

realtimepublishers.comtm

*The Administrator
Shortcut Guidetm To*



**User Management
and Provisioning**

abridean

Dave Kearns

Chapter 3: Applying the Technology: The Details	37
A Provisioning Approach to Identity Information Management	37
Policies Are Essential to Provisioning	39
Provisioning Software Needs to Be Robust	39
Communicating with Enterprise Data Stores	40
Provisioning Connects to Many Identity Information Stores	41
Choosing a Path	41
Best of Breed vs. Integrated Suite	42
Develop, Hire Consultants, or Buy Off-Shelf	43
Developing In-House	43
Hiring a Consulting Firm	44
Buying an Off-The-Shelf Solution	44
Leveraging Prebuilt Drivers and Connector Toolkits	45
Prebuilt Drivers	45
Connector Toolkits	46
Selecting the Type of Underlying Platform	46
Enterprise Directory Service	47
Metadirectory Service	49
Virtual Directory Service	50
Application-Specific Considerations	51
HR Applications	51
Messaging and Collaboration	52
Portals and Content Delivery Systems	52
Emerging Technologies and Standards	53
Considering Markup Languages: XML, SPML, and SAML	53
Assessing Web Services	55
Evaluating the Liberty Alliance	56
Regulatory Requirements	57
HIPAA	57
The Sarbanes-Oxley Act	58
The Graham Leach Bliley Act	59
Summary	60

Copyright Statement

© 2004 Realtimedpublishers.com, Inc. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtimedpublishers.com, Inc. (the "Materials") and this site and any such Materials are protected by international copyright and trademark laws.

THE MATERIALS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtimedpublishers.com, Inc or its web site sponsors. In no event shall Realtimedpublishers.com, Inc. or its web site sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

The Materials (including but not limited to the text, images, audio, and/or video) may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, in whole or in part, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.

Realtimedpublishers.com and the Realtimedpublishers logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

If you have any questions about these terms, or if you would like information about licensing materials from Realtimedpublishers.com, please contact us via e-mail at info@realtimedpublishers.com.

Chapter 3: Applying the Technology: The Details

When you stop to consider the scope of what provisioning applications are designed to do, you can fully appreciate why deploying one is neither simple nor easy. By implementing provisioning, you are trying to automate IT processes via corporate policy that will ensure that the people who are using your enterprise resources have all the necessary access to systems and information—and, yet, have only the type of access that they are supposed to have.

In addition, this capability must work both ways—automatically providing the user accounts and access rights where appropriate and automatically disabling the same user accounts and access rights once they are no longer needed. Yet, the provisioning process, while rooted in IT operations, extends into enterprise operations beyond managing users and the information they access.

A Provisioning Approach to Identity Information Management

Automating the creation of user accounts and assignment of the necessary access—and only the necessary access—is at the core of provisioning, yet provisioning is about much more than just user accounts and passwords. In many aspects, provisioning also functions to help manage the security of information within the enterprise while controlling access to enterprise information resources.

One of the most common uses of provisioning technology is in the so-called hire-fire scenario, in which the provisioning application is responsible for establishing user accounts and access rights within the enterprise network operating systems (OSs), messaging applications, essential databases, customer relationship management applications, and Line-Of-Business (LOB) applications. As Figure 3.1 illustrates, the hire-and-fire scenario use of a provisioning application supplies a company with a critical capability—the automated addition of a user to all enterprise applications and IT systems upon hiring, and the automatic disabling of that same user account (and all of the user’s access rights and permissions) at the point that the user is no longer with the company.

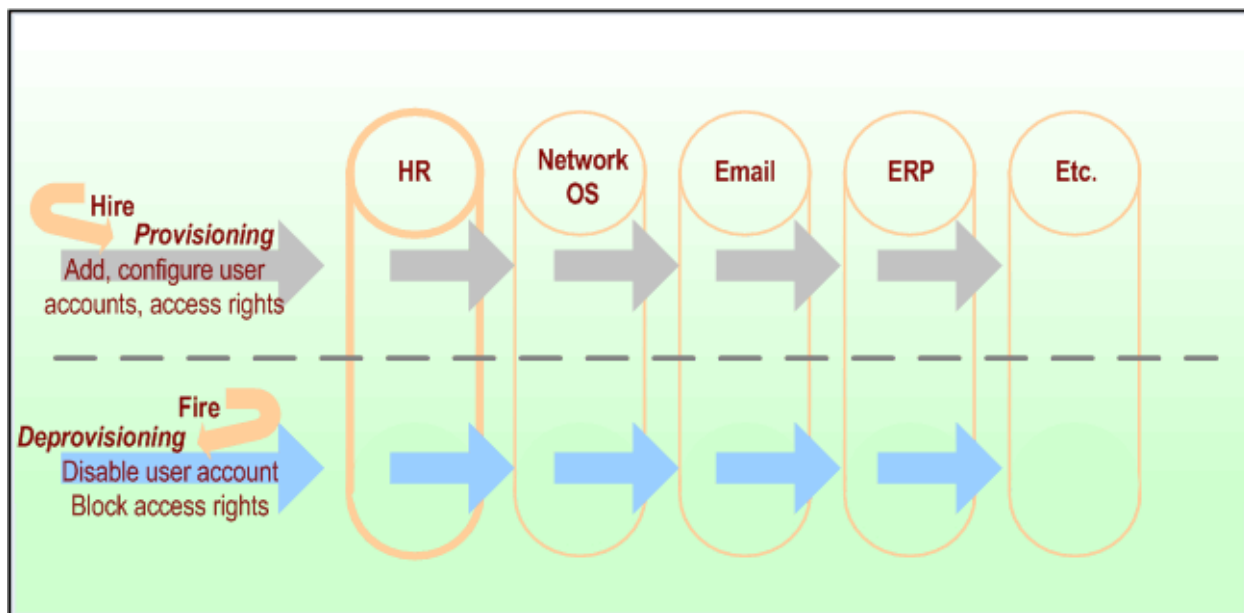


Figure 3.1: The process of provisioning and deprovisioning spans core identity information repositories.

Providing user accounts with the correct access rights and privileges is not only a security concern but also a serious cost factor—for many companies, this process can take days (or even weeks), can involve the work of multiple administrators, and slows the assimilation of a new employee into the company’s workflow. Additionally, there are logistical issues that can add to costs and impede employee assimilation—for example, scheduling meetings with the right managers or administrators (or catching them at their desks) to gain needed approval and provisioning actions.

To a considerable degree, the information and resources involved in the provisioning process and network or application security is the same—user accounts and the related permissions that grant access rights to enterprise information, services, applications, or other network resources are common ground for provisioning applications and security subsystems. Comprehensive provisioning applications might extend beyond the scope of IT security by initiating business processes that facilitate requisitioning of physical materials or facilities (such as an office, desk, chair, telephone, pager). However, much of the core function of automated provisioning is to provide the new employee with access to the enterprise networks and core business applications.

As stated earlier, implementing provisioning is neither an easy nor simple process; rather, it will take significant time, effort, and cost to implement. Despite these efforts and time and monetary costs, provisioning can provide substantial savings over time in the creation and management of user accounts and identity information throughout your enterprise.

Policies Are Essential to Provisioning

Policy-based provisioning allows you to establish sets of rules related to the business roles that new employees will be taking on. For example, although all employees need user accounts within enterprise networks as well as access to common applications, only employees who will be working from remote locations (branch offices, home, and so on) need accounts on remote access servers and the ability to access enterprise resources from locations outside your organization's firewalls.

