
I AM Who I Say I AM

BY DAVID BAUM

In today's highly connected business world, the lines dividing corporate networks are blurred. E-commerce sites, enterprise information portals, supply chain management systems, strategic sourcing systems, on-line marketplaces, customer relationship management (CRM) systems, and enterprise resource planning (ERP) applications are all strategically linked to exchange information and help people collaborate. Yet, while these networked business systems improve employee productivity and allow companies to build online communities, they also present serious security challenges. The user base that IT professionals need to manage is growing in size, diversity, and complexity, making it difficult to identify and authorize users.

>>

ILLUSTRATION BY MIGUEL S. SALMERON



In the age of global online information systems, authenticating users and controlling access to corporate information has become significantly more complex.

In the past, IT security was designed mainly to keep people out of a network. Today, more and more of these internal applications need to be exposed and shared with outsiders—from partners and customers to remote users in the field. In essence, organizations need to open their virtual doors to the world while ensuring that only the trusted walk through them.

To resolve this enterprise-access quandary, many companies are turning to identity and access management (IAM) solutions. These software products—also known as identity man-

agement (IdM) solutions—promise to reduce the costs associated with application deployments and user management by aggregating control and visibility across multiple applications. They also protect an organization from network attacks by applying centralized security policies in a uniform fashion.

Maintaining a secure e-business infrastructure requires a comprehensive IAM system that maintains detailed profiles about each user's personal credentials and professional roles. Such

a system should establish rule-based and role-based policies about who can access information resources, and it should maintain those policies and profiles in one place for easy, coordinated management.

SKINNING A SLIPPERY CAT

Some companies have approached these security issues by enforcing separate access policies for individual software applications—each of which uses its own data repository to keep track of user identities. According to **Gerry Gebel**, an analyst at the IT research firm, **Burton Group**, this is very common, but usually not intentional. “It’s simply what happens when there is no plan or architecture in place, or when application owners are permitted to operate independently over time,” he says.

However it arises, this type of distributed IAM architecture soon becomes a liability as online business processes grow in number and

complexity, since developers must maintain different identity management frameworks for each application, and users must remember a growing number of usernames, passwords, and login procedures to access business systems.

In a perfect world, enterprises would deploy centralized enterprise identity management systems that use rule-based and role-based authentication, access control, and personalization technologies to target resources to each user—yet still permit delegated and distributed control. (See sidebar, “Benefits of Centralized Identity Management.”) While this is a lofty goal, Gebel believes devising a single repository to hold all identity, credential, and policy data is simply not realistic for large enterprises. “A more reasonable goal is to devise an IAM architecture where some data is stored centrally, shared data is synchronized between repositories, and application-specific data is maintained in local repositories,” he says. “Then, applications and IAM system developers know where to find necessary data and can use the appropriate access methods to retrieve it. Enterprises can use a mix of directories, databases, metadirectories, and virtual directories to accomplish this.”

This strategy introduces the notion of directory services. In a modern IAM system, virtual directories can combine multiple physical directories into a single view without the need to synchronize multiple directories. When properly integrated with the e-business infrastructure, this type of infrastructure makes it easier for system administrators to manage privacy preferences and exert central control over who is authorized to access personally identifiable information—without needing to physically centralize all IAM data. Identity provisioning solutions can then extend these policies to IT assets such as PCs, operating systems, e-mail systems, directories, relational databases, and legacy systems.

“Ideally, the system should be configured to control access based on business policies and user roles to ensure regulatory compliance,” continues Gebel. “Each business application must know who someone is, what their role or relationship is with the organization, and what resources and information they are permitted to access.”

METHODS OF AUTHORIZING USERS

It's imperative that organizations implement a secure identity management solution that leverages a common identity foundation across the entire infrastructure. The solution must include and integrate all critical components: policy-based identity management, access control, and auditing.

