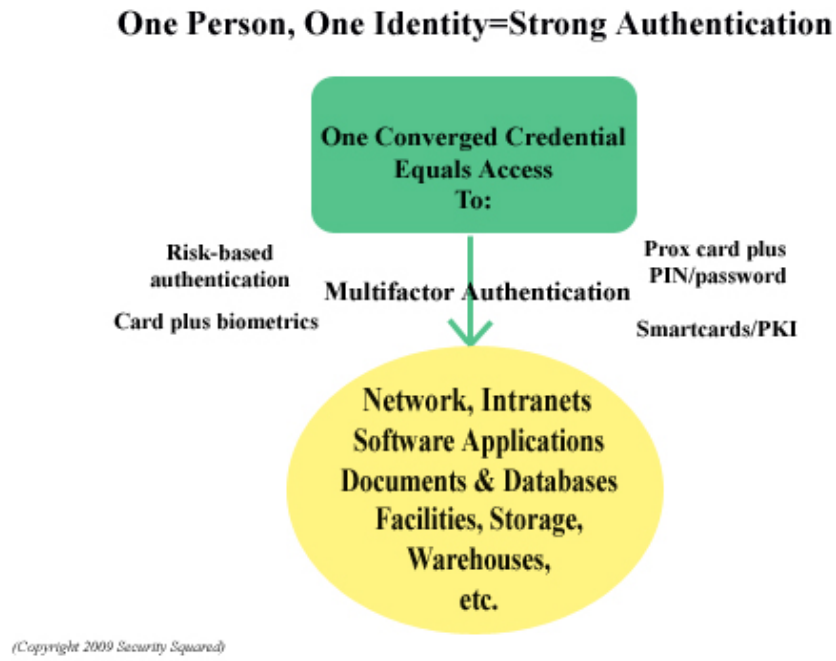
In turn, linking this streamlined physical credential with logical IAM means an individual can use a single credential for physical access as well as network and applications access. Further, the two types of access can be correlated: a swipe at the door reader tells the network that IMA PERSON has entered the building and thus should be authenticated for network access, provided Ima's SSO goes smoothly. The correlated door swipe and SSO also alert the network that Ima apparently is still in the building when someone tries to access her accounts from an IP address outside the network. Did Ima slip out without swiping her badge, or is this a hack in progress?

Authenticating the one identity

Once identities converge, it becomes critical to ensure the person holding that physical/logical credential is truly who you think they are. “At the point where customers have done enterprise single sign-on (SSO) and have created a single point of entry into ten different applications, they sometimes step back and say, ‘I really need a second factor,’ ” says Joe Anthony, program director of identity and applications security management, IBM Tivoli.

“The big opportunity with the convergence is using the badge or physical access system as a multi-factor authentication device,” said CA’s Hansen.

These authentication factors can include one-time-only password generating tokens or cards; biometrics plus cards; smart cards with chips enabling use of Public Key Infrastructure (PKI) and digital certificates. It’s possible video facial recognition applications might be added to this list.



“We’re seeing a lot of questions and more technologies popping up around risk-based authentication and authorization,” said Sun’s Raskin. These solutions use algorithms to analyze keystrokes, location, devices and other variables to determine whether there's risk associated with someone logging into an application.

However, stronger authentication requires infrastructure investment, such as card management systems, certificate authority software, additional readers on devices, etc.

The issue then is striking the right balance between authentication strength and its cost, said Dan DeBlasio, director of business development for identity and access management, Americas, at HID Global. “How can we strengthen that access at the IT side and do it in a convenient way, with minimum cost of entry and yet make it multi-application to minimize risk?”

HID's answer is a converged IAM strategy based on a proximity card that can be used as the primary physical credential, then act as a second factor to a user's PIN or password to the enterprise network in designated settings.

Specific industries will also shape their authentication methods. Health care has high security needs but also high data availability requirements, noted Imprivata's Ting. He said many health care providers require a card read, plus password or PIN at the start of a shift for login. Then, as different caregivers use the same workstation throughout the day, sometimes just minutes apart, a card swipe alone is sufficient for data access.

"That gets even more secure," Ting added, "when you combine location to know the person who is swiping that badge is actually within a known location in the hospital."