Provisioning systems assess the business roles and related rules in order to establish profiles for employees. These systems also determine the nature and type of services and access to resources to be allocated and the equipment and facilities needed to support the work that the employee is expected to do. Establishing a set of policies for provisioning will provide a common foundation for administrators, management tools, network OSs, applications, and users, as well as facilitate the standardization of the configurations for user environments.

In fact, a substantial part of the time and effort of implementing automated provisioning will be taken up in establishing the business and security policies that govern user accounts and access rights. This process requires discussion, negotiation, and (with any luck) agreements among business managers throughout the various divisions controlling the identity information repositories and business applications in your enterprise.

Although this process won't be easy, it will be worth the difficulty. Once you've established the policies by which classes of users gain access to information and resources, you will no longer need to discuss it on a per-user basis—the policy will be established and it will be automatically implemented.

There might be exceptions to the policies, so be sure to establish a process for dealing with them. A manual review by administrators knowledgeable of the employee's role in the organization can help to track the handling of policy exceptions as well as errors in initial assignment. How a new employee is assigned organizational roles by policy might not always be exact, and placing them into roles that are the "closest match" might not entirely fit. As a result, it can be useful to have an administrator verify that the assigned rights and appropriate assets—and *only* those rights and assets—have been granted.

Provisioning Software Needs to Be Robust

A provisioning/deprovisioning solution at its core automates the identity information management for the people involved in your business across multiple applications, platforms, and operations. At minimum, it must provide unified control over the user identity information; thus, of necessity, it must have access to most, if not all, the identity information repositories in the enterprise.

Provisioning systems need to be self-correcting to some degree—they should be able to identify problems, redundancies, and inconsistencies in the provisioning process, and have some configurable mechanism for automatically correcting these errors when possible. When an activity requires a person to take action, the notification process should be automated. If an application or database server is down during a provisioning operation, for example, the user account information will not be able to be added. The provisioning software should generate a notification of this failure, and provide some direction for how to resolve it.

You can more easily manage the security and operational concerns if you establish policies that require that all additions are routed through your provisioning application (perhaps as triggered by entries in the Human Resources—HR—database), thus establishing consistent policy-based control over accounts and access.

Yet, to some degree, provisioning systems need to be aware of and responsive to the information that is put into the applications and services that they will be manipulating. If a new email account is directly added to the email server, for example, the provisioning system should be able to cross-reference this email account with user accounts in the network OS and an employee entry in the HR database, and provide some kind of integration between these systems. Although this form of “reverse synchronization” is very useful, it can be difficult to implement across all possible applications in use in your enterprise.

Communicating with Enterprise Data Stores

Provisioning applications need to be able to communicate with many types of data sources, especially directories, databases, and other identity information repositories. To do so, they must support common industry protocols and methods for accessing these data stores:

- Lightweight Directory Access Protocol (LDAP)—Because LDAP is the de facto standard for most directory service (and many email) products, selecting provisioning software that can communicate via LDAP with all directories within your network environment seems necessary.
- Structured query language (SQL)—Similarly, the ability for the provisioning application to use SQL to communicate with the wide range of databases (such as Oracle, MySQL, Microsoft SQL Server, and others) is also a central requirement (many HR, Customer Relationship Management—CRM, and Enterprise Resource Planning—ERP—applications use SQL). A provisioning application should support either the Open Database Connectivity (ODBC) interface or the Java Database Connectivity interface to allow programmatic access to SQL-based databases.
- Extensible markup language (XML)—Support for the import and export of identity information via XML is important (perhaps even critical) to the integration with your current and future enterprise applications.

Provisioning Connects to Many Identity Information Stores

In addition to integrating with an underlying directory service (enterprise, meta, or virtual), provisioning applications must be able to connect to all of the repositories of identity information within your enterprise. To do so, specialized namespace connectors (aka drivers, adapters) must either exist as part of the provisioning application or the application must provide a means for the connectors to be easily developed to meet your specific requirements.

Provisioning applications typically provide connectors for common forms of information exchange between services or applications, such as connectors for SQL to exchange information with databases (and the HR, CRM, ERP applications that use them), LDAP to exchange information with directories (such as network OSs and email applications), and XML to exchange information with most of the newer enterprise applications. In addition to these standardized connectors, it is common to need to communicate with specialized or proprietary applications in enterprise identity management and integration projects; thus, most provisioning systems will support some way to customize connectors. If your organization has legacy applications with data stores that are inaccessible via standard connectors, you can use third-party products such as Novell's DirXML, which supports creation of custom connectors to exchange information with such proprietary data sources.


Choosing a Path

What is the right provisioning solution? The one that works best for your business, of course. One of the aspects of all systems is described as *equifinality*, which asserts that within any system, there are many paths that can lead to the same outcome. Such is also true with provisioning options—you can approach it several ways.

The desired outcome is automated provisioning and deprovisioning of user accounts, information, and resources in a way that is seamlessly integrated with your existing IT infrastructure and business operations. There is more than one right way to do so; however, within the context of your current business and technology environments, certain approaches will be more suitable than others.

Selecting your path to an identity information management solution that uses automated provisioning requires the assessment of the underlying platform that will host the user management data store as well as the specifics of the provisioning application itself. The underlying directory technology and specific provisioning application that you select must be rooted in what exactly you need it to do and in the context of the environment in which you are going to be doing it. Not all approaches to a provisioning solution—even some that technically work—will necessarily yield the results that you are looking for.

In a number of ways, provisioning involves federated identity management—that is, the cross-correlating of a user's identity as it is stored in multiple different applications, services, or even different Internet portals or Web sites; and then, by automated means, adding or removing user accounts and permissions to facilitate or block access to the services and resources provided by each of these. The path that you choose through this technological, political, and religious minefield of information management will, of course, need to be based upon the business and IT requirements of your specific enterprise.

 For more information about the technological, political, and religious challenges to user management and provisioning, refer back to Chapters 1 and 2.

Best of Breed vs. Integrated Suite


Provisioning is a technology that, by definition, spans a wide range of enterprise applications, services, and the network software infrastructure. When evaluating a new technology with enterprise-wide application implications, the choice of whether to select an integrated suite of applications or to find the best of each type of application and implement them separately is always subject to debate. Although there are arguments in favor of each approach, what you choose, of course, depends upon your environment and your requirements.

Best of Breed

In brief, choosing the best of breed involves selecting individual products from different vendors based on the products' capabilities, while ensuring interoperability with your current enterprise applications and IT environment. The best of breed approach lets you leverage your existing IT software infrastructure—you can retain your messaging and collaboration applications, network OSs, and all of your business applications.

Approaching your provisioning solution by buying the best of breed software applications enables you to facilitate the automation of provisioning the IT user accounts and related access permissions while leveraging the identity information data stores contained in your existing business and network applications. The best of breed strategy can provide the ability to keep your existing identity information in place without first having to migrate or export the identity information sources.

In employing this strategy, however, you will want to carefully research operational and implementation issues, with particular attention to interoperability with your other applications. A best of breed approach is also likely to take more time to maintain and more effort to troubleshoot problems, as you will have to check with multiple vendors.

 Applications designated “best of breed” might not always be “best” across the board. Organizational requirements differ, and features in standalone applications might not be better for your environment than those found in an integrated suite. Matching the features of the provisioning applications or modules to your organization's list of functional requirements will highlight which components of a provisioning solution are best for you.

Integrated Suite

An integrated suite of applications to support provisioning addresses the interoperability questions involved in making the provisioning solutions work correctly. Finding an integrated suite that precisely fulfills all your business's IT requirements and operational considerations is unlikely—it is generally far easier to find individual applications that more closely meet your needs. Finding a suite of provisioning-related applications, however, is becoming easier, as big vendors such as Microsoft and Sun Microsystems are now supplying integrated solutions.