The first step to achieving this vision is to eliminate identity "silos" that separate business resources. Identity at most organizations is established with a username and password stored in a simple LDAP directory. For simple transactions, a text-based user ID and password are adequate. However, since ID/password combinations are easy to crack, organizations with higher security needs often rely on strong authentication methods such as tokens, smart cards, and biometrics to bolster their user authentication procedures. These organizations typically base their authentication methods on three identifying factors: what you know (usernames and passwords), what you have (unique identifiers such as encryption keys, tokens, or digital certificates) and who you are (biometrics such as eye scans, fingerprints, and face scans, all of which identify you uniquely).

Isolated LDAP directories work great for individual applications. But most users need to access multiple applications—some of which pre-date online business practices altogether. To solve the problem, IAM systems enforce security policies via identity profiles assigned to each user. Each profile might include a user's name, title, organization name, department name, function, level, contract details, employment type, and reporting relationship. Associated auditing and reporting applications track how users navigate the network and what they try to access, alerting administrators to anomalies or possible problems.

For example, consider the many types of users that contact an insurance company online. One group includes employees needing access to the company network via the Internet, intranet, or extranet. Another group includes independent insurance brokers who write business with the company. A third group includes customers who want to review their policies or make payments online. It's in the insurance company's best interest to allow each of these users to access its systems—after a proper >>

Benefits of Centralized Identity Management

- Streamlines user administration tasks, improving accuracy and efficiency
- Reduces help desk costs by simplifying end-user and administrative processes
- Boosts productivity by consolidating and automating IT administrative tasks
- Shortens application development lifecycles via a "build once, leverage always" model
- Simplifies interaction with customers, partners and suppliers
- Improves security via centralized management of passwords and security credentials
- Restricts access to corporate information by distinguishing legitimate users from intruders
- Helps managers comply with government regulations

In essence, organizations need to open their virtual doors to the world while ensuring that only the trusted walk through them.

authentication process, that is.

In response to these business requirements, IAM solutions solve two main functions: administration and real-time enforcement. Administration entails managing user accounts, user profiles, and corporate policies across the entire IT environment via a combination of user roles and business rules. Real-time enforcement is addressed by access management solutions that can authenticate users and enforce access control policies for each user of enterprise IT resources.

CASE IN POINT

Symetra Financial in Bellevue, Wash., has confronted these issues head on.

According to **Lynda Brown**, assistant vice president and IT director at Symetra, IT pros needed to rapidly implement an off-the-shelf access management solution to replace three homegrown access-management tools. Ideally, the new solution would allow employees, distributors, and customers to secure insurance-related applica-

tions through Symetra's Web sites via single sign-on procedures. Symetra selected Oracle COREid Access & Identity for the job because it provides a full range of identity management and security functions, including Web single sign-on, user self-service and self-registration, reporting and auditing, policy management, dynamic groups, and delegated administration.

In phase one of the project, Symetra rolled out the IAM system to roughly one million customers and 20,000 distributors, giving them cohesive access to a new method of authentication. In the second phase, Symetra plans to add centralized authorization and self-administration capabilities.

BUSINESS DRIVERS FOR IAM

Symetra's story illustrates the three primary business drivers for IAM software: bolstering security, increasing business efficiency and simplifying compliance initiatives.

Security is easy to understand: organizations must be confident in the integrity of business resources, systems, and services. Efficiency is the watchword for everything. IT pros must manage the processes related to provisioning and authorizing users while keeping costs down, so they can open up access to the right people in the value chain. The right infrastructure will simplify system administration and reduce help desk costs. It will also tighten the relationship between employees and the business resources they depend on to work productively.

With respect to compliance, nearly every type of organization around the world—from publicly traded corporations to hospitals, schools, and government entities—is subject to regulations that mandate privacy and accountability. Gartner research indicates that regulatory compliance spending is growing at a rate twice that of IT spending. In many cases, discretionary IT budgets are entirely consumed by compliance efforts, stifling initiatives that are important to business growth. No part of the global economy is immune to the impact of regulatory activity.²

The challenge is to ensure that the right people have appropriate access to the right resources at the right time—and to be able to disable access when a user leaves the company, or their responsibilities change. Not only that, but you need to be able to prove that you have these controls in place. When you have a central place to provision users and grant access rights, it's much easier to manage. For example, if access to your financial system is tightly constrained, it's a lot easier to prove that financial results were correctly concluded.

