

[**Editor's Note:** The following excerpt is from Chapter 5 of the free eBook *The Definitive Guide to Security Management* (Realtimerepublishers.com) written by Dan Sullivan and available from a link at <http://www3.ca.com/ebook/>.]

## Chapter 5: Identity and Access Management

The concepts of identity and access are central to security management. Such was the case in the past when mainframe computing was the dominant paradigm and it is still true today—when distributed computing models, such as Web services, define the dominant model for system design. The emerging use of Web services can potentially create very large user populations and relatively open access to computational services. This chapter will focus on the challenge of managing large user populations through identity and access management (IAM).

 Chapter 6 will address access management.

Identity is a fundamental concept about how we manage information about persons allowed access to information, applications, and services. An identity must exist before a user can do productive work. At the same time that identities are used to control access to data, that same data must be protected to ensure data integrity and privacy of confidential information. Identities and access management are fundamentally linked and cannot be separated.

Logically, a person should have one identity. However, the need for access has helped to create silos of identity and access domains that are costly and difficult to manage. However, these concerns involve more than administration costs. Managing risks—such as information theft, breaches, and attacks—increasingly depends upon effective identity and access management. Regulatory compliance also entails identity management, access control, and tamper-proof audit controls that are substantially more difficult in silo-like environments.

Effective identity management depends on integrating user management (provisioning and identity management), controlling access to resources based on identities, and auditing activities with protected assets. Identity management is not an optional practice—organizations are driven to identity management by the need to:

- Reduce costs and improve operational efficiencies
- Comply with regulations
- Enable more agile business operations
- Mitigate risks

Identity management has always been an integral part of IT management but emerging technologies, increasing risks, and the need to comply with government regulations are putting the spotlight on this central area of security management.

## Spotlight on Identity

Identity management is the process of provisioning access to resources by establishing identity information, using that identity for access control, and managing the repository of identity and access control information. In the simplest case, an identity is equivalent to a user ID on a single system. The ID has a range of attributes, such as name, department, and a list of organizational roles. More typically, an identity is associated with users or services that have multiple user IDs on a variety of systems. For example, a user can have user IDs on:

- A network file system hosting shared directories
- Multiple mainframe applications
- A customer relationship management (CRM) system
- Enterprise data warehouse
- Supply chain partner's fulfillment application

In fact, according to Gartner Research, the average internal user has 18 accounts. In fact, staff, partners, and customers are not the only identities in an IT environment. Consider a United States bank that must comply with the Graham-Leach Bliley (GLB) Act. To do so, the bank must manage, report on, and audit employee activities with customer transactions as well as the activities of business partners and customers who have access to protected data. The cost of complying with GLB in an environment averaging 18 accounts per internal users is unsustainable in competitive markets. Understanding and managing users and service accounts with access to IT servers is a basic security management task. Regardless of whether an organization has formal procedures or an identity management system, the organization still has to manage identities. The questions that must be address are: How well are identities managed? and How much does the management cost?

As we examine the business drivers for improved identity management, it is crucial to recognize that identity management is not optional—any organization with multiple systems and multiple users is already managing identities. The goal is to lower the cost of identity management, comply with regulations, and mitigate security risks.

## The Need for Identity Management

The nature of a “user” has evolved over the past decade. In the past, a user was typically an employee of an organization who used a terminal to access a mainframe or mini-computer. Changes in business models are driving changes in the pool of users. Now, consultants, contractors, business partners, and customers are using systems that were once limited to a much smaller internal user base.

### *Who Is in the IT Environment?*

There are many types of users in an IT environment: employees, contractors, consultants, supply chain partners, and customers. How do administrators and security professionals know who is who? There are several potential sources of identity information:

- Employees and contractors are tracked in a human resources (HR) system.
- Contractors are tracked in an accounts payable system.
- Consultants are not listed in the HR system, but if they have physical access to facilities, some identifying information could be logged in the facility’s management security system.
- Customers are listed in one or more customer databases.
- Supply chain partners may be managed on an ad hoc basis with no centralized repository.

Where can a security manager go to get identity information about all users across all systems? If silos of identities exist, costs and risks skyrocket—organizations need to be aware of, control, and track who has access to what. Without a centralized mechanism for identity management, security professionals must depend on cobbled together information from other systems to ensure compliance and security.

Non-security systems, such as HR and customer databases, have become surrogates for identity management systems. These systems can provide some basic user identity information, but they cannot provide other essential services, such as auditing and access controls. It is also time consuming and very costly for security professionals to piece together identity information from multiple sources, especially when the systems track different information and use different formats for data. With user populations being very dynamic, silo and disjointed identity efforts will only continue to drive up IT costs and increase risks. In such an environment, it would take an army of administrators to address day-to-day user changes. Only a consolidated repository of identity information that supports auditing and access control can effectively and efficiently track users.

### **What Can Users Do?**

A greater challenge to identity management is knowing in detail what users are enabled to do. Access controls in most organizations are distributed across multiple platforms:

- Windows servers are used for network file systems
- Linux servers are used for Web servers
- UNIX systems run back-end database applications
- Mainframes run core operational systems

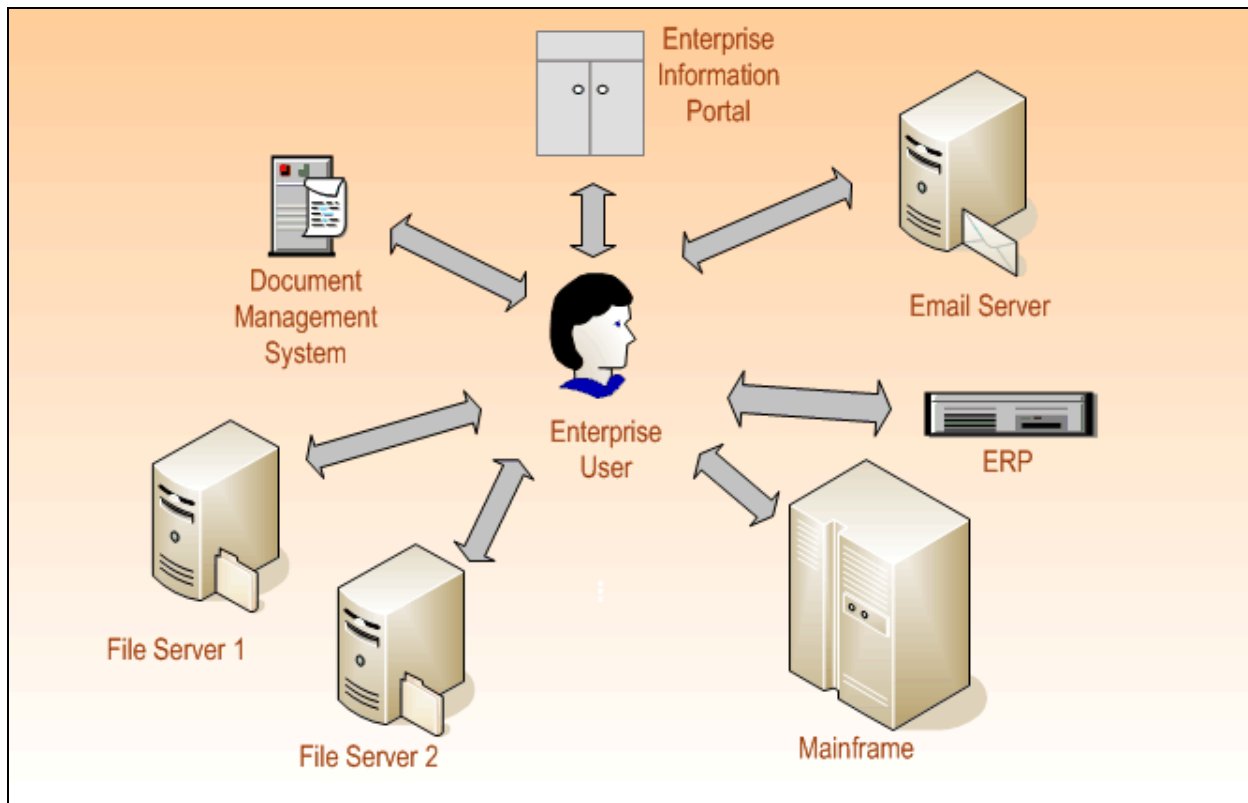
No one platform can meet all the needs of an organization. The fact that platforms apply different access control mechanism means that there will not be a single access control function without a specialized application. Lack of centralization also makes user identity and access provisioning an increasingly difficult task. As you can see, all of these challenges are interconnected.