Buying a suite of integrated applications for provisioning can provide a more seamless connection between identity data sources as well as allow you to consult a single vendor in order to resolve issues or obtain technical support when needed. Most businesses, however, do not use a single platform for network servers and business applications.

If you want to buy an integrated suite of applications that encompasses the entire scope of the identity information repositories that you use in your enterprise, keep in mind that it entails migrating all of this information from your legacy applications to the new integrated suite of applications supporting the provisioning software. Because of the cost, logistics, and disruption that such a large-scale migration would have for existing business operations, the choice of an integrated suite would seem less practical for most businesses, unless they already have most of that integrated suite deployed, or they are establishing a new business in which no information repositories currently exist.

Develop, Hire Consultants, or Buy Off-Shelf

Whether you decide to develop your provisioning solutions in-house, buy a commercial provisioning application off the shelf, or bring in consultants to develop a provisioning solution for you, you will want to review your provisioning requirements and goals in light of the experience of companies that have already implemented provisioning solutions. Although automated provisioning is still a relatively new technology, many companies of all sizes have already explored this territory; it makes sense to take advantage of what these companies learned in the process.

Developing In-House

There are positives and negatives to developing your provisioning solution in-house. Perhaps the most significant upside is that, by developing it yourself, you can make sure it will meet your business needs and your IT operational requirements precisely. Additionally, your provisioning solution can be dynamically modified as needed to meet changing business requirements and conditions within your IT environment.

One of the downsides to developing your provisioning solution in-house is the upfront costs of the developers, and the allocation of these developers and their expertise away from other projects within the organization. It will also take substantial time to develop the necessary coding and test it in your environment before your custom solution is successful and seamless. Of course, any solution needs to be well tested before deployment regardless of whether you develop your provisioning solution in-house or buy it off the shelf.

Designing, creating, and maintaining custom provisioning software to match your business and operational requirements also necessitates substantial development expertise. You might not have this development talent available within your organization, thus it could require hiring of additional talent to effectively produce a solution in-house.



In addition to the development team required to build the solution, you'll need to include teams to handle documentation, support, and upgrading of your custom provisioning application. As a result of employee turnover and reassignment, documentation of such custom applications is essential to an enterprise in order to be able to continue to maintain it. Be sure you assess the costs of documentation, support, and upgrading efforts alongside the development costs.

Hiring a Consulting Firm

Another approach to achieving the needed functionality of an automated provisioning solution is to hire consultants with experience in developing provisioning solutions in the enterprise environment. Like the approach of developing the provisioning solution in-house, hiring consultants to develop the provisioning application can allow you to make sure that it exactly meets your business and IT requirements. By hiring consultants, you can have the custom provisioning solution developed without having to reassign your own development team away from existing projects or hiring developers if you don't already have this kind of talent in-house.

You should, however, be clear that this method is not an inexpensive approach. When hiring a consulting firm capable of developing custom provisioning software suitable for an enterprise environment, you must assume that the upfront costs will be considerable. In addition to the cost, having a provisioning solution custom developed by a consulting firm is still going to take significant time to build, test, and deploy.

When shopping for a consulting firm to implement a provisioning or other identity management project for your business, look for a consulting team that has extensive experience in identity management, directory services, and development and implementation of directory-enabled applications. Make sure that the firm you hire has extensive experience in the development of namespace connectors for both standard interfaces and custom applications. Verify the consulting team's track record in directory and identity management projects with substantial scalability to ensure that they are clearly capable of handling enterprise-level identity management projects.

Buying an Off-The-Shelf Solution

Another approach is to buy an existing commercial provisioning solution. In most cases, the provisioning solution is tried and tested and has been implemented by other companies before you; thus, unlike an internally developed solution, off-the-shelf products have most of the bugs worked out. Such being the case will allow you to quickly deploy a provisioning solution as opposed to taking the substantial time required to develop the software on your own prior to being able to deploy it.

Because organizations have a largely common set of operations to which they want to apply a provisioning solution (add user accounts, disable user accounts, and so on), an off-the-shelf commercial provisioning application should be able to meet most of your baseline functional requirements. In theory, implementing an off-the-shelf provisioning application (or suite of applications) should allow you to minimize the expense and time to implement the solution and provide for faster return on investment (ROI).

The downside to buying an off-the-shelf provisioning solution is that it might not address all of your provisioning needs. You might have identity information repositories with which it simply cannot exchange information, you might have technical requirements that it cannot address, and it might have an approach to implementation that conflicts with your business operations. Although most commercial provisioning applications allow you to customize drivers or connectors to communicate with information stores that the application does not natively talk to, developing these custom connectors requires additional expertise, time, and expense.

One example of an off-the-shelf provisioning solution is *abrideanProvisor*, a provisioning application that can integrate your existing identity information repositories, enabling automated user management without substantial changes to your current business applications and IT infrastructure. *abrideanProvisor*'s support for a range of underlying directory architectures and products allows you to leverage your existing databases and directories without having to add another directory layer (such as a metadirectory or enterprise directory) to your IT environment. Using a virtual directory—with products such as *RadiantLogic RadiantOne* virtual directory—avoids the additional network traffic generated by replication and synchronization of information between your distributed identity information data stores. In this environment, *Provisor* maintains pointers to all of your core identity information sources and directly manipulates information in its original repositories.

Another off-the-shelf solution is *Netegrity IdentityMinder eProvision 4.0*, which enables you to establish policies that control user access to enterprise services, applications, and resources. (*Netegrity* acquired its provisioning technology when the company purchased *Business Layers* and its *DayOne* provisioning solution). In addition to creating user accounts and assigning access permissions, this product includes a workflow engine interface that allows drag-and-drop modeling of workflow processes (as opposed to having to develop scripts to accomplish this effect).



In addition to these three basic approaches (in-house, consultants, or commercial application), a hybrid approach can also be used. Through this method, you purchase an off-the-shelf solution and either hire consultants or have in-house developers customize it to fit your requirements.

Leveraging Prebuilt Drivers and Connector Toolkits

Commercial provisioning solutions contain a default set of *drivers*—also referred to as *adapters* or *connectors*—that enable it to exchange information with common identity information repositories (directories, databases, and so on). Some of these provisioning applications also provide a toolkit to let you create custom drivers as needed.

Prebuilt Drivers

Using prebuilt drivers will, probably most significantly, expedite implementation of a provisioning solution. Optimally, the provisioning solution you select will have prebuilt drivers to exchange data with all of the critical identity information repositories used in your enterprise. Common prebuilt drivers include:

- Network OSs
- Directory services
- Email and collaboration services
- Databases

Having prebuilt drivers available makes it much easier, not to mention faster, to implement your provisioning solution and to begin to reap some of the benefits of automating account management processes. Prior to investing in a provisioning solution, carefully consider the impact of a product that does not have a prebuilt driver for a mission-critical or high-visibility application.

Connector Toolkits

Although communicating with common applications and standard interfaces (such as SQL and LDAP) is essential in a provisioning solution, businesses commonly also have identity information stored in less standard data structures and/or proprietary applications. As a result, the availability of software toolkits that allow you to build connectors to effectively access and manipulate the identity information belonging to disparate and perhaps uncommon (or even one of a kind) applications can be a critical aspect of whether a given provisioning solution will work in your environment.

Connector toolkits provide flexibility yet require in-house or consulting expertise to develop and test. Accordingly, in addition to the availability of connector toolkits, you will need to evaluate whether you have the development expertise to customize connectors in-house. If not, make sure to include in your evaluation a *realistic* assessment of the cost and time of hiring the expertise to build the necessary connectors.