Segregation of duties is another key issue, since companies must ensure that users only have access to certain applications. For example, in a procurement system, the same person can't issue a purchase order and also approve payment against it. The provisioning system must enforce this separation of duties, and leave an audit trail so managers can prove to an inspector or regulator that a company has the correct controls in place.

Identity management is a base-level technology that provides fundamental infrastructure to automate the manual compliance controls that are in place. IAM solutions lower the overall cost of compliance by enforcing these >>



ILLUSTRATION BY TODD DAVIDSON

Employing a unified identity management framework has streamlined ordering, warranty processing, and communication via a single dealer portal that allows ordering across brands.

controls in a sustainable fashion, so managers don't need to revisit the same issues every year.

MAKING B2B CONNECTIONS

When properly implemented, IAM solutions enable users to take advantage of single sign-on capabilities, which means they can use a single desktop login procedure rather than trying to remember multiple passwords. Single sign-on technology makes life easier for help desk personnel and system administrators by

reducing time spent helping users who may have forgotten specific passwords for different applications, or who need general assistance with managing their access to applications and Web content.

It was precisely these business benefits that motivated construction and industrial goods leader **Ingersoll-Rand** to deploy a centralized identity management system. The company needed a way to help its 40,000 employee organization, along with its worldwide dealer network, com-

municate more effectively as a single entity. For IT manager **Jim McDonald**, that meant reducing the number of user IDs and passwords required for dealers, and creating a common front-end to ease the transition between sites and applications.

"We wanted to simplify things for our dealers by putting one common face on multiple applications," says McDonald. "By consolidating the interface down to one Web site where our dealers could transact and do business using one login procedure and password, we knew we could make it easier for them to carry multiple brands."

Ingersoll-Rand surveyed the landscape for identity management vendors. "Everybody had their fingers on some level of single sign on," adds McDonald. "The real differentiating factor was the ability to handle heterogeneous environments."

Ingersoll-Rand now uses Oracle COREid Access & Identity to pull disparate applica-

tions together—not only from a user administration standpoint, but also from a security standpoint. According to McDonald, the software includes plug-ins for various hardware and software environments so they can obtain single sign-on and user management capabilities right out of the box. "This middleware technology is very important to our business," says McDonald.

Managing a centralized directory of user privileges gives Ingersoll-Rand a single point of contact for user administration. It also improves service levels for customers, providing dealers with an easy-to-use portal interface and a single sign-on solution to navigate across different applications. Additionally, the centralized infrastructure streamlines user identity management as new applications come online or are removed from the system. "We estimate that about 20 percent of the application development process is spent on security," says McDonald. "We have essentially outsourced that activity to Oracle."

For Ingersoll-Rand, employing a unified identity management framework has streamlined ordering, warranty processing, and communication via a single dealer portal that allows ordering across brands. The new infrastructure allows the company's business applications to leverage centrally defined policies to grant rights to sensitive parts of an application, or permit and deny access to certain types of data based on employees' roles within the organization.

UNIFIED CONTROL THROUGH IAM SUITES

According to Gartner analyst **Roberta J. Witty**, enterprises with highly heterogeneous IT environments often see the value in implementing all-encompassing IAM solutions. However, many of these enterprises find these solutions difficult to integrate with their existing hardware and software infrastructures. In some cases, the answer is to choose a vendor that offers an IAM suite or has integrated other vendors' functionalities with a common identity administration facility.

Some IAM suites not only unify access and control functions among business applications, but also tie IAM policies to the underlying database—an approach that is appealing to

dthree, an online marketing management company based in Ontario.

dthree helps companies build brand awareness and nurture customer relationships via the Internet. Within this emerging market, where the online experience is married with information, dthree's expertise attracts premium clients such as **InBev**, **Johnson & Johnson**, and **Rogers**.