### **The Need to Provide Access to Multiple Resources**

Consider the process of adding a new employee to an organization, for example, a mid-level manager. The person will need to be provided access to systems such as (see Figure 5.1):

- Workstation
- Several network file system directories
- A number of ERP modules
- A business intelligence reporting system
- Email system
- Document management system
- The enterprise portal
- Several discussion forums within the enterprise portal
- A mainframe application for production reporting

The type of access granted depends on several factors. Workstation and some network directories access are dictated by the employee's physical location. Access to other network directories, ERP modules, business intelligence reporting systems, and other systems are a function of the employee's organizational role. Still others, such as membership in discussion forums, are granted based on the discretion of the discussion moderator. Again, often there is no single place an administrator can turn to add a new user. The challenges to managing the breadth of account and access control decisions are much greater without a unified identity management process. To make this situation even worse, without a centralized identity management function, this set of events is repeating itself over and over throughout an organization.



**Figure 5.1: A single role within an organization can require multiple identifiers to access IT resources.**

Similar problems occur when a person terminates. HR may know a person has left the organization, but does the mainframe administrator know? How about the database administrator that manages user roles for the data warehouse reporting system? Terminating software developers raise additional concerns. Have they used shared accounts in development and test environments? Do they know administrator passwords to development servers? If so, those passwords need to be changed. The following list highlights examples of the damage caused by former employees who retain access to systems:

- For several days, a \$1 billion per year computer monitor manufacturer's Taiwan office was unable to access critical files that were deleted by a former network administrator that had been terminated 2 weeks earlier.
- A former AS/400 programmer caused \$80,000 in damage to his former employer after breaking in from a remote location.
- After being terminated, a former administrator to a transportation services company deleted the company's customer database and changed system passwords.
- After being fired, a former employee accessed his company's servers, deleted 675 files, changed access control levels, altered billing records, and sent email with false statements about the company to hundreds of its customers.


For more information about these and similar cases, see the Department of Justice cybercrime Web site at <http://www.usdoj.gov/criminal/cybercrime/cccases.html>.

## Complying with Regulations

Business and governments are subject to a range of information security regulations created by federal, state, and international governing bodies. In addition to GLB, which was mentioned earlier, some of the best-known regulations are the Sarbanes-Oxley Act, the Health Insurance Portability and Accountability Act (HIPAA), California Senate Bill 1386, the European Union Privacy Directive, and the United States Food and Drug Administration (FDA) pharmaceutical regulation, 21 CFR Part 11. Commercial organizations are not the only ones subject to regulation—United States government agencies are subject to several regulations, including the Federal Security Information Security Act (FISMA).

Regulations often fall into two categories:

- Ensure privacy—Requires that “appropriate” access to personal data is managed and that auditors are provided with tamper-proof tracking of activities
- Ensure data validity—Requires that “appropriate” access to financial data is managed (only authorized users can change data) and that auditors are provided with tamper-proof tracking of activities

 The following sections briefly explore these regulations. Chapter 8 will cover regulations in more detail.

## The Sarbanes-Oxley Act

The Sarbanes-Oxley Act was passed in the United States after a series of high-profile accounting scandals. The goal of the act is to protect investors and other stakeholders in companies that report financial information to the public. Companies, and especially its officers and directors, are responsible for preventing financial fraud. They are also required to implement procedures that control and monitor operations related to financial management. This requirement includes controlling access to financial and related information (such as sales projections), auditing changes to that information, and reviewing those audit logs to ensure compliance.

## HIPAA

HIPAA defines medical records and related information as protected health information that is subject to particular controls. The protected information ranges from details of a patient’s condition and diagnosis to personal identifiers, such as names, phone numbers, account numbers, and biometric identifiers (for example, finger prints and voice prints). Failure to comply with data protection standards carries fines of as much as \$25,000 per year per standards violation.

### California Senate Bill 1386

California Senate Bill 1386 requires companies doing business with California residents to notify those customers of any security breach where there is a reasonable belief that the unauthorized person accessed unencrypted personal information.

### The European Union Privacy Directive

The European Union Privacy Directive requires businesses collecting information about member country citizens to follow several regulations related to:

- Data collection transparency
- Limited purpose of data collection
- Data quality
- Controlled transfer of data
- Special protections for sensitive data, such as information identifying race or ethnic origin, religion, and political opinions.

Transferring information outside of European Union countries is prohibited unless adequate safeguards are in place in the target country.

### 21 CFR Part 11


The United States regulations on the development of pharmaceutical products, known as 21 CFR Part 11, dictate information security controls, including:

- Protection of records
- Access controls
- Authentication
- Audit trail controls
- Authority checks
- Electronic signature security

The objective of these regulations is to ensure the integrity of drug development and related biotechnology processes.

### Government Regulations of Government Agencies

Governments are also required to comply with security regulations. For example, United States federal agencies are subject to National Institute of Standards and Technology (NIST) guidelines on information security that emphasize continuous monitoring. A recent survey by the Government Accounting Office (GAO) found that systems at four agencies did not always have routine quality review processes to determine whether the guidelines were met. The reason: obstacles to implementing the guidelines, including lack of resources and staff.

 The GAO report, "Information Security: Agencies Need to Implement Consistent Processes in Authorizing Systems for Operations," is available at <http://www.gao.gov/new.items/d04376.pdf>.

Compliance issues are faced by organizations, both commercial and government. The motivations for regulations range from ensured privacy to public safety. The specifics of the requirements vary but a common theme across regulations is the need to protect the integrity of information and the need to understand the history of changes in information through adequate audit controls. With a growing numbers of users, systems, and regulations, a centralized management system, along with formal policies and procedures, is a cornerstone to meeting those requirements.