Right now, enterprises may choose from many authentication devices, and several vendors mentioned expecting to see some industry consolidation around one or two methods as technologies and standards mature. "I think we'll see some nice evolutions in price points as well as types of technology people can leverage," said Anthony.

IV. The Human Factor

While the technological tools available to manage logical and physical identities continue to grow in sophistication, they are just that: Tools designed to help humans create effective identity management strategies—and there's no getting around the extensive, people-focused methodology necessary to create such strategies.

"When you look at what identity management really means, there's a lot more to it than just defining identities: there's roles and business rules and processes around it," said Greg Thornbury, vice president for Dallas-based SecureNet Inc., a systems integrator that has been implementing converged IAM solutions for the last nine years.

"It doesn't do any good at all for me to push changes to an identity sitting in a database across the U.S. if I still have someone who can walk in tomorrow and manually create an identity and violate those business rules and processes," he said.

"Identity management is a process, not a technology," agreed ID management consultant Huntington.

That process begins with figuring out where identities currently exist, understanding how they are being created and by whom, what the de facto procedures are for managing them. Streamlining these practices means involving a myriad of enterprise functions, said Huntington. "I have to put everyone around the table and figure out who owns all these identities," he said.

"Understanding how many identities you have for single individuals really outlines the scope of the challenge," said HID's DeBlasio.

Enterprise identity creators include HR, IT, physical security, plus business units. Other identities may be owned by third parties who often access the enterprise virtually or physically: trusted

customers, contractors, temporary workers, repair, delivery and maintenance workers; custodial crews; visitors and guests.

Security itself may be credentialing some of these identities via the PACS and card management system. “A lot of people with passes [to your enterprise] aren’t in your IT systems,” said Huntington, echoing several vendors who said clients have realized the same fact after reviewing identities.

Just what should be the ultimate authoritative identity source may depend on human factors. Many physical and logical identity management solution vendors, from CA, Sun and IBM to Quantum Secure and AlertEnterprise, prefer to tap an HR-owned data source.

Hansen

However, some enterprises prefer identity management solutions to tap Active Directory, Microsoft’s widely used enterprise directory tool, or a similar Lightweight Directory Access Protocol (LDAP) based tool, in lieu of HR systems.

Using Active Directory as the primary data source means IT owns the initial onboarding process for an identity, argued CA’s Hansen, “That’s not IT’s role,” he said. “It’s absolutely critical that HR owns the onboarding process.”

Yet HR departments in his client base—energy, health care, food processing, critical infrastructure and governments--often are reluctant to permit a direct link into a live database, said SecureNet’s Thornbury. In those cases, SecureNet might be given access to a database copy or do batch updates, but eight of ten times finds itself tapping Active Directory as the authoritative data source for enterprise employee data.

“We’ve done it both ways. It’s great to connect straight to HR—that’s truly the originating point for a lot of that data,” said Thornbury. “But in other cases, it seems like HR doesn’t keep up everything the way that IT does from an employee location standpoint.

“A lot of what we do as an integrator is work with our clients and do a lot of listening to find out what is the best authoritative source,” he said. “You’re going to find in a lot of organizations that answer is not going to be consistent.”

Whatever the authoritative identity data source turns out to be, it’s rare to find a company that has only one such source. Different divisions may run different HR systems. Many vendors say contractor data is usually in a separate data source, and visitors may be run through a PACS or separate visitor management system.

