realtimepublishers.com™

The Definitive Guide™ To

Identity Management

SafeNet®
The Foundation of Information Security

Archie Reed

Copyright Statement

© 2004 Realtimepublishers.com, Inc. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtimepublishers.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 Realtimepublishers.com, Inc or its web site sponsors. In no event shall Realtimepublishers.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.

Realtimepublishers.com and the Realtimepublishers 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 Realtimepublishers.com, please contact us via e-mail at info@realtimepublishers.com.

Chapter 3: Identity Management Applications

Time has been spent in the previous chapters gaining a common vocabulary and baseline understanding of the Identity Management components and concepts. Given the argument that in the Identity Management space no one size solution fits all, the goal now is to provide a run down of the Identity Management players and the key differentiators in their products.

One of the common ways to progress Identity Management projects is to focus on key initiatives that can immediately provide return on investment (ROI). There is a danger in the planning phase, however, of considering only a single part of the Identity Management equation. For example, consider the impact of implementing a password management solution and later implementing a provisioning solution that provides its own password management. This situation could result in significant integration costs or the need to re-implement the same functionality based on technology from a different vendor.

This chapter deals with the vendors who provide solutions in the Identity Management market. As we go through the various options for your specific requirements, consider the long-term issues and goals of your organization. Maintaining this perspective as we move toward Chapter 4 will smoothly shift our focus to the business and technical side of your Identity Management implementation.

Self Service

The ultimate goal of delegated administration solutions is to allow individuals to manage their account information and ultimately be able to provision and de-provision their services—self service. The reason for this setup is to minimize the costs associated with customer care and Help desk measures. Processing behind the scenes can range from simple, such as group membership affecting broader access to resources, through complex workflow that requires approvals or external service activation.

Provider Self-Service

Within the consumer vendor space, such as commercial Web sites, telecommunications providers, and more general service providers there is a need to offer services to individuals and organizations. Traditionally, providers have focused on being able to offer packages of services that are predefined and sold through stores or partners. The goal today is to allow *a la carte* service choices.

Consider a cell phone provider who wants to enable its customers to add or remove (preferably add, of course) extra capabilities or options to existing agreements. In this case, the option to allow this transaction is generally associated with the stores that sell the devices. However, in some cases, customers can go to the provider Web site to do so. Even the simple capabilities from providers such as Sprint in the USA allow customers to log on to the Web site and change parameters of their accounts such as the Web sites they can see from the phone. The primary issue faced by providers is matching requests for service to billing events.

To realize revenue through tiered services, usage-based services, and content, you must manage service level agreements (SLAs) such that you provide quick and efficient provisioning of services. You can accomplish SLA management through a delegated administrative model. For example, Bridgewater Systems provides central control of subscriber access to the network, services, content, and applications. Bridgewater Systems provides the ability to know who accesses your network, what they're accessing, and from where they can access it, as well as the ability to control and optimize the use of resources on a per-customer basis (business, consumer, wholesaler, retailer) and minimize and eliminate abuse and non-revenue usage on your network.

Enterprise Self-Service

The requirements for enterprise self-service revolve more around requesting accounts be set up on specific systems to allow employees to perform their jobs. Beyond the password management requirements, which we will discuss shortly, the most common identity issue faced by employees in the enterprise is gaining access to resources (for example, enterprise applications, premises or buildings, communications services). In these cases, it is common that the employee knows more about what he or she needs to do his or her job than others, and the ability for employees to easily request and acquire those necessities is significant.

Often employee requests go through tortuous bureaucracy including paperwork, processes, approvals, and so forth. Implementing enterprise self-service solutions (including password management) requires the Help desk and support groups to be extensively involved and necessitates that you clearly identify the business processes that are required to support the provisioning of resources. We will discuss this in detail in Chapter 4. For example, Courion offers three products that relate to enterprise self-service and password management. The company's PasswordCourier provides functions such as password reset and synchronization.

Password Management

Password management is seen as one of the key costs in both enterprise and commercial businesses. The cost of dealing with forgotten passwords can be significant, in some cases at least 25 percent of Help desk or support center costs. Hence, one of the goals of many organizations is to allow individuals to manage many of their password problems—forgotten or standard password resets in particular. Password-management products offer a solution for the immediate issues faced in these situations, with expected costs ranging from $1 to $15 per user, depending on the quality of the offering, how many password issues they solve, and the size of the deal. The more complex the passwords and more passwords a user has to remember, the more likely it is that the user will forget them or create an insecure way to remember them (that is, write them down somewhere).

Let's first consider enterprise-specific solutions. There are several methods that vendors offer to support password management in the enterprise. When existing systems already implement password policies, you need to corral their capabilities using a password management solution.

Some of the primary vendors in the password management space include BindView, Blockade, Courion, and Symark Software. In addition, vendors of larger Identity Management offerings that include password management functionality include Oblix, Waveset, Computer Associates, and Protocom Development Systems.