## Benefits of Identity Management

The benefits of identity management center around three areas:

- Economies of scale
- Improved system integration
- Operational cost reductions

### *Leveraging the Economies of Scale*

All IT applications have a need for identity and access controls. Every time someone uses an IT resource, from a desktop word processor to an ERP system, some level of authentication and authorization is required. Developing and maintaining authentication in each system is obviously inefficient. Consider a simple interaction with an enterprise information portal:

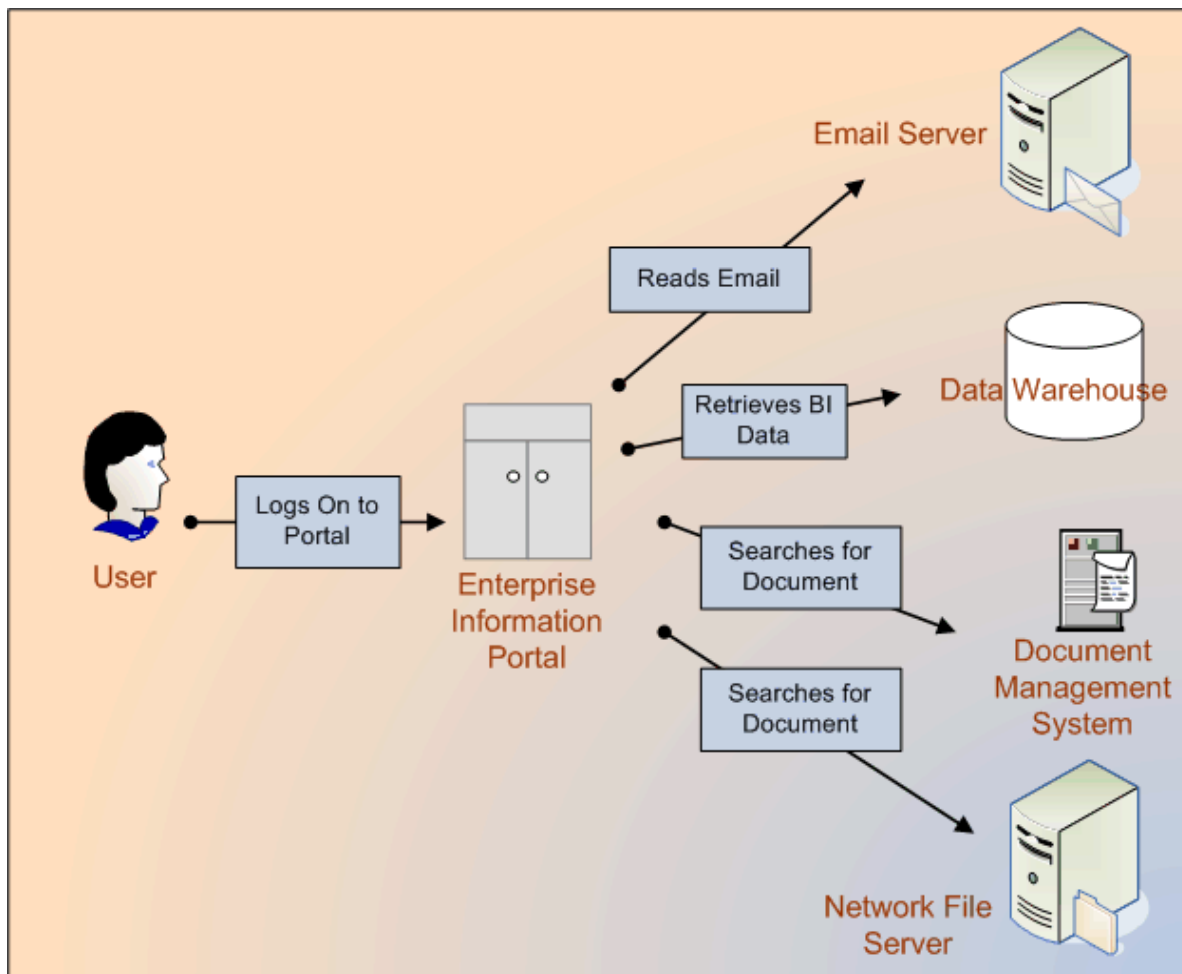
- User logs on to the portal
- User reads email in a Web client deployed through a portlet
- User reviews a detailed display in a business intelligence dashboard
- User searches for document on a new marketing initiative

In this example, as Figure 5.2 shows, a total of five systems are accessed for this session. (A search can span multiple systems. Before a document is retrieved by the search system, the application ensures that the user has appropriate access to the document.) From a development perspective, authentication is better done through a centralized service rather than developing separate mechanisms for each application. When there are many users and several applications within a changing environment, the need for identity management increases.



## Managing Identities in Distributed Environments

Windows developers can use the desktop OS' user management controls to identify a user and control access to functions and services. If the application needs data or services provided by another server, the authentication may become more complex. If the other application also uses Windows authentication services, there is no additional complexity from the developer's perspective. For example, a Microsoft SQL Server database that uses Windows authentication can provide data to a Windows client application without additional authentication. If the database runs on a Linux server and does not interoperate with Windows authentication, an extra authentication step is required.