In many ways, if you can buy a provisioning application that has pre-existing drivers to connect to the various applications, directories, databases, and other identity information stores currently in use on your network, it will be faster and more cost-effective to implement than if you have to build custom drivers. However, there is also an advantage to provisioning applications that provide extensive toolkits that enable you to customize the connectors to these various data sources: they provide you with greater flexibility and a wider scope of applications with which you can interface.

Selecting the Type of Underlying Platform

As we discussed in Chapter 2, the most common approaches to the storage and management of identity information employ some kind of an underlying directory service that provides authentication and controls access to information stored within the enterprise network. Why use a directory in provisioning? A directory service provides scalability, reliability, and enables policy-based management of user accounts and the requisite authentication and authorization services.

Provisioning is fundamentally a directory-enabled application that relies upon change events in either the underlying directory or connected applications (such as the HR application) to initiate the provisioning process that will update all related and contingent identity information repositories. Accordingly, the scalability of a provisioning application will be substantially impacted by the selection of its underlying directory and information integration architecture. As a result of the provisioning application using a directory service product, you can leverage common characteristics of the directory to support scalable and robust provisioning operations.

Directory services are designed with a distributed architecture using multiple directory system agent (DSA) servers to ensure robust and reliable operations throughout a distributed enterprise. Directory services are designed with fault tolerance in mind by implementing multiple directory servers that can handle authentication and authorization should one or more directory servers fail.

The underlying directory service technology also facilitates the use of policy-based controls for the provisioning process. A directory service is designed to enable policy-based networking, managing user accounts and identity information, and handling authentication and access control to all network accessible resources (perhaps more realistically, to as many resources as possible, and at the very least, the most important). Thus, a directory serves as a logical platform for provisioning technologies that automate the implementation of user accounts, identity information, and access permissions across diverse applications and networks.

There are three approaches taken in the architecture of the underlying directory service to manage this information—you can use an enterprise directory, a metadirectory service, or a virtual directory service to handle the user identity information. There is no “one size fits all” solution for managing this information in various business and network environments. Each company must evaluate its own business goals, operational requirements, IT infrastructure, and the demands that will be placed upon the provisioning process in order to determine the best underlying platform for their provisioning application.



All provisioning applications do not allow selection of the directory service it will use. If the directory platform matters to you (and it probably does if you have an enterprise directory deployed), you will want to check provisioning product offerings carefully to verify that they will work with the directories that are critical to your environment.

Enterprise Directory Service

Employing an enterprise directory service as the platform for provisioning is theoretically a more effective overall solution in that it unifies and integrates identity information from all the different identity information repositories throughout the enterprise, simplifying the provisioning process (see Figure 3.2). In this scenario, all the identity information and related data is stored, managed, and updated in a single enterprise directory data store, providing a single authoritative source for all identity information in the enterprise.

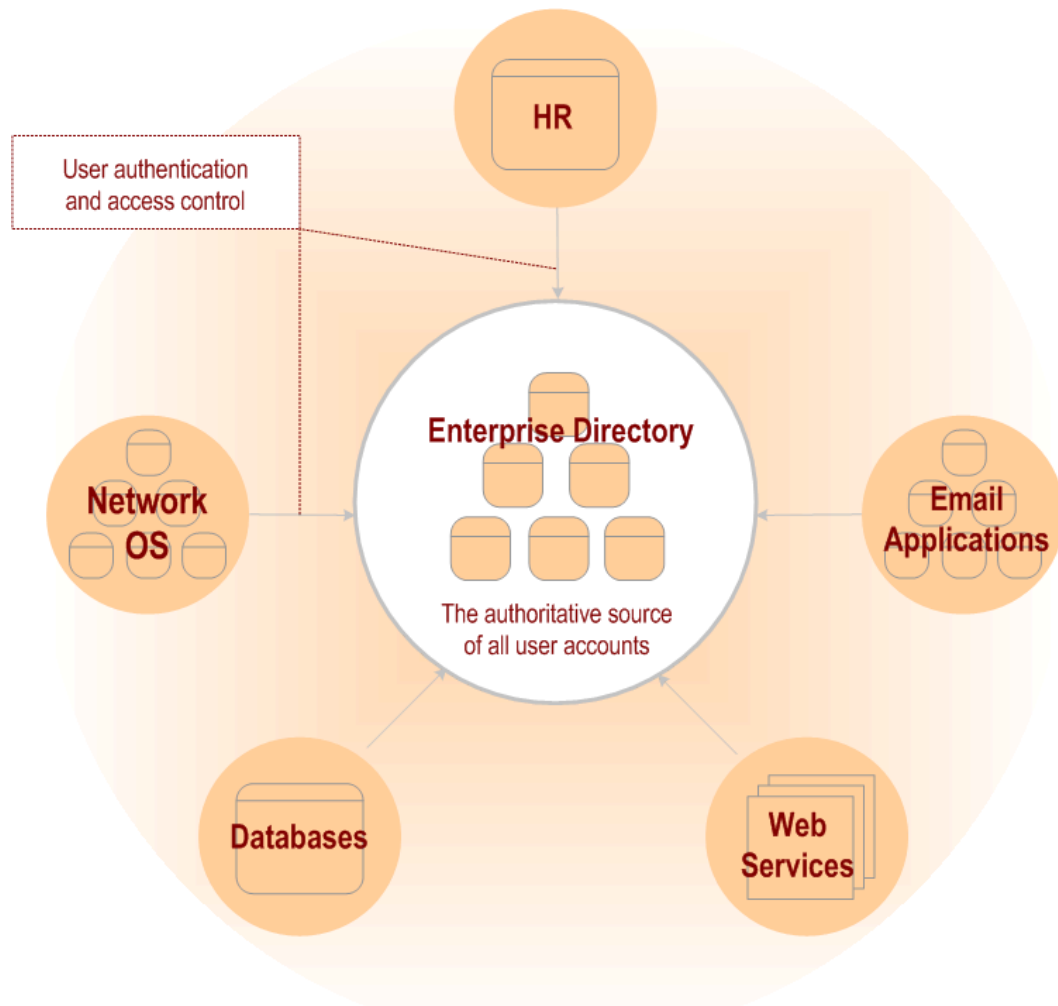


Figure 3.2: An enterprise directory service serves as the core authoritative source of user account information.

Yet, an enterprise directory service is also much less practical to employ in that it requires adherence to a single directory service throughout all divisions of the enterprise. In many cases, managers are responsible for controlling the identity information within their division and are using LOB applications and other identity information repositories that might not lend themselves to enterprise-wide integration. As discussed earlier, the religious and political issues involved in attempting to implement an enterprise directory service can present prohibitive roadblocks to using one as the underlying platform for a provisioning solution.

Metadirectory Service

A metadirectory service provides a more practical option as the underlying platform for a provisioning solution in that it retains the existing identity information data stores. Data from the existing identity information repositories are copied into the metadirectory data store while leaving those repositories intact.

In this scenario, the metadirectory contains all the identity information, yet the metadirectory can bidirectionally synchronize with all the other identity information repositories throughout the enterprise whenever any of that information changes (see Figure 3.3). There are, however, latency issues created by this approach in terms of the amount of time that passes between changes to the information in one repository and those changes being reflected in the metadirectory (and vice versa).