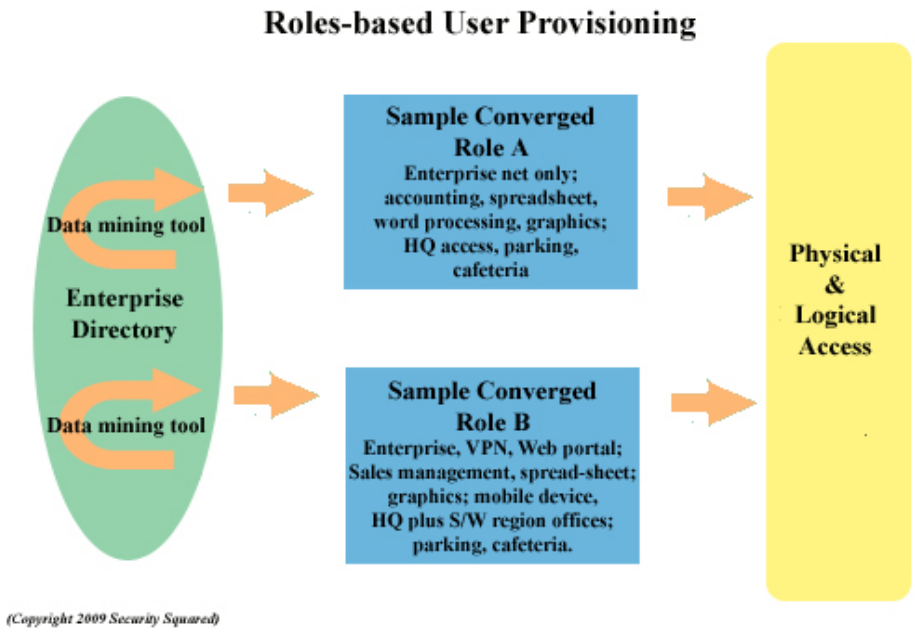
Rather than trying to create a single data source, what’s critical is creating processes that include enforceable rules for creating, maintaining and terminating master identities in the designated authoritative data sources.

Identity rules and roles

Rules for creating, provisioning and managing the logical/physical identities as they change over time are influenced or defined by regulatory bodies as well as by internal needs and practices.

Roles-based provisioning tools can help enterprises see how their identities are behaving. CA, IBM, Sun and others offer data mining tools in their identity management suites that examine user actions and then suggest which sets of users might be grouped under roles as well as help define those roles. In the future, new users automatically can be assigned a role that, by definition, contains all their logical access rights.

Further, these logical roles can be associated with predefined physical roles in a PACS. Then, when PACS are integrated with each other and to the enterprise directory, "physical access rights can be automatically given" by the PACS based on data in the enterprise directory, said Johnson Controls' Arcement.



Roles-based provisioning greatly simplifies meeting compliance requirements because a manager can certify that a role is correct and that the right staff members have the right roles, instead of trying to match staff members to various applications and their functions, said Raskin.

However, some business unit managers want more control over roles than predefinitions always allow, said Lenel's Larsen. He said that's especially the case regarding project-specific privileges.

Other vendors noted clients rarely start out knowing all the rules they'll need to associate with roles, whether within applications and systems or facilities, such as only permitting someone onto a factory floor or airport tarmac after they've successfully completed safety training. "What's important is that you install an infrastructure and an architecture that allows you the flexibility to create and customize rules," said Arcement.

Some IBM Tivoli customers start without any rules, instead deploying data capture tools to see how users are interacting with an application. That data then helps them decide what rules should be, said Anthony.

Championing converged IAM

Rules that help an enterprise fulfill its regulatory compliance obligations are a clear, powerful driver behind IAM convergence. Yet the IAM process also offers an array of benefits that have different appeal to various enterprise audiences.

"We used to go in selling the IT people the value of the security, and it turns out what they are more interested in is SSO, password management and auditing capabilities," said Imprivata's Ting. He noted the physical security leaders like the ability to incorporate their access data with the IT rules and policy data.

Huntington and others point out converged IAM most benefits security when logical and physical security alerts are monitored and correlated from a centralized console. Otherwise, convergence is not compelling, said Jasvir Gill, founder and CEO of AlertEnterprise, which integrates physical, logical and control systems.

"The reason is integrating IT and physical access is not good enough," said Gill. "Unless you are doing risk analysis across all these environments, people really don't see the value," he said.

Raskin

Industries with the toughest security and compliance reporting requirements, such as finance, transportation, power/critical infrastructure, health care, are among the early experimenters with converged identities, vendors agreed.