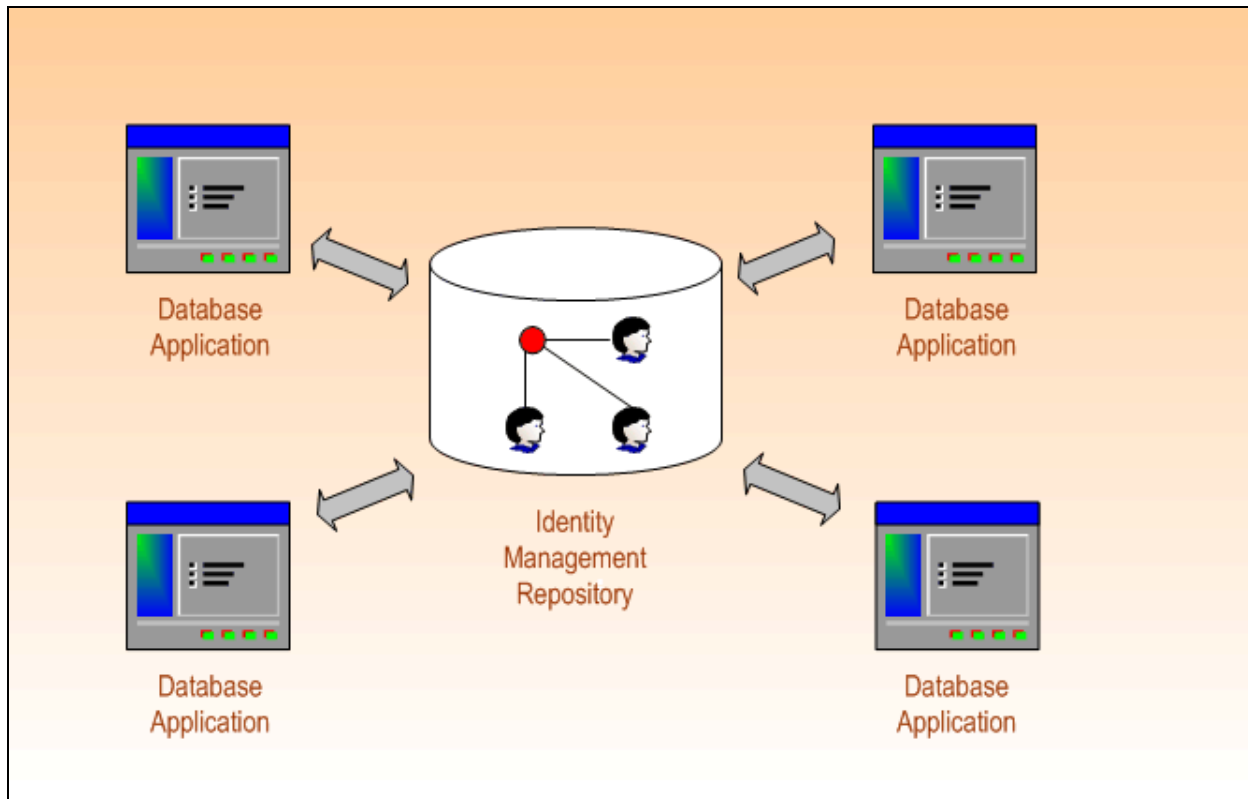


**Figure 5.2:** Routine tasks, such as reading email, reviewing a report, and searching for documents can require multiple authentications.

Database systems provide user and roles management services. A common practice among database application developers is to create user accounts within the application itself. Doing so leads to a proliferation of accounts even across the same database server. For example, a user would have one account to log on to a transaction processing system and another account to log into a reporting system.

This scenario requires database developers and administrators to create and manage redundant roles and accounts. As the number of applications grows, so do the administrative headaches. A more efficient method for large-scale deployments is to use a centralized authentication and authorization service.

With an identity management system, users and their roles are defined once. Designers develop applications to use common authentication services provided by the identity management system rather than using OS- or database-specific user IDs. Any change to a user's identity record is made once and then is immediately available to all applications that use the centralized system (see Figure 5.3).



**Figure 5.3: Centralized identity management reduces the amount of application-specific authorization management.**

### **Rewards of Integration**

Integration is the hallmark of enterprise applications. Information integration has long been a concern at large and mid-sized organizations. In the past, and sometimes today, applications are developed as information silos. This design does not reflect the way work actually flows through organizations. Orders placed in one system need information from inventory control applications; fulfillment systems need information from the customer order system; accounts billable programs need data from both the order and fulfillment systems. ERP systems have evolved to incorporate these functions into a single application. They use a common architecture and Application Programming Interfaces (APIs), which ease information sharing with other systems. The same principals apply to security integration.

When developers must code for different authentication systems (Windows, UNIX, mainframe, and so on), the time and resources required to develop, debug, and maintain are greater than if a single authentication mechanism is used. These costs can be significant and negatively impact the level of controls put in place. The goal of using a single authentication and identity management system begs the question: Which mechanism works across the diverse platforms found in today's heterogeneous environments?

Several non-proprietary standards have been created to support essential components of identity management:

- User provisioning
- Access control, authentication, and authorization assertions
- Policy definition
- Directory management

These standards are discussed in more technical detail in the sidebar “Industry Standards for Identity Management.”

#### **Industry Standards for Identity Management**

Industry standard protocols are enabling cost-effective identity management. The major protocols are:

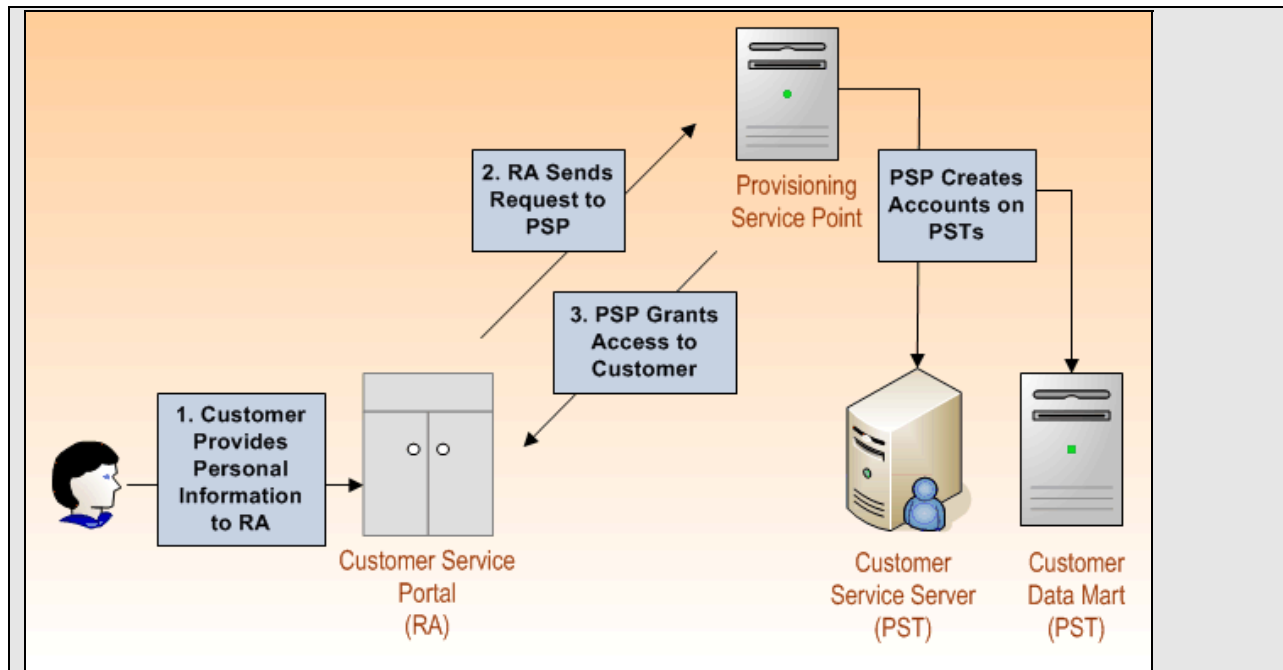
- Service Provisioning Markup Language (SPML)
- Security Assertions Markup Language (SAML)
- eXtensible Access Control Markup Language (XACML)
- Lightweight Directory Access Protocol (LDAP) and X.500
- Directory Services Markup Language (DSML)
- Universal Description Discovery Integration (UDDI)
- Liberty Alliance specification
- WS-S (Web Services Security)

These standards function together to support the full life cycle of identity management, from provisioning through execution of access controls and management of identity directories to deprovisioning.