"Record-level security allows us to deliver results in a personalized fashion, and to use a generic portal to deliver business intelligence," says **Igor Nesmyanovich**, CIO at dthree. "Our identity management model is integrated with the database security model, so we can personalize front-end reports as well as back-end data marts."

dthree helps clients design and implement personalized marketing campaigns, deliver them through multiple channels, and analyze the results. According to Nesmyanovich, traditional marketing organizations typically don't have the expertise to devise truly interactive Web sites—let alone to effectively use the data they gain from their customers' online experiences. dthree helps these clients create, manage and promote online experiences that build lucrative, long-term relationships with their customers. Because its online applications are accessible to both internal and external users, IAM technology is an important part of dthree's infrastructure.

"On the Internet, we not only reach a wide audience for a comparatively low cost; we deliver different messages and formats to different segments," explains Nesmyanovich. "Privacy and security are big elements of our overall strategy because we are responsible for client data."

The foundation of dthree's services is a software platform called IntelliMaxx that presents customer profiles and purchasing trends to authorized users. Different users see different views of the same data, depending on their identities. For example, a senior executive might be permitted to view the results of 10 corporate brands while a brand manager might only be able to see one. "If a person logs in, we can ensure that the front-end portal view is personalized, and at the same time, the data view is personalized," says Nesmyanovich. "An executive and a brand manager can each run the same report, yet only retrieve data based on their security permissions." >>

Essential Ingredients of IAM

Today's identity and access management solutions must span a complete range of functionality—from initial identity provisioning to long-term management; from highly secure access to cross-organization deployment; from fine-grained authorization to federated trading relationships—all of which should be built on a robust and well-proven security infrastructure. A comprehensive solution should include the following essential ingredients:

- **Directory Services** that provide a single centralized LDAP-based repository for user management, along with advanced productivity-enhancing features such as dynamic groups, user self-registration, and multi-directory integration. These services also include virtual directory technology to ensure no single vendor's LDAP directory is required to tap into identity data residing elsewhere.
- **Identity Administration** capabilities to help reduce security risk by governing how digital identities, groups, and organizations are created, maintained, and leveraged throughout an organization. The solution should provide a simple, controlled means to change user, role, group, and organizational information that dynamically affects access privileges.
- **Authentication, Authorization, and Single Sign-On** to manage who has access to what information and when. Single sign-on delivers dramatic cost savings by reducing time spent with thousands of users addressing password reset and update issues.
- **Federated Identity Management** to link internal employees to external portals, or external constituents to internal portals, without the burden of managing their identity and credential information in both places. This drastically reduces the costs and complexity of managing partners' users, and accelerates the adoption of networked business portals.
- **User Provisioning** to manage the creation of and on going changes to users and their privileges. This includes connecting users to the resources they need to be productive, and revoking unauthorized access to protect proprietary information.
- **Web Services Management**—in a service oriented architecture, to expose business applications and information to the Internet for use by customers, business partners, and employees. A robust, secure framework is critical for managing access control, monitoring, and auditing these services.

As more companies move their business processes to the Web, they find themselves with a greater need to extend the boundaries of their enterprise to include partner applications.

These users also enjoy the cohesion of a portal that is connected to multiple applications, enabling them to access several information systems with a single user name and password. “We have one portal that uses the same security model throughout our infrastructure,” confirms Nesmyanovich. “It works with Microsoft Active Directory to decide which information should be shown to intranet users, and Oracle Internet Directory to control access for extranet users. We don’t need to create accounts in the internal system for our external users, yet these people can log in and see relevant information.”

EXTENDING THE BOUNDARIES OF THE NETWORK

As more companies move their business processes to the Web, they find themselves with a greater need to extend the boundaries of their enterprise to include partner applications. The tricky part is to manage access to these applications without negating the Web’s real value as an open, ubiquitous network—and with-

out creating new administrative headaches for the IT department.