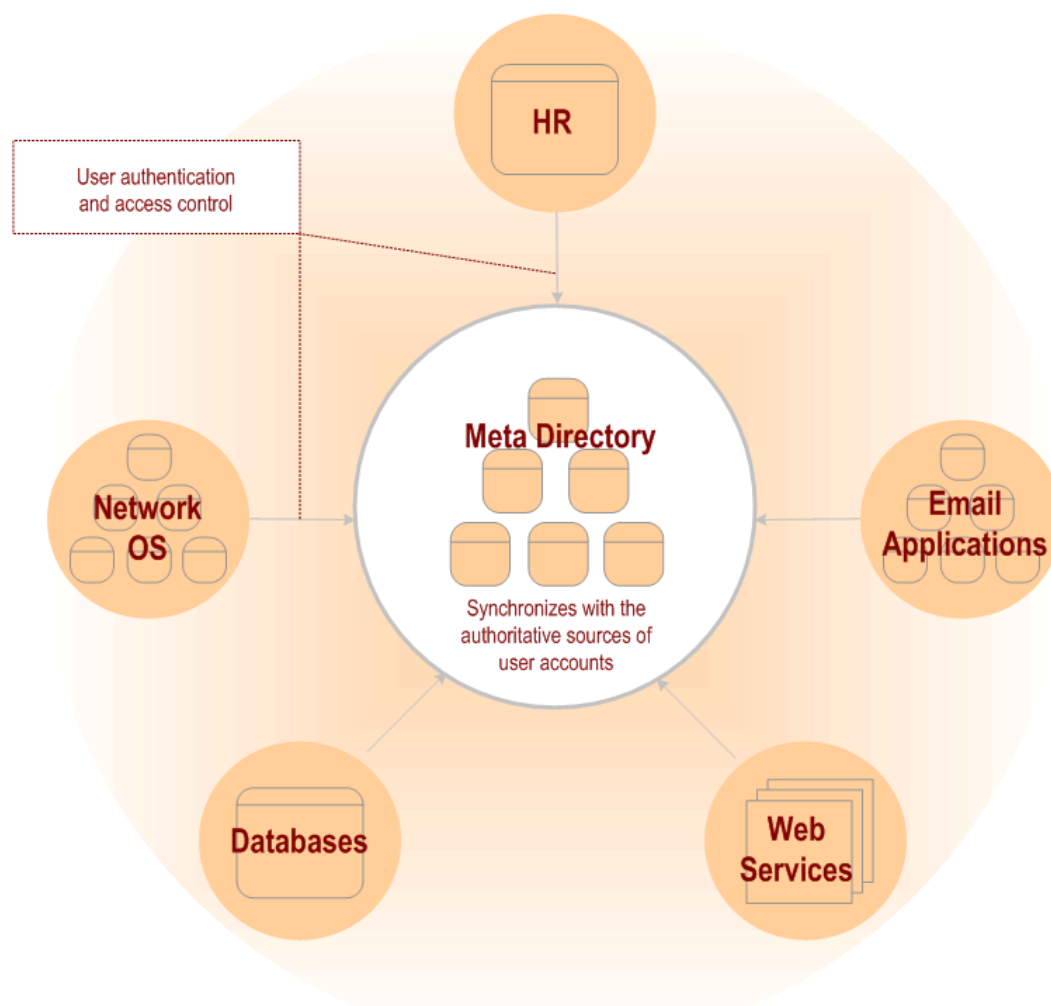


Figure 3.3: A metadirectory synchronizes with other sources of user account information.

In some ways, you still have some of the religious and political issues that affect the enterprise directory scenario in that there still are subdivisions of control over identity information and responsibility for that information. In most cases, the business and network management teams must define which of the information repositories are going to be the authoritative data source for which pieces of information and determine who will have access to the information as well as control over adding or updating the information. Yet, the addition of a metadirectory used only to implement a provisioning solution adds another layer of directory management to your overall IT environment, and can significantly increase the amount of network traffic to support metadirectory operations and synchronization processes.

Virtual Directory Service

For many organizations, an underlying virtual directory service provides the most efficient approach to implementation of a provisioning solution in that it doesn't attempt to duplicate the information already stored within the existing identity information repositories. Instead, a virtual directory service only maintains a set of pointers to where the information already exists and provides a common access point for a provisioning solution to use to access or update the information stored in any of the identity information repositories currently in use (see Figure 3.4).

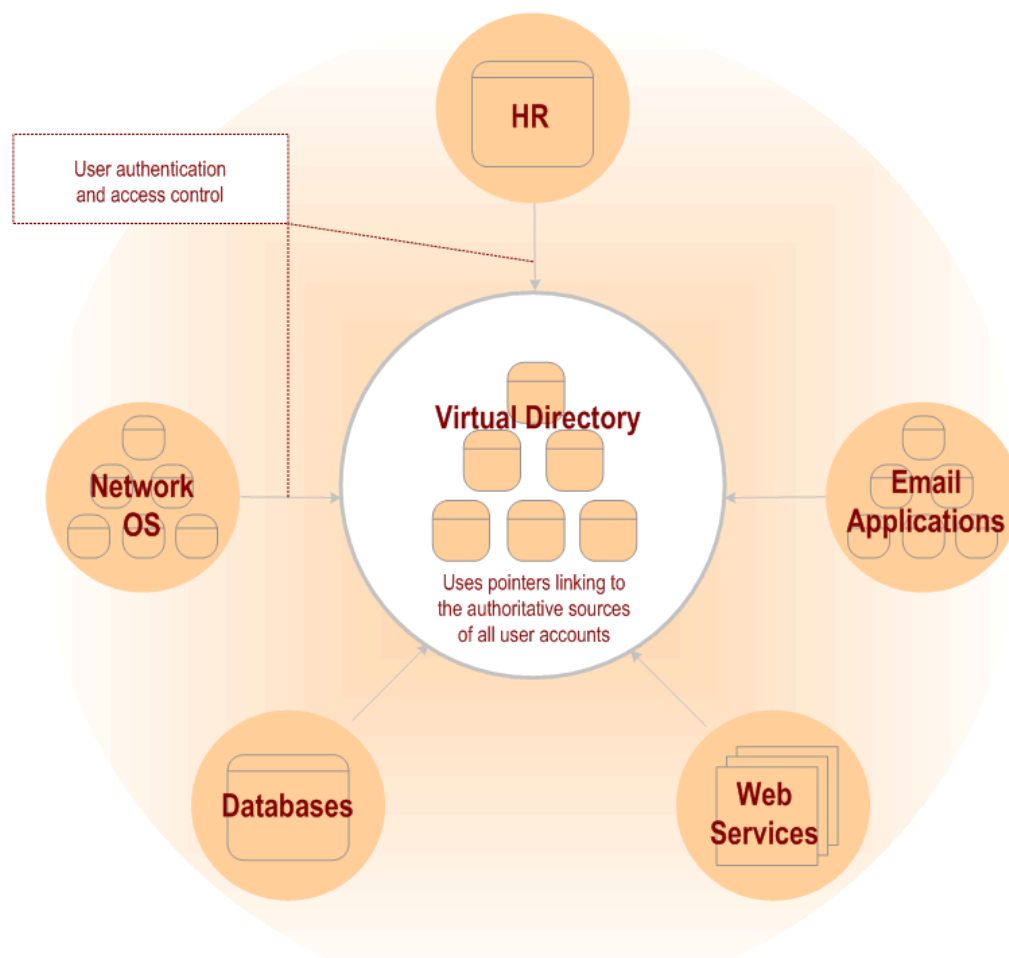


Figure 3.4: A virtual directory service relies upon other repositories as the authoritative source of the user account information.

A virtual directory service also minimizes the amount of synchronization and related network traffic, as it only has to update its pointers when the actual location of its information changes—as opposed to having to synchronize each time the information itself changes (as would be the case in using a metadirectory platform for provisioning).