Service Provisioning Markup Language (SPML) provides a standard protocol for provisioning and deprovisioning users and resources without using proprietary APIs and for communicating with other identity management systems. It also has methods to query, suspend, and reactivate users and their accounts across distributed systems. The protocol uses three entities:

- Provisioning Service Points (PSPs)—Servers that respond to requests for provisioning
- Provisioning Service Targets (PST)—Systems controlled within the provisioning system
- Requesting Authority (RA)—Entities requesting access to a system

As Figure 5.4 illustrates, PSPs accept requests from RAs to gain access to resources, the PSTs.



**Figure 5.4: SPML enables centralized control of provisioning through PSPs.**

SAML is used to describe the characteristics, roles, and privileges of a user or a resource within a security domain. (These XML-based assertions enable authentications to be shared among trusted applications resulting in Web Single Sign On—SSO.)

XACML is used to exchange requests for and results of access control decisions. XACML consists of two parts, a policy definition language for describing which access rights a user has, and a request/response language for exchanging that information. The policy definition language lets administrators restrict activities—such as reading, writing, and updating an object—to a user based on the roles and attributes the user has. This language can also specify access control criteria based on protocols, for example, denying FTP access. For more technical details about XACML, see “eXtensible Access Control Markup Language (XACML) version 1.0” at <http://www.oasis-open.org/committees/download.php/2406/oasis-xacml-1.0.pdf>.


Several directory protocols are used for managing identity information, including X.500, LDAP, and DSML. X.500 is the overall protocol for directory namespace, query, and update services and is an extensive protocol. LDAP is smaller protocol with fewer features but is more easily implemented than X.500. It also manages namespace, query, and update services, so it is often used for identity management services. DSML specifies a means to describe structure of a directory in XML format. Version 2 of the protocol includes methods for describing directory queries and updates in XML.

UDDI is a protocol for maintaining directories of information about Web services, including security-related services.

These protocols all provide underlying services required to manage identities. The Liberty Alliance and the WS-Federation are creating broader initiatives to manage identities across organizational boundaries. This development is commonly known as federated identity management. Federated identity management is an emerging process and the two frameworks are likely to evolve and develop further.

### **Operational Efficiencies: Cost Reductions and Improved Operations**

Typically, IT projects are justified based on return on investment (ROI) or similar capital expenditure analysis. These methods quantify costs and benefits and compare results to determine which projects hold the greatest financial promise. Common costs in IT initiatives include the initial costs of hardware, software, installation, and customization, as well as ongoing operational costs, such as maintenance and administration. Less well-understood but just as important are adjustment costs related to changes in business processes that are made to realize the potential value of an investment. Some benefits of a technology investment are easily quantified, such as a reduction in workforce or replacement of more costly equipment. Other benefits are more difficult to measure. For example, improved identity management may enable the deployment of a sales support system that allows account representatives to share information about clients, proposals, and contracts. The collaboration that follows from using such a system may improve sales but one may not be able to definitively identify a formal cause-and-effect relationship between the application and the business outcome.

 Chapter 7 explores adjustment costs and ROI in more detail.

When assessing the value of identity management, it is also useful to consider the cost of *not* implementing a solution. In such as case, organizations would still incur real costs relating to provisioning (for example, Help desk—such as password reset, and redundant identity efforts). Without identity management, multiple administrators would need to add new accounts when an employee, contractor, or consultant joins the organization. Help desk costs for password resets would continue. The organizations would also continue to run the risk of not removing access to all accounts when a user terminates. With an identity management system, de-provisioning is centrally managed; removing a user's rights from the identity management systems ensures that the user is removed from all target platforms as well. As noted earlier, the cost of not curtailing access to former employees and contractors can be the cost of recovering from an insider attack.

Without identity management, organizations are still required to comply with privacy, confidentiality, quality assurance, and financial integrity regulations. Many regulations require proof of compliance through audit controls. Without a centralized identity management system, any audit trail that is kept is distributed across multiple systems and is difficult to aggregate. Even with the best intentions to comply, it is difficult and costly to enforce the same level of compliance across all administrators. Monitoring silos of audit information will also incur costs not associated with a centralized monitoring mechanism.

There are also unknown or difficult-to-measure costs associated with not implementing an identity management solution:

- What is the value of lost confidential information?
- Could the disclosure of client information cause the loss of future business?
- How would the disclosure of confidential marketing information to a competitor affect a marketing initiative?
- Do employees make copies of documents describing proprietary processes before they leave?

Cost reductions come in the form of hard cost savings, such as reduced support desk costs, and in soft cost savings, such as reduced risk in disclosing confidential information. Again, regardless of whether an organization deploys an identity management system, the organization will still incur the cost of managing identities. In the following section, the discussion shifts away from the technical and business benefits of identity management to an examination of the functional requirements of those systems.

## **The Structure of Identity Management**

The growing complexity of distributed IT environments that can span organizational lines is driving the need for effective and cost-efficient identity management. Open standards are in place and others are in development that enable cross-vendor authentication and authorization services. For many organizations, today's most pressing questions center on what to look for in an identity management system and how to deploy one. Important dimensions of identity management systems include:

- Technologies and components that make them up
- How they work across organizations
- How they work in heterogeneous environments
- Tightly coupled processes
- Management and administration
- Their integration with other information security management systems

### ***Constituent Technologies***

Identity management systems provide several services across broad, heterogeneous environments. To do so, the systems use several key technologies:

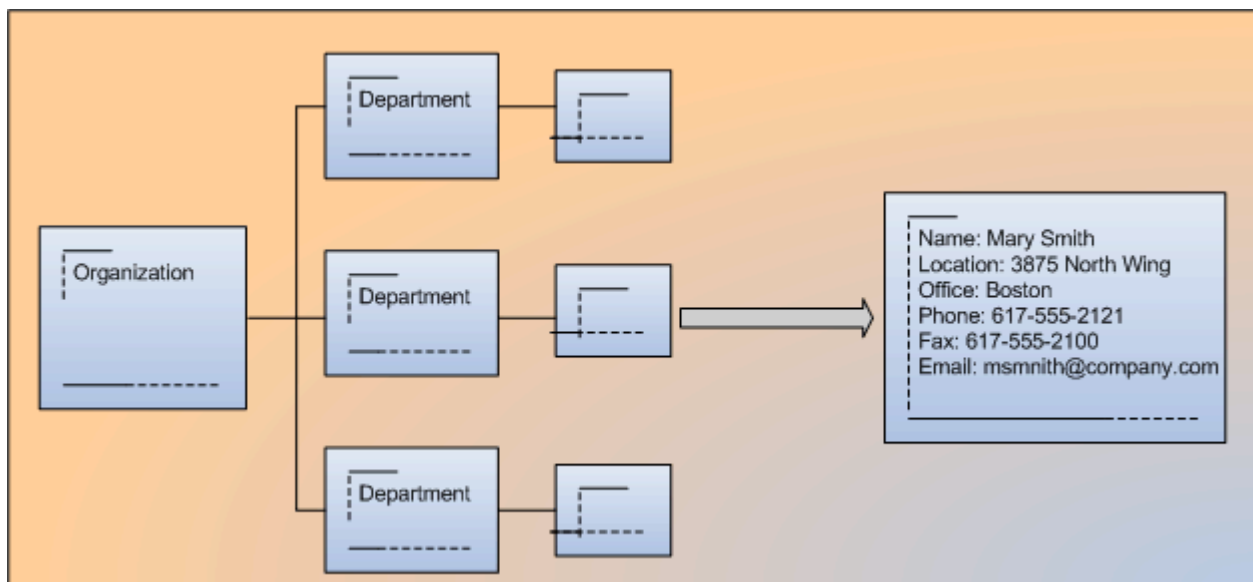
- Directories and virtual directories
- Provisioning
- Identity administration
- User self administration
- Password management
- Auditing

## Directories

Identity and access management involves users, and users are stored in directories. Through standards, directories provide a platform- and vendor-independent security service. They avoid duplication by managing shared information such as profiles and policies, and help provide common services such as authentication and authorization.