After you have aligned your decision to deploy a password management tool with the need for more extensive Identity Management capabilities, you'll need to consider the following key decision criteria (regardless of whether the password management tools are distinct from other solutions):

- Where does the tool store the password information; specifically, does it use its own database or does it rely on an existing source of user information, such as a directory or database (or can it do both)?
- How does the product secure the information it stores? More specifically, what encryption solutions are used, and how is that process secured?
- Which end user access methods are employed (for example, HTTP, VoiceML, SMS, or WML)?
- Which standards does the solution support? Key standards are Lightweight Directory Access Protocol (LDAP) as a directory and SQL for most database access (albeit most vendors offer distinct flavors of their own). Beyond that, is there a standard API to manage the system from other applications?

Password Reset

Managing password resets across systems, whether in the enterprise or for a commercial site, the common solution is to provide a Help desk or call center that can manage the process, interact with the individual, and enact the change. Traditionally, password changes performed by a Help or support desk require the individual to answer one or more "challenges" before the user is allowed to request the change. In effect, this challenge is usually more of the something-you-know type of question and answer set, organized previously between the two parties. This process also requires an initiation process, wherein the user will provide the answer to a predefined question such as those discussed in Chapter 1. For example, Courion ProfileCourier is designed to let users privately and securely register authentication questions and answers, then store the results for later use in reset situations within existing databases and LDAP directories.

☞ An article related to password reset capabilities is available at http://www.networkmagazine.com/article/printableArticle?doc_id=NMG20020103S0002.

Password Synchronization

Password synchronization solutions use a sync engine to ensure that passwords are consistent across systems. This functionality allows for users to use the same password across multiple systems. When one password is reset, all are updated automatically. Unfortunately, this capability does not solve the potential issue of naming. We'll discuss the naming issue in detail in Chapter 4, but for now, consider the synchronization solution as a stop-gap in the land of Identity Management solutions. Password policy enforcement solutions ensure that new passwords follow not only OS requirements (number of characters) but also the network department's policies (such as restrictions on reusing the same password).

Single and Similar Sign-On

Chapter 2 outlined the basics of single and similar sign-on. What that discussion highlighted was that there are many different “flavors” of SSO. End users, security experts, industry commentators, and vendors all have their own thoughts about what SSO is, how it can benefit business productivity, and how it should fit into an Identity Management framework. Many vendors who target products at this particular market are quick to claim that their particular product will solve your SSO (and Identity Management) problems. However, unless your view of SSO (and more important, your business requirements) lines up exactly with that particular vendor, the reality may be very different. None of the vendors truly has a full solution for your specific environment, and you might require combinations of strategies and products to you’re your organization’s business, technical, and security needs. This section will discuss products in the SSO space and highlight their strengths and weaknesses, using the models outlined in Chapter 2 as a basis.

Network Operating System-Based SSO

Network operating system (NOS)-based SSO is probably the most understood area of authentication management, though few people would consider it a part of the SSO space. When a user logs onto a NOS (Microsoft NT 4.0 or Win2K, Novell eDirectory/NDS, and various implementations of UNIX NIS products), the user receives some form of token to identify who they are to that NOS. When the user accesses other resources, such as printers and file shares, that are part of the NOS, the user doesn’t need to explicitly provide credentials—SSO, if you will. Other applications can be developed that leverage the native APIs of the OS such that credentials don’t need to be explicitly supplied by the user as well. Most of the Microsoft BackOffice products such as Exchange function this way.

This feature has some major drawbacks. For example, NOS-based SSO requires all application vendors to write their applications to use the native OS APIs—an onerous and largely improbable task. Also, it requires a company to standardize on a single vendor’s OS. This situation lead to the OS “wars” of the mid-1990’s. The advent of the Internet changed the landscape tremendously. Application vendors wanted to develop their applications for eBusiness and not for a specific OS. The OS, in many ways, became secondary, and eBusiness directories such as Netscape became very popular. Also, both Novell and eventually Microsoft came out with LDAP-compliant directory stores allowing vendors to utilize the LDAP repository (whatever it happened to be) rather than the NOS directory using the native APIs. In addition, both Sun Microsystems and IBM now offer the option of replacing the local security database or NIS infrastructure with their respective directory products, making it much easier to rely on the NOS infrastructure for reduced and consolidated logons and making integration with enterprise SSO and/or Web-based access control systems easier.

Although it is easy to discount the NOS in today’s world, it should be evaluated, particularly within corporate intranets. Although most applications today run on Web servers, some have the ability to make use of the underlying NOS credentials and authorization capabilities (groups, for example). Although not as fully featured as a Web-based access control system, it may suffice in certain circumstances. Also, there are still many applications that integrate natively with the respective OSs, and this is a valid way of reducing sign-on. In addition, with the introduction of Kerberos in Win2K, cross-platform Kerberos communities can sometimes be established (although with difficulties).