Application-Specific Considerations

Automating provisioning and deprovisioning of user accounts and related identity information will present both challenges and opportunities through the process of integrating and cross-mapping user identity information between disparate systems. To begin with, user identity information will not necessarily be referenced in the same way in different systems (for instance, the names of users might be constructed using differing formats), presenting technical challenges in exchanging and updating information. Additionally, the ownership and responsibility for each of these different identity repositories is likely to be under the control of different divisions and management within the enterprise, creating both political and religious questions of control and desired approach to implementing the provisioning solution.

Although each application presents a distinct set of issues and concerns, there are a few categories that are both common and critical to most businesses—specifically, HR, messaging and collaboration, and portals and content delivery systems.

HR Applications

At minimum, enterprise provisioning solutions will need to be able to leverage the information in your HR application and to use changes in that information to generate enterprise-wide automatic updates of user account information and status. HR applications are the logical trigger points for provisioning in multiple scenarios—hiring and firing, change of position, change of location, and so on. Many provisioning solutions are designed to work exactly that way—using the addition of an employee as the trigger to cause that user's information to be populated to the network OS and email and core business applications as well as to assign access rights and privileges to enterprise resources.

One consideration when looking for a provisioning solution is whether it provides the right level of access to the HR data and provides the needed level of controls over the limits to the access to that information. HR data is commonly considered the authoritative data source of user (that is, employee) information from an enterprise perspective, so the provisioning software should be able to leverage this HR data without modifying it. Stringent auditing controls for access to and dissemination of this information should be another core feature of the provisioning application.

Provisioning user accounts throughout your enterprise applications based on changes to the HR database also provides an opportunity to improve overall security in the enterprise IT infrastructure by automatically setting user access and permissions based on their job functions, expected roles, and location. Similarly, the ability to deprovision user accounts based upon a status change in the HR database (such as firing or being laid off) will also improve security by automatically disabling user accounts and prohibiting access to sensitive enterprise information and resources.

Messaging and Collaboration

Messaging and collaboration services such as Microsoft Exchange Server and SharePoint Portal Server are applications that present an obvious scenario for user provisioning. Everyone, virtually irrespective of their job description, needs an email account, and setting up email accounts requires far more information than just a username and password:

- Distribution group membership
- Physical location at which the new employee will be working
- Addressing information, phone numbers, and other key location or job function data

As an example of how provisioning applications can help in the management and security of messaging systems, consider Microsoft Exchange Server 2000/2003 and its integration with Active Directory (AD). This integration supplies enhanced administrative rights to Exchange administrators, and thus puts overall network security and delegation of Exchange-related tasks somewhat at odds. Provisioning applications can mitigate the security vulnerabilities by automatically limiting Exchange administrators to only the rights that are necessary to carry out the management of Exchange. Furthermore, provisioning can assist with controlling major projects such as Exchange migration, ensuring the security of the process, and providing an audit trail.

Portals and Content Delivery Systems

Content delivery systems of all sorts are facing a balancing act between facilitating personalization of the content to which a user wants access and the ability to maintain the privacy and security of the user's identity information. To facilitate personalization, companies must obtain and collate information about a person's preferences and patterns of information access and usage. Yet, to do so, and to bring this information to bear in the context of the user's Web site experience, companies must monitor users' activities and associate the results of the monitoring with the users' profiles.

Additionally, the different services available via content delivery systems, even at the same site, frequently require multiple logons and multiple user profiles that are storing much of the same identity information. Especially in the context of the Internet—where the user may go from site to site seeking information and services at various portals and content delivery systems—having to identify and authenticate themselves to each site can render the user experience frustrating at best.

Given these constraints, implementing some sort of single sign-on (SSO) or federated identity management system can not only provide a more seamless user experience but also give the companies developing these Web services, portals, and content delivery systems more reliable information about their visitors. Yet in this context of cross-enterprise federation of users (and provisioning of access), the strength of the security measures within the identity management system is even more significant.

Emerging Technologies and Standards

When considering any provisioning and user management solution, you must be aware of how changes to the industry standards and enhancements in technologies can affect the future of your IT and business operations. Problems that exist in current technological initiatives or platforms, or which deter ongoing business workflow operations, might be issues that can be alleviated by application of technologies that have been recently introduced (or are still emerging). As a result, paying attention to developments in the industry could potentially help you solve intransigent problems, and save you time, money, or frustration.

Industry-leading vendors of directory and provisioning software are integrating their identity management solutions into applications and product suites that leverage key emerging technology standards such as XML and Web Services. For example, Microsoft is integrating namespace federation services into AD as part of the Windows Server 2003 update currently scheduled for 2005. This new Active Directory Federation Service (ADFS) supports mapping user accounts between not only different identity information data stores within an enterprise but also between different companies. This service will provide an underlying mechanism to enable cross-company authentication and authorization of user accounts. This capability will facilitate integration of corporate partnering efforts, providing partners with needed access to enterprise resources as well as support portal-to-portal user recognition and access control. This new federation service for identity information will be used by Microsoft to enable SSO functionality via Web Services and related protocols.

Considering Markup Languages: XML, SPML, and SAML

XML is becoming the de facto industry standard for information exchange between applications, services, and information repositories of all sorts. XML provides a structured format used for exporting or importing any set of data, which allows XML-compliant software to integrate data from any source. Industry vendors of a wide range of applications, services, directories, databases, and virtually every other kind of software have adopted XML as the global method of exchanging information.

With XML, businesses increasingly can be assured that their provisioning applications will be able to exchange and update identity information contained in most enterprise applications. Interoperability between the provisioning software and your legacy directories and databases is enhanced with XML, enabling the integration of all the identity and information that needs to be accessible to support a fully automated user management and provisioning solution.

Support for XML in the provisioning solution should be considered a central element—as an emerging standard with widespread industry support, interoperability between the provisioning solution and future enterprise applications may well be contingent upon XML functionality. In addition, multiple XML-based specifications supporting security and provisioning are gaining acceptance in the industry, and vendors are beginning to integrate these specifications into their new product offerings.

SPML

The Service Provisioning Markup Language (SPML), for example, is rooted in XML and is designed to provide a framework for dealing with system resource allocation—defining the provisioning of user accounts and permissions for networks, services, applications, and systems within an enterprise as well as between organizations. The SPML standard is approved by the Organization for the Advancement of Structured Information Standards (OASIS).

SPML, as an XML-based specification, provides the functionality and support for provisioning operations across different platforms. This capability will allow administrators to automate user account provisioning for both internal and external enterprise networks, applications, services, and resources. The use of SPML could allow the replacement of vendor-specific and proprietary namespace connectors/adapters with open-standardized XML schema for the exchange of provisioning-related information, enhancing the overall interoperability and freeing provisioning applications from vendor-specific constraints.

In addition to easing provisioning deployments, SPML-compliant services will facilitate authenticated access to diverse network resources, reduce administrative overhead in providing access to these enterprise resources, support two-factor authentication, and create a comprehensive audit trail. The design of SPML allows it to interoperate with the latest versions of Security Assertion Markup Language (SAML) and the WS-Security standards supported by OASIS as well as the Simple Object Access Protocol (SOAP) standards supported by W3C (in version 1.2 of SOAP).

SPML has been gathering substantial vendor support—from such companies as Sun Microsystems, Novell, PeopleSoft, BEA Systems, and many others—who see it as a means of making it faster and cheaper to deploy Web Services-based provisioning solutions and simplify management of these applications.