“Federating” identity data allows multiple companies to operate independently, yet cooperate for business purposes. Federation servers provide cross-domain single sign-on to help organizations securely link their business partners into a corporate portal or extranet while also increasing their compliance with privacy and security regulations.

For example, a hospital and a lab might wish to link their business applications so authorized users can order tests and access patient records without additional logins. Due to HIPAA regulations, both healthcare providers must ensure that these patient records remain confidential. If a hospital sends a record to a third-party laboratory, the hospital is liable for the confidentiality of that record.

In this case, the hospital might create a Web portal that physicians can use to order lab tests.

Behind the scenes, a federated identity system protects patient privacy without requiring doctors to maintain unique user IDs and passwords.

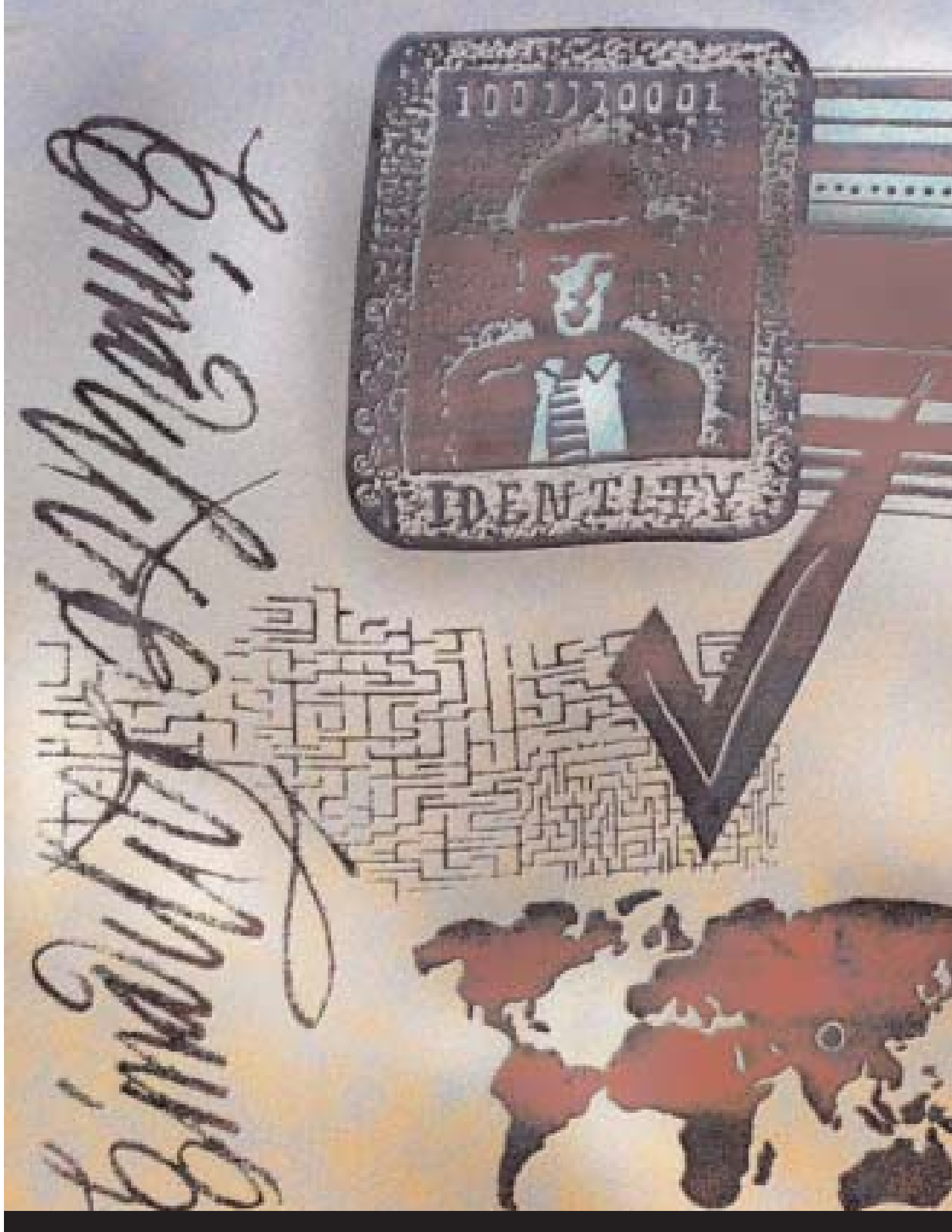
These same business dynamics are at work throughout the commercial business world. For example, if a real estate company has a partnership with a mortgage broker, their joint customers should be able to move online among related business applications without the need for a second login procedure.