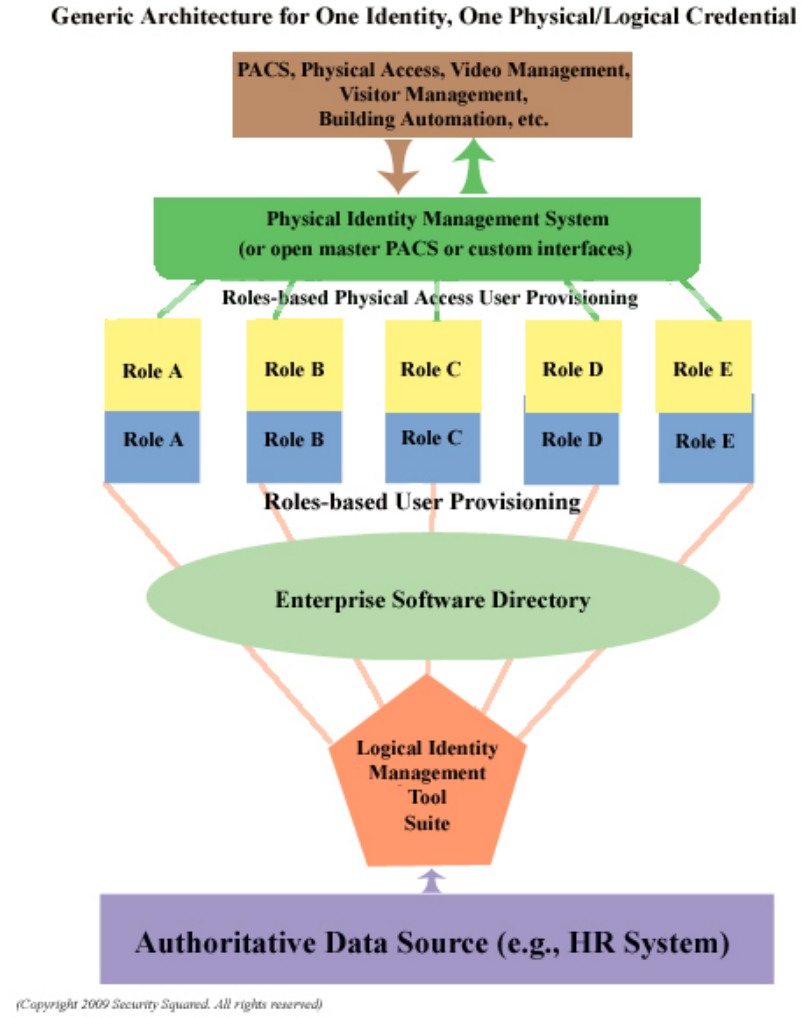
In other markets, converged identities may take awhile to make inroads. "When customers come into Sun to talk about the problems they need to solve, they're still sitting there saying how do I get my provisioning infrastructure set up, how do I just start to do roles," said Raskin. "Most organizations haven't completed single sign-on and are just starting federation, let alone getting into these more complex things."

Yet even less regulated industries running a patchwork of identity solutions could benefit from identity convergence. "A lot of people don't realize how much money they're spending, trying to manage a lot of disparity in their access control systems," said Arcement.

Fluid boundaries

Forward-thinking enterprises also want to take advantage of a more IP-centric physical security backbone that can be integrated with IT systems, said Anthony. "We're starting to see more convergence of the organizational structure, and that's when we see people looking across the different boundaries and trying to make better sense of the data available to them," he said.

"Part of the discussion driving this is that people are trying to take both sides of their house to a new level," said Hansen. He and others noted that desire usually involves competition between physical security and IT security experts, with some nascent jockeying for control of the whole.



Physical access control integrated with logical access control may turn out to be just one piece of that whole. Lenel has launched a green initiative involving ALC, a sister UTC company, and Cisco Systems, which is running and analyzing the proof of concept project. According to Larsen, it involves a PACS integrated with a facility's IP telephone network system as well as its building automation energy management system. A visiting employee comes to the facility and requests office space at a kiosk. The integrated systems then activate the assigned space: his phone number is transferred to the IP phone; printers activate and the building automation system adjusts the room's light and temperature based on a predefined profile in the PACS.

The system can also use intelligent video monitoring and analytics to check conference rooms, determining when they're empty; the PACS then notifies the building automation system to turn off the lights and other room resources. "It's taking it all to the next level," said Larsen.

Converged physical-logical identity and access management is a young concept. Yet it is a logical outgrowth of the IT and physical security systems many enterprises of all sizes and industries already have invested in. Converged IAM is a way to get more out of those systems and improve business, compliance and security practices. It is undoubtedly a major project, yet it can be handled in stages. The open questions are how long it will take enterprises to embrace the concept and whether IT/physical security will drive the process or be forced along for the ride. Whichever the case, it's sure to be an interesting journey.