SAML

Another OASIS standard, SAML manages the exchange of authentication and access control data between different organizations and works with SPML. SAML provides an open methodology for handling user identity authentication that is independent of vendor-specific authentication schemes. SAML is gaining widespread industry support as a vendor-neutral cross-platform authentication interface and is supported by vendors such as Sun Microsystems, IBM, Microsoft, Novell, and RSA Security. SPML and SAML work together to enable organizations to automatically create and authenticate user accounts, providing a foundation for Web Services-based provisioning and SSO applications.

Assessing Web Services

Web Services are slowly coming to the forefront as a communication and commerce platform, providing unique opportunities to integrate diverse business and technological objectives and operations. From a business perspective, enhanced methods of working with partners and sharing information, services, and technological resources enable inter-business synergy that was previously difficult at best. With Web Services-based identity management functionality, business can allow personnel from new business partners to access resources that were previously only available to internal staff. Similarly, businesses that have developed in-house applications and tools can now expose the capabilities those tools provide via a Web Services interface, leveraging existing functionality to add value to new customer markets via the Internet.

Web Services are fundamentally rooted in XML, using document type definitions (DTDs) to set the structure of the XML documents being manipulated for the purposes of providing the Web Services. Using XML allows for communication with a wide range of applications and data sources; XML is, by design, an extensible data format easing interoperability across platforms. Web Services leverage the XML Infoset, XML schema, and XML Namespaces as key underlying elements within the Web Services architecture (see Figure 3.5).

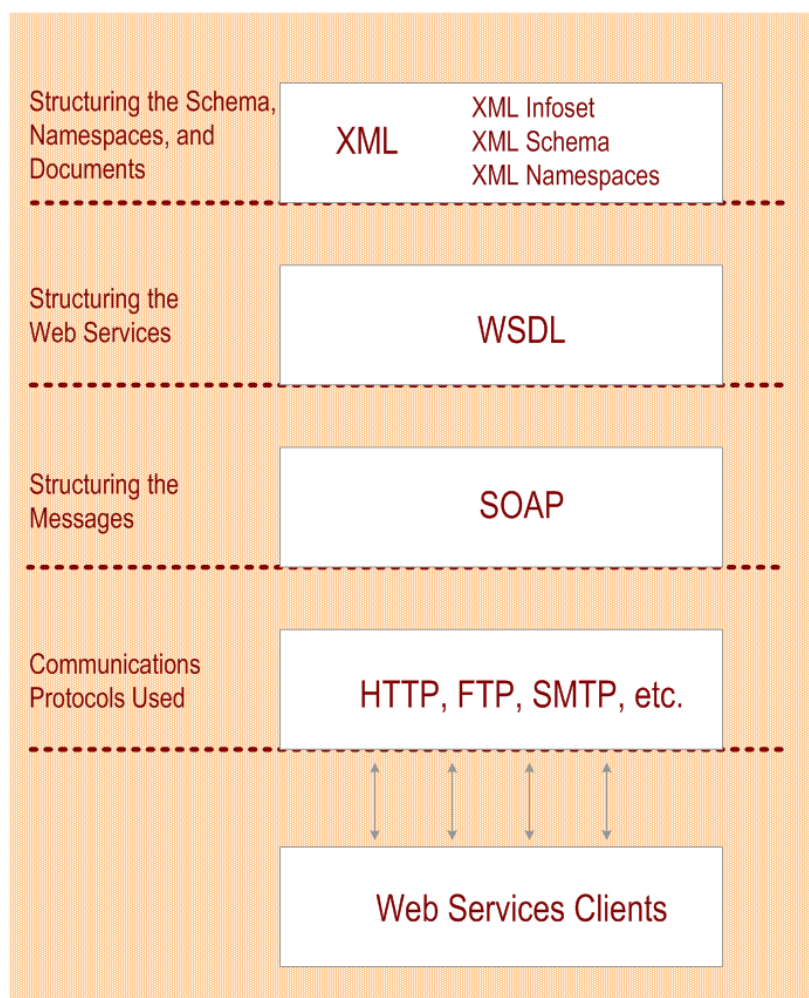


Figure 3.5: XML is the foundation for structuring Web Services and messaging, and uses common transport protocols to communicate with clients.

A core standard used for specifying how XML documents define specific Web Services are structured is the Web Service Description Language (WSDL). Web Services handle communications with clients, applications, and other service via SOAP. Fundamentally, Web Services interoperate with client applications via messages that are constructed using SOAP and are transmitted via one of several Internet communication protocols such as HTTP, FTP, SMTP, and others.

To support the range of operations needed in this new Web Services paradigm, additional Web Services protocols and standards are being developed, including a range of security standards and protocols such as WS-Security, WS-Secure Conversation, WS-Federation, WS-Trust, WS-Policy, WS-Authorization, and WS-Privacy; These protocols and standards provide secure communication, cross-enterprise policy support, authentication and authorization management, and identity federation.

 For more information about these emerging Web Service standards for security and federation, check out the OASIS Web site at <http://www.oasis-open.org>.

The support for these protocols as well as XML and its operational derivatives (such as SAML) is an essential part of providing Web-based support for the SSO functionality so desperately needed for inter-business identity federation—the mapping of user accounts and the underlying identities they represent between the Web sites, portals, and Web services. Provisioning user accounts in the Web environment and authenticating identities across platforms, sites, and services will be greatly enhanced by these Web Services developments.

Evaluating the Liberty Alliance

The Liberty Alliance is a cross-company identity information management and federation initiative driven by Sun Microsystems and supported by a wide range of industry vendors. The Liberty Alliance is dedicated to developing and implementing an identity management system that will effectively provide users and businesses with an SSO capability, such that all users could connect to any of the Web sites, services, or portals subscribing to the Liberty Alliance specifications and only have to log on once. This potential capability is a far cry from the existing state of affairs in which virtually every Web site or portal requires users to log on to each site independently.

The identity management service being proposed by the Liberty Alliance is a federated model, allowing users credentials to be recognized by each of the independent Web sites irrespective of how the corresponding user identity data is stored at the destination site. In this model, which is similar to how automated teller machines (ATMs) work, only the information necessary to authenticate who you are (your identity) and the appropriate degree of information access (your authorization) is shared. This setup differs significantly from the model employed by Microsoft's Passport system, which involves the user identity information being stored in a single structured format on Microsoft servers, requiring each vendor to authenticate incoming user traffic against this data store.

Regulatory Requirements

New federal regulations have driven the need for identity management solutions capable of providing a high level of security for sensitive information and resources. Provisioning solutions can greatly assist in managing information security by automating the assignment or removal of permissions and access controls for users in the enterprise.

Three recent pieces of legislation play a foremost role in the new demands for information security in the enterprise: the Health Information Portability and Accountability Act (HIPAA), the Sarbanes-Oxley Act, and the Graham Leach Bliley Act. Each of these laws places additional responsibilities on corporate executives and IT departments to control, monitor, and audit their information systems. Because of the civil and criminal penalties that can be enforced against companies and their executives for lack of compliance, user management and provisioning initiatives go a long way toward helping organizations meet these requirements.

HIPAA

HIPAA is legislation that is intended to protect the confidentiality of personal medical information, both in terms of its usage while providing healthcare services as well as in the transmission and handling of patient information. This information must be protected even during the insurance review of the services provided and in the accounting related to the healthcare services.

HIPAA includes regulations that cover privacy of information as well as lay out security requirements for managing the information, respectively known as the Privacy Rules and the Security Rules. Although delineated separately and having different start dates for enforcement, these two sets of rules are interconnected and interdependent regulations.

The HIPAA regulations define *covered entities* as businesses that are responsible for controlling and managing the medical information they handle (such as businesses that provide medical services, insurance companies that review and process medical information, and so on). HIPAA specifies that these entities must safeguard this data—described as Personal Health Information (PHI)—from disclosure (unintentional as well as intentional) or misuse in any way that violates the HIPAA standards or implementation specifications. By now, if you are one of these covered entities, your organization has had many meetings involving your executive, legal, HR, and IT departments to discuss the HIPAA regulations and the implications for your business.