The great benefits of directories is realized when common functions are delegated to the Directory Service, and “directory-enabled” applications leverage the directory to avoid having to develop and maintain their own information base about users, customers, suppliers, or other applications (see Figure 5.5).

Though directories are similar to databases in that they store information, in a distributed environment, directories are much more flexible, secure, and easier to interface to. Directories provide a naturally object-oriented, dynamically configurable repository with standards for access, security, and information management. They differ from databases in that they are service oriented, instead of storage oriented, and, out-of-the-box, directories provide security, speed, distribution, replication, universal data types, and extensible rules for managing information. To facilitate potentially unlimited scalability, directories organize their data hierarchically.



**Figure 5.5: Directories are hierarchical databases of information about named objects, such as employees, customers, and partners.**

Directories are designed for fast response times to queries as information in a directory is generally queried much more often than it is updated. Reliability is also a key concern for enterprise directories, which is the reason that directories built on top of relational databases are preferred over directories that have proprietary information stores.



## Implementation Options for Directories

Two common directory standards are X.500 and LDAP. X.500 was developed first and is used in large-scale directory deployments. LDAP was developed as a simple string-based interface for accessing an X.500 directory.

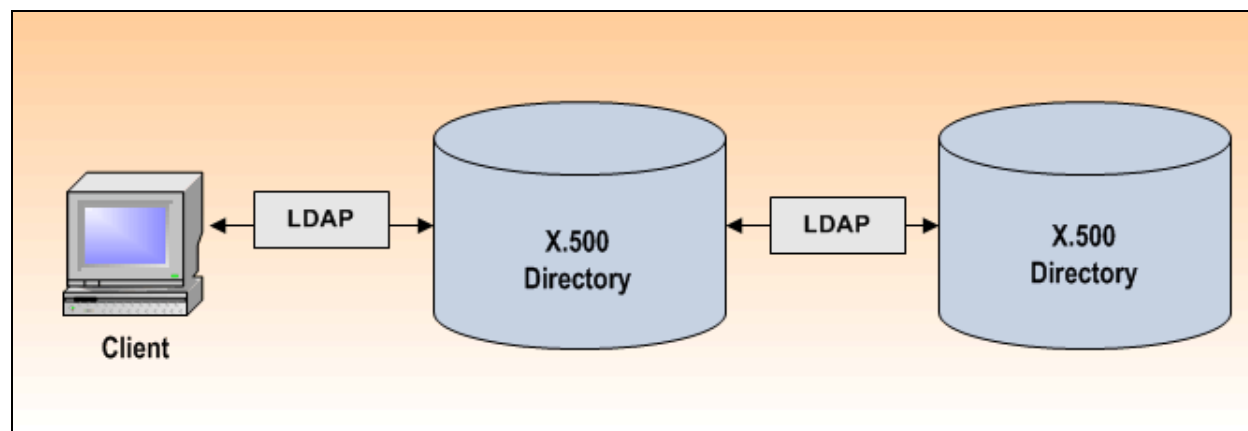
Contrary to popular opinion, LDAP and X.500 are complementary. LDAP is a client-to-server protocol, and X.500 defines server-to-server protocols required for distribution and replication. It is better to support both protocols rather than just one.

### Standalone Directories

There are many “LDAP-only” products on the market. These directories provide adequate departmental solutions but do not scale into Internet-facing solutions, and electronic business requires distribution and replication across multiple locations. If there are more than one in an organization, the directory information is segmented into “islands” because LDAP-only servers cannot communicate between themselves in any standard way. Technically speaking, LDAP-only servers cannot “chain” queries to other LDAP-only servers; instead, they use “referrals” between directory islands. This communication method requires much more interaction from applications and means that the directory network is not transparent to the end application.

### Distributed Directories

A distributed directory, sometimes called a backbone directory, provides a seamless view of information to the user or application. A backbone directory allows information to be distributed across many servers, perhaps hundreds of servers, in a way that is transparent to the user. This distribution is analogous to a telephone or mobile phone network—the user is unaware of how many servers are in the network. The difference between a backbone directory and a set of standalone directories is the provision of high-speed switching and routing services. The backbone is composed of many directory servers linked together, and all necessary servers cooperate to resolve queries. As Figure 5.6 shows, in an X.500 directory, “chaining” of requests is provided by the Distributed Systems Protocol (DSP).



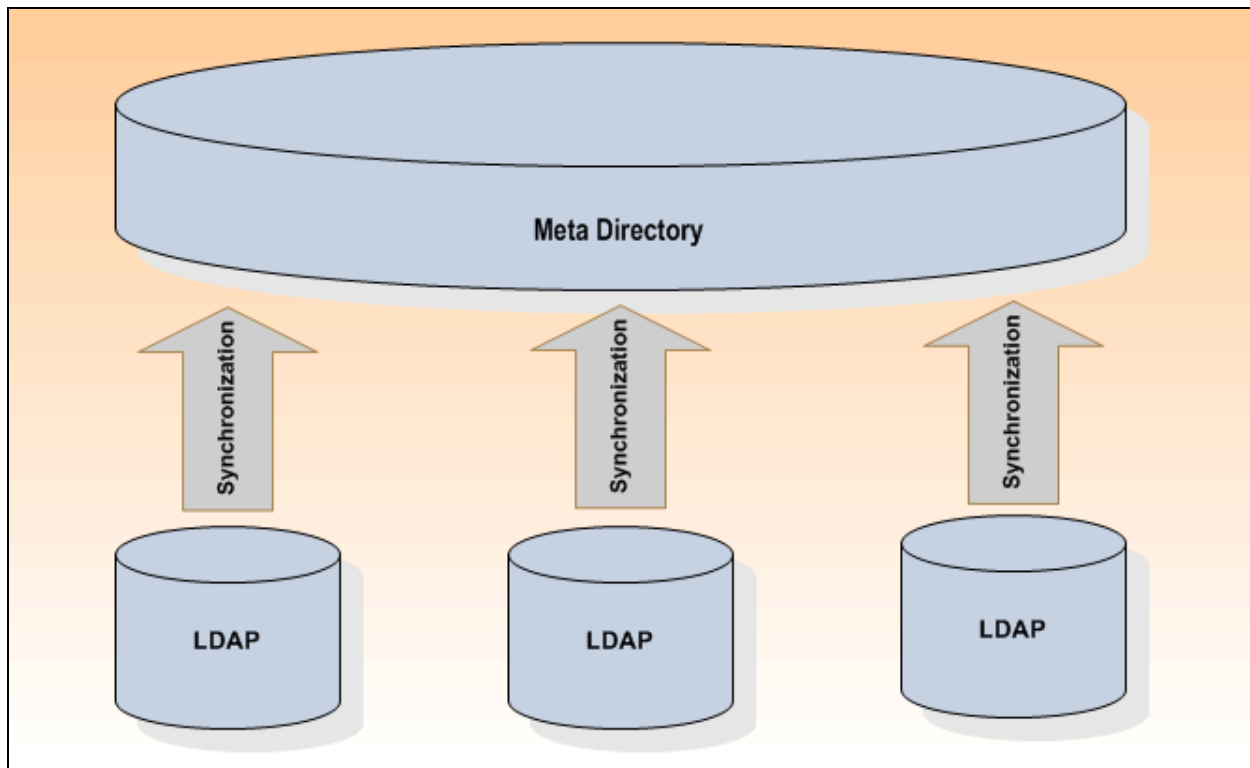
**Figure 5.6:** X.500 directories support distributed queries across multiple directories.