According to the Burton Group’s Gebel, each of these scenarios implies sharing limited aspects of identity between security domains. “Federated identity enables two organizations to administer their own users and interact with business partners utilizing industry standards,” he says. “Each domain registers users, validates their identity, issues credentials, and assigns a profile to control access within the enterprise and at partner sites. During runtime access to partner sites, users authenticate locally and are granted access to partner systems based on sharing limited user attributes through federation standards. It is no longer necessary for partners to maintain excessive information about an enterprise’s user community.”

The business community drove the requirements for federated identities because they already had these kinds of relationships and they wanted to be able to express them technically. Standards such as Security Assertion Markup Language (SAML) are now making it easier to swap these kinds of trust credentials. As enterprises externalize their business processes over the Internet to customers and trading partners, the need for these secure, federated exchanges will become more common.

A centralized identity management solution helps an organization orchestrate an ever growing set of IT resources, allowing a diverse set of people to interact with the network in a personalized and secure way. This approach not only protects network resources and safeguards financial assets, but also enables the auditing and reporting capabilities necessary for high levels of security and compliance.

It’s very likely that this type of federated technology will soon extend beyond business transactions to accommodate social interactions as well. Web sites devoted to music, entertainment, politics, hobbies and gaming can all benefit from a managed exchange of identity. >>



A complete IAM system should include a software solution for managing the operations of Web services and the interactions between these services.

HISTORICAL PRECEDENTS FOR IAM

Many of these security issues are easier to understand against the backdrop of history. IAM is a relatively young concept. It started with directory management tools in the '90s, which took the form of simple repositories of user information, privileges, and access rights. Later came single sign-on, which involves consolidating access privileges through a centralized repository. Then came identity administration—a set of programs and procedures that

help administrators manage large repositories of user information.

Up until the mid '90s, most workers accessed only a handful of business applications, such as a work-specific application for finance or sales force automation, e-mail, and perhaps a virtual private network (VPN) application for communication. Today, workers commonly depend on a dozen business applications or more, from expense reporting applications to investment portals.

While HR is the logical starting point for user authorization and identity on a corporate intranet, Gebel believes that over time the industry will see this same emphasis within supply chain management and customer relationship management applications, since these business systems represent key contact points for members of an extended value chain. The logical strategy to accomplish this takes the form of a three-part progression:

- Build identity management into your business processes as part of e-business applications
- Make it a part of your application development and deployment framework via middleware services
- Enable these functions as independent Web services via a service oriented architecture

INCORPORATING WEB SERVICES

Today, as the IAM business continues to evolve, the hot areas are user provisioning, federated identity, and Web services management.

What's happening with Web services today is very similar to the genesis of identity management technology eight or 10 years ago, as people started depending on more and more software applications.

Identity management systems have typically been focused on securing and managing user-to-application interactions. However, many organizations also need to manage interactions between the applications themselves. Web services provide a standard and simple way to connect applications over the Internet, but they require management of security and other runtime operations to work effectively.

A complete IAM system should include a software solution for managing the operations of Web services and the interactions between these services. This includes tools for building security and operational policies that can be layered over new or existing applications. It also requires runtime facilities for intercepting calls to and from an application or service and then executing these policies. Finally, it should have dashboards for monitoring these policies as they execute, so administrators can maintain adequate service levels and troubleshoot potential problems.