One of the requirements that HIPAA brings to your IT environment is the need to perform regular audits of IT activities to verify that personal health information has been protected from unauthorized disclosure and/or illegitimate usage. In addition to establishing baseline security requirements for patient information, HIPAA requires that the information that *is* used or disclosed be kept to the least amount of information necessary in order to perform the required action (the intended use, request, or disclosure activity). In other words, not only do you have to prevent the information from unauthorized access or use, you must also make sure that when it is used, the minimum amount of information is disclosed.

To comply with these requirements, organizations that are considered covered entities must have security policies and procedures in place to ensure that appropriate levels of access control are implemented and that the disclosure and/or use of the personal health information is audited. Ensuring that the right users have the correct level of access, and that all use of the personal healthcare information is consistently audited, is a daunting task if done manually. This challenge becomes much easier if user account creation and the assignment of access rights is automated and controlled by policies established to enforce HIPAA compliance throughout the enterprise.

Thus, this area is one in which integration of the provisioning software with your HR database (which identify who has access to personal healthcare information) becomes far more than merely a cost-reduction measure and security improvement—it becomes a liability-minimizing mechanism for your organization. Not only will the appropriate access rights and permissions be assigned to the appropriate users, but auditing of that provisioning will also be automatic.

It is in regulation-compliance situations that a provisioning solution becomes more than merely advantageous—such a solution becomes a technology essential to implement within your enterprise. Tracking the requisite information without an automated process is not only laborious but also mistake prone—people can misunderstand the policy, incorrectly assign a user's access rights, or forget to disable a user account when the user leaves the company or moves to a position in which the user no longer needs access to personal healthcare information. Automated provisioning and deprovisioning avoids these kinds of errors, and consequently avoids the concomitant risks and liabilities. As an added bonus, the now-mandatory detailed auditing of who has access to what personal healthcare information (as well as how and when was it accessed, and in what capacity it was used) are part of the feature set that most provisioning solutions provide.

 For more information regarding HIPAA, go to <http://www.hhs.gov/ocr/hipaa/> and <http://www.wedi.org/snip/public/articles/index%7E6.htm>.

The Sarbanes-Oxley Act

Another key new federal regulation is the Sarbanes-Oxley Act, which requires extensive and rather stringent control and monitoring over the handling of financial information and financial reporting. The corporate executives (chief financial officers—CFOs—and chief executive officers—CEOs) of businesses regulated under the Sarbanes-Oxley Act are now required to assess their corporate reports and personally certify the accuracy and of the report contents. Serious penalties (including criminal charges) can be enforced against corporate offices for infractions of rules in the Sarbanes-Oxley Act.

Companies that are affected by this act must oversee the implementation of internal controls for financial systems and subsidiary systems and applications that are used in the generation or reporting of that financial information. These subsidiary systems should be considered in depth—monitoring and controlling requirements of Sarbanes-Oxley apply not only to the specific financial applications that contain the information or produce the reports but also to the entire IT infrastructure that supports the financial operations and applications. These systems frequently cross business, functional, and geographical boundaries, as well as span networks, services, applications, and IT divisions.

Adherence to Sarbanes-Oxley requirements must be documented, explicitly detailing the internal procedures used by the enterprise, and must demonstrate compliance with the all of the Sarbanes-Oxley requirements. Yet, in order to do so, these executive officers must have access to far more detailed procedural and auditing information that shows every internal procedure used to track financial information and demonstrate control over that information and the processes that produce it.

In this arena, provisioning can lend a very large helping hand, by establishing access controls that limit who has access to the financial information and what information they have access to. All of this responsibility can be automated using a provisioning solution, enabling company executives to set policies that render company operations in compliance with the Sarbanes-Oxley requirements. Importantly, provisioning solutions also manage the deprovisioning of user accounts and access to sensitive information, not only improving overall security but also helping you meet the strict access control demands specified in the Sarbanes-Oxley regulations.

 For further clarification of the Sarbanes-Oxley Act of 2002, review the information at <http://www.sarbanes-oxley.com/> and <http://www.sec.gov/spotlight/sarbanes-oxley.htm>.

The Graham Leach Bliley Act

The Graham Leach Bliley Act of 1999 is a federal regulation that addresses a range of issues affecting how banks, insurance firms, and other companies handling financial information operate, and additionally specifies new rules for the management and protection of identity information in financial transactions. This act defines a set of regulations that requires companies to handle customer financial information with new security and privacy constraints in mind.

To begin with, companies must strictly control how their employees access customers' financial information, limiting access to the specific customer financial data that is needed to perform the tasks related to their job, and not allowing employees to globally access information that falls outside of the purview of their job. An employee at a bank who is responsible for processing credit-card applications for customers, for instance, is not allowed to access mortgage or loan-related information for those same customers.

In addition to specifying access controls and limitations, the Graham Leach Bliley Act regulates how companies create and store customer financial information, how long the information must be stored, and how access to the information is monitored and audited. There are also secondary considerations, such as the response of major accounting and auditing firms to the regulations presented in the Graham Leach Bliley Act, that require companies that use, store, or access such customer financial information to pass information security audits.

Once again, provisioning comes to the rescue of beleaguered CEOs, CFOs, and IT administrators—the features and functionality of automated user management and provisioning can also assist companies in managing their user accounts; enabling them to set policies that control access to sensitive information and supplying the auditing capabilities necessary to document compliance with this act and other federal regulations.

By carefully assessing your company's responsibilities under these new federal regulations and integrating your business and IT operational requirements into the design of policies that are implemented by your provisioning application, you can be assured that each user is granted access to only the appropriate systems and information. Additionally, when someone leaves the company, that user's access is automatically deprovisioned, protecting you from a range of liabilities. This ongoing auditing included in the provisioning and deprovisioning operations that assist in demonstrating compliance with these federal regulations is a benefit not to be overlooked.

 For more information regarding the Graham Leach Bliley Act of 1999, check out the details at <http://banking.senate.gov/conf/> and <http://www.keytlaw.com/Links/glbact.htm>.

Summary

Throughout this chapter, we've looked at the fundamentals of automated provisioning systems and how they are employed. In addition, we have evaluated operational aspects of the provisioning applications in the enterprise environment. Recognizing that each business and its IT environment is different, various strategies for assessing and selecting provisioning solutions were presented. Which strategy to use—integrated suite or best of breed—and whether to develop provisioning yourself, hire consultants to build it for you, or to buy it off the shelf, fundamentally comes down to your assessment of what works best for your company.

In all of the provisioning applications, an underlying directory service provides infrastructure support for the identity management, authentication, and access control operations that must be performed. Accordingly, the various directory architectures were reviewed in the context of implementing provisioning solutions.

Application-specific factors involved with the integration of provisioning with common enterprise applications, such as HR software, messaging systems, portals, and content delivery systems highlighted the significance of provisioning as technology that crosses platform and application boundaries.

Support for provisioning is also being seen in some emerging technologies and standards, where developments in XML-based specifications are supporting provisioning operations. Web Services technologies are supplying cross-business integration of services and provisioning efforts are buoyed by the inter-business Web-based authentication and authorization mechanisms developed by the Liberty Alliance consortium.

With the advent of several new federal regulations requiring companies to control, monitor, and audit information access much more closely, provisioning is shown to play a key role in enabling companies to meet the new demands of the HIPAA, Sarbanes-Oxley, and Gramm Leach Bliley regulations.