Many organizations that have deployed LDAP directories are finding the need to provide a consolidated view of multiple directories. Two approaches to this problem are meta directories and virtual directories.



### Meta Directories

Meta directories are databases of information replicated from other directories. Because information is copied from source directories, there is no need for additional protocols to support distributed query or update operations (see Figure 5.7). Thus, the implementation of a consolidated view of multiple directories is simplified, but there are drawbacks. For example, a meta directory is out of synch with its source directories when they are updated between synchronization operations.



**Figure 5.7:** Meta directories depend on synchronizing IAM information from multiple stores to a single repository.

### Virtual Directories

Virtual directories provide a single logical view of multiple directories (see Figure 5.8). Unlike, meta directories, information in virtual directories is not copied from source directories to a single repository. Virtual directories attempt to do what meta directories do “on-the-fly,” which has advantages in that data is not copied, but has limitations in terms of performance flexibility.

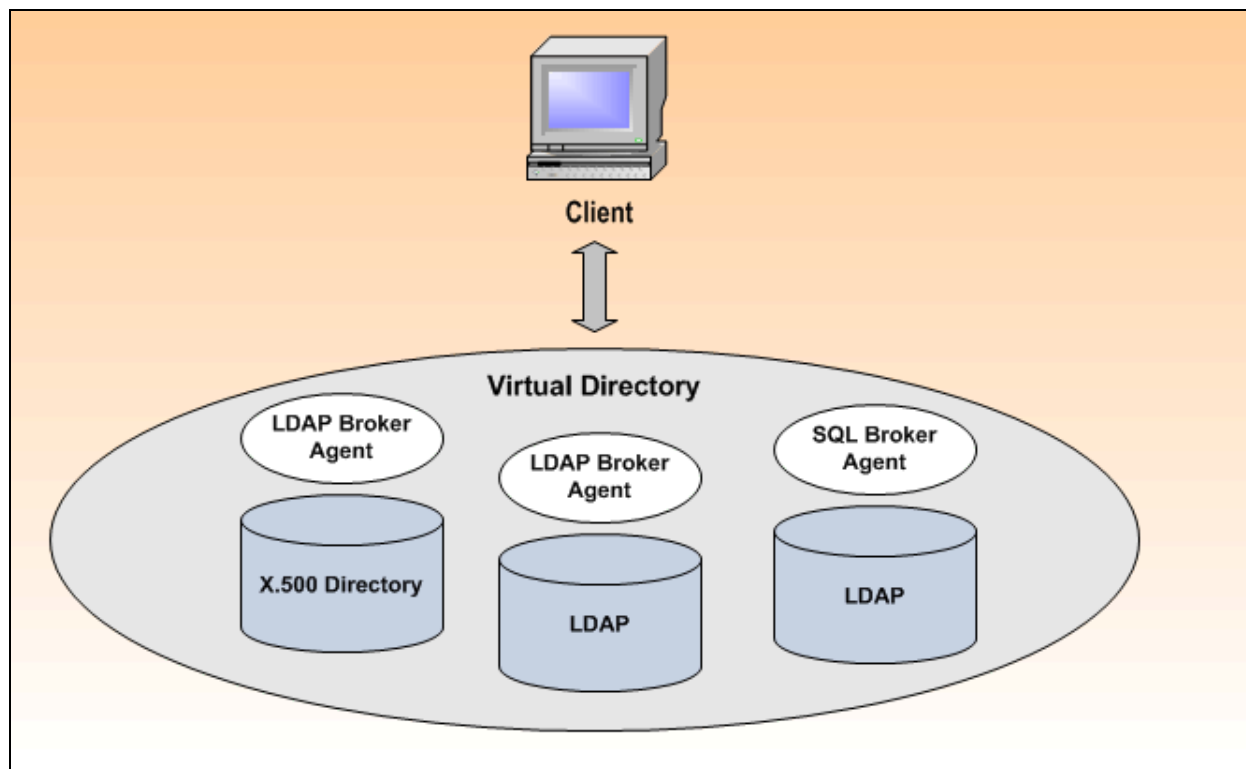


Figure 5.8: Virtual directories provide a logical view of multiple directories without replicating data.

### Provisioning

Provisioning is the process of coordinating the creation of user accounts, email authorizations in the form of rules and roles, and other tasks such as provisioning of physical resources associated with enabling new users. In addition to the protocols discussed in the sidebar, industry standards for identity management and provisioning systems should include a workflow component.

Workflow allows administrators to specify a sequence of events to add users based on the users' roles and the approval of others in the organization. The automated process ensures consistency and allows auditing of each step in the provisioning process.

It should also be noted that the provisioning process and other identity management operations should be the same system for all entity types. However, the way and extent that employees are provisioned will differ from customers and partners. Different system and different administration methods should not be required for different types of users.


Another element of provisioning is password management. Users in even small and midsized organizations need multiple passwords to use personal, departmental, and enterprise applications. In addition, passwords must be changed on a regular basis for security practices and regulatory compliance. Keeping track of passwords creates predictable problems, such as users who write down passwords, reuse the same password on several systems, and forget passwords, which results in calls to the Help desk (which increases costs). Password management and self-service applications are designed to solve these types of problems. Self-service applications allow users to self-register and reset passwords with assistance from Help desks or systems administrators, reducing Help desk calls anywhere from 25 to 60 percent.

Two general approaches have been used to minimize the burden on users to remember passwords: password synchronization and SSO. Password synchronization systems set all user passwords to the same word. Doing so saves the user from having to remember multiple passwords, but at a relatively high cost: If someone discovers the password to any one of those systems, that person has the password to all of them. Although password synchronization is an option for password management, this method is definitely not recommended.