"Identity management systems must contend with the growing use of Web services applications," says Gebel. "Web services applications should be able to integrate easily with an enterprise's identity infrastructure. For example, a Web services-based application could make an authentication service request to an IAM component that supports a service-oriented architecture."

IAM will gradually move from application-based identity management to Internet-enabled *entity management*. Centralized servers will govern access and control as they carry out the business policies of the organization, enforcing security for users, applications, devices, and other IT resources.

WHERE'S THE PAYOFF?

While CIOs may complain that security technology is a necessary evil with no real ROI, IAM software pays off in several ways. For one thing, there are fewer password resets, meaning fewer help desk calls. Secondly, employees are more productive because they no longer have to manage multiple usernames and passwords. Centralized IAM software also facilitates regulatory compliance, and it helps developers deploy new systems faster, since they already have a security infrastructure in place that they can leverage.

In the long run, IAM ensures greater business agility as well. As companies wrestle with increasing IT management costs, more stringent regulatory compliance issues, and a host of complex security vulnerabilities, integrating IAM solutions into the application development process enables them to design cohesive identity management systems that support multi-vendor applications.

It's not enough to simply provide identity and access management tools. Customers need those functions to closely support the business functions of the entire enterprise. [s]

About the Author: **David Baum** (david@dbaum-comm.com) is a freelance business writer with more than 20 years experience writing about emerging technologies for publications such as *InformationWeek*, *Computerworld*, *InfoWorld*, *iQ*, *Packet*, *Oracle Magazine*, and *Profit Magazine*.¹

FOOTNOTES

- 1 PLUMMER, DARYL C., ET. AL., "GARTNER'S TOP PREDICTIONS FOR 2006 AND BEYOND" (NOV 2005).
- 2 WITTY, ROBERTA J., ET. AL., "IDENTITY AND ACCESS MANAGEMENT DEFINED," (NOVEMBER 2003).

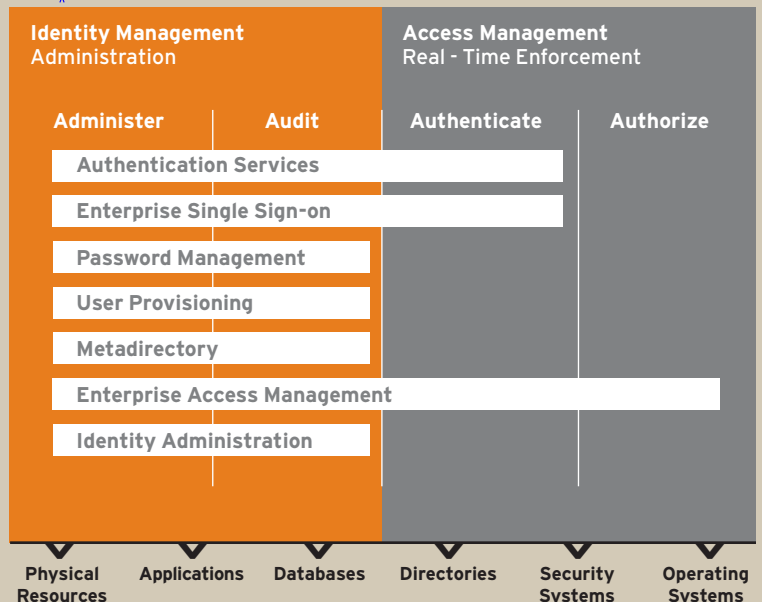


Four Pillars of Information Security

Gartner analysts recently identified four "A's" of information security.

- Enterprises need to ensure that users are properly identified and that these identities are validated to IT resources (*authentication*).
- They need to know that users can only access what their job function allows them to access within the enterprise (*authorization*).
- They need to have a consolidated method for managing user access (*administration*).
- Finally, they need to ensure that the activities associated with user access (administration and real-time enforcement) are logged for day-to-day monitoring, regulatory and investigative purposes (*audit*).¹

FIGURE 1:



User identities, transactions, roles, policies and privileges.
(SOURCE: GARTNER RESEARCH)