SSO is more complex. The SSO server stores individual passwords for each system that a user accesses. A user authenticates once with the SSO server, for example, when logging on to a network or an enterprise portal. When an application challenges a user for credentials, the SSO server intercepts the request and responds on behalf of the user. SSO servers work directly with Web-based applications intercepting HTTP traffic and responding to password requests. Legacy applications, however, typically require specialized, sometimes custom, code to implement SSO.

## Auditing and Reporting


Effective security management and compliance procedures require auditing of significant events that occur in information systems. Identity management's central role in access control makes it necessary to have reliable, tamper-proof logging of all operations (such as authenticating with an application, querying database records, and modifying customer information). Most OSs offer logging functionality, however, these log files can easily be tampered with—secure logging is a requirement in order to provide creditable proof during security and regulatory audits. Audit reporting allows managers and administrators to monitor activities and to demonstrate compliance with relevant regulations. Effective audit reporting is also a key driver to reducing costs associated with proving compliance.

 Chapter 7 provides more information about the impact of auditing and reporting on the cost of compliance.

## Policy and Tools for Trust Management

Trust management entails the ability to verify the authenticity of identities from other identity management systems in a federated environment. The traditional organizational boundaries that have marked the reaches of enterprise applications no longer limit the reach of these systems. Commercial and government organizations need to share identity information in order to effectively and efficiently use multi-organizations systems.

For example, engineers at an aircraft manufacturer need access to product specifications from a parts supplier. With the thousands of parts required for components and sub-components, online access to product information is required to support collaborative development. Rather than duplicate identity information in each organization's directory, federated directories have trust relationships between identity management systems.

 The U.S. federal government has launched an initiative to develop a federated identity management system to support its e-government initiatives. Details are available at <http://www.cio.gov/eauthentication/>.

Federation and trust management are emerging technologies; however, major enterprise vendors are supporting federation standards, such as those of the Liberty Alliance.

 For more information about the Liberty Alliance, see <http://www.projectliberty.org/>.

The infrastructure of trust management depends on Public Key Infrastructure (PKI) technologies. PKI enables trust in distributed environments through the trusted third parties, certificate authorities (CAs), key management used for digital signatures, and message encryption.

 For more on PKI, see NIST's PKI Web site at <http://csrc.nist.gov/pki/>.

## Tightly Intergrated Processes

Provisioning, auditing, and access control are related in identity management. Provisioning tasks, such as creating accounts, should be logged in an audit trail. Audit trails should include access control details as well. Attempted violations of access control rules should be logged by enforcement systems. Even though enforcement systems will vary by platform, a logically centralized view of enforcement audits should be available to systems administrators.

### **Workflow**

Identity management operations that touch multiple systems should be executed through a workflow mechanism. Workflow allows organizations to maintain business controls by ensuring that proper approvals are always obtained. In addition, workflow provides accountability by auditing these approvals (providing information about when the approval happened and by whom). Workflows also help to enable modular designs of identity management systems.

### **Phased Deployments**

Although it is true that identity management operations can be tightly integrated, organizations usually do not deploy a full identity management system at one time. A better approach is to adopt a single module at a time and integrate the modules in a phased implementation. However, since IAM solutions are closely related and require multiple integration points, leading analysts have indicated that the majority of enterprise will be turning to integrated suites from a single vendor rather than struggling with “after the fact” integration, which has been a key cause of failure for many identity projects. Thus, once a loner-view IAM plan is in place, organizations should implement modules that will address the most pressing pain points in the organizations. For example,

- If Help desk support costs are increasing rapidly and users are becoming increasingly frustrated with the proliferation of passwords they must manage, then start with SSO or self-service password reset.
- If your organization has high turnover and has felt the effects of poor account management (for example, a former disgruntled employee has hacked into one of your servers), then a provisioning system would be a good start.
- If your users need to access a large number of systems and your administrative staff is spending too much time resetting passwords and monitoring access on multiple systems, then look to an enforcement module to start.

Modules that are deployed separately still need to integrate—an argument for standardization based on widely recognized protocols, such as SPML and SAML, and broader initiatives, such as the Liberty Alliance. This integration requires more than just workflow to move data; the modules must also maintain tamper-proof audit data to stay in compliance with many regulations.

### **End User and Administration Support**

Identity management systems ideally provide a single point of access for end users to manage their identity information and a management console for administrators. Users should have a single resource for common operations such as:

- Updating passwords
- Requesting access to applications and other resources
- Updating personal information in their identity management profiles
- Retrieving security policies

Administrator management consoles can encompass common operations, such as reviewing alerts from security systems and modifying policies.

## Integration with Other Security Systems

Security information management is the practice of collecting, collating, and analyzing information about your environment. Identity management systems must provide information about activities related to provisioning and policy enforcement, in aggregate form, so that it can be correlated with other events.

For example, a virus attack may be detected in a regional office and shortly after that an unusual number of passwords are reset. These are two distinct types of security information that alone warrant one type of response but together can indicate a more serious threat. By combining and correlating information, security professionals can more effectively respond to multi-faceted attacks.

Identity management systems play a central role in enterprise security management. They provide a consistent means of identifying and authenticating users across applications and services. They include workflow services that enable a consistent, less error prone mechanism for accomplishing and auditing multi-step tasks common in provisioning. The systems can be built on broadly adopted protocols that enable interoperability. The technology for deploying enterprise identity management exists today and is evolving to support trans-enterprise federated identity management.

## Summary

Identity management is not an optional process. Even if formal identity management is not in use, organizations must still manage identities. They must still

- Create accounts for new employees, contractors, customers, and partners.
- Define roles related to particular work tasks. There are often redundant and inconsistent definitions of roles, especially as the size of the organization grows.
- Associate work tasks with roles.
- Define access control rules in individual servers, file systems, and applications.
- Create and publish policies that are then enforced, perhaps to varying degrees, on individual systems.
- Review systems and application logs and alerts.
- Try to correlate events across multiple systems, with mixed success.
- Comply with regulations regarding privacy, confidentiality, and the integrity of public reporting

The net effect is that organizations pay for identity management whether they realize it or not. Although the previous list of tasks is costly, it does not address missed opportunities and the cost of errors. Managers may wonder

- Has the business lost customers because provisioning through the so called “customer self-service” site is too cumbersome and frustrating for users?
- Has data been altered because a terminated employee still had access to a database account?
- Do unauthorized users have read access to confidential customer information?
- How much lost time is due to delays in getting access to applications that employees have legitimate use for?

The identity management process is fundamental to security management and to the efficient management of applications across, and beyond, the enterprise. The combination of directories, workflow, auditing, reporting, and enforcement mechanisms can effectively address the problems cited. The challenges to implementing identity management are not trivial, but modular identity management systems can be deployed incrementally. The most pressing problems can be addressed first, knowing that other modules can be phased in later. Standards are also in place and continuing to develop to share information across identity management systems. The role of identity management, like many other aspects of security management, is not limited by organizational boundaries. The next chapter will delve even deeper into IAM, focusing on access enforcement and management and auditing.

**[Editor’s Note:** This content was excerpted from the free eBook *The Definitive Guide to Security Management* (Realtimepublishers.com) written by Dan Sullivan and available from a link at <http://www3.ca.com/ebook/>.]