- For more information about Kerberos, check out the following Web sources:
- http://web.mit.edu/kerberos/www/
- http://www.ietf.org/rfc/rfc1510.txt
- http://support.microsoft.com/default.aspx?scid=KB;en-us;248758&

Web-Based Access Control SSO

There are many vendors in the Web-based access control SSO market, though consolidation and attrition is bound to reduce this list to a much smaller number over the next few years. Table 3.1 shows the main vendors as well as their products and URLs.

Vendor	Home Page	Product
Baltimore Technologies	http://www.baltimore.com	Select Access
CrossLogix	http://www.crosslogix.com	CrossLogix3
Entegrity Solutions	http://www.entegrity.com/	AssureAccess
Entrust	http://www.entrust.com	GetAccess
Evidian	http://www.evidian.com	PortalXpert
IBM	http://www.ibm.com	Tivoli Access Manager
Netegrity	http://www.netegrity.com	SiteMinder
Novell	http://www.novell.com	iChain
Oblix	http://www.oblix.com	NetPoint
OpenNetwork Technologies	http://www.opennetwork.com/	DirectorySmart
Oracle	http://www.oracle.com	Oracle9*i*AS SSO Server
RSA Security	http://www.rsa.com	ClearTrust
Sun Microsystems	http://www.sunmicrosystems.com	Sun ONE Identity Server
Avalon Works (Texar)	http://www.avalonworks.com	SecureRealms

Table 3.1: Web-based access control SSO vendors and their products.

Overview

As you might recall from Chapter 2, Web-Based Authentication Managers (WAM) authenticate users or defer authentication to a directory (or other source) and enables a session for multiple heterogeneous applications. In addition to SSO, most Web-based access control solutions implement some form of authorization/role-based access control often based on proprietary technology, and increasingly based on the maturing SAML standard, as the following steps walk you through.

1. An end user accesses a particular URL (or other Web resource such as an Enterprise Java Bean—EJB) that has been protected by a Web-based access control system.
2. The user's request for the resource is intercepted and redirected to a central authentication Web form.
3. The user enters his or her credentials, and the WAM then carries out the authentication against a central user database (often an LDAP-compliant directory).
4. The Web-based access control system now sets some form of access token in the user's browser to identify the user for further interactions with Web-based access control–protected resources. This is usually of the form of a non-persistent encrypted cookie that contains information that uniquely identifies the person in the underlying user database—passwords are not stored in the token.
5. Once the user is authenticated, most Web-based access control systems perform authorization and role-based access control for the resource based on preconfigured policies. Each of the vendors has a policy server of some form to provide the authorization. Basing the interaction with this component on SAML has become common practice for most vendors, though the implementations are still challenged in the interoperability area. If the user is authorized, the user is granted access to the resource.
6. Although the access token is valid (not expired), future access to Web-based access control–protected resources skip the authentication process (steps 1 through 4) as the identity of the user is known by examining the access token, thus providing SSO. These resources could be on different Web servers on different platforms across the company (and across domains in some cases). The authorization policies are still applied, but this is transparent to a user unless the user is denied access.

Web-based access control systems can provide a great deal of flexibility. Some common additional functions include:

- The ability to configure additional authentication schemes (or write your own). For example, certificate authentication or hardware tokens (for example, SafeNet's iKey and RSA Security's SecureID) can replace or complement the traditional user ID and password during authentication against a particular Web site.
- The ability to configure additional authorization schemes (or write your own). For example, an organization may have a specific database with role information they want to access. For security reasons, it might not be appropriate to synchronize this data with a central source, so they could write a custom authorization plug-in to perform the policy assertions directly against the special purpose database.
- Personalization can be achieved by passing attributes relating to the end user to the requested Web site or application. Integrating Web-based access control applications with portals is a common use of this technique, allowing personalization to be achieved within the portal and SSO between the portal and other intranet or Internet resources.
- Access controls to allow or deny access during particular times of the day or from individual IP addresses.
- Auditing of successful and failed attempts to access resources can be logged (both authentication and authorization attempts) with many of the vendor products.
- Ability to integrate non Web-based applications into the Web-based access control system. This feature usually requires custom development using a software development kit (SDK) provided by the vendor. This feature is particularly useful within corporate intranets, as it allows a common security framework to be used for Web-based and non Web-based applications. However, this kind of custom development is usually a non-trivial task.

As you can see, Web-based access control systems can play an integral part in a security framework and Identity Management system. The four A's, as outlined in Chapter 1, are available (Authentication, Authorization, Access Control, and Auditing). However, in and of themselves, they are not a total Identity Management solution (though some vendors such as Oblix and OpenNetwork offer strong Identity Management components to complement their Web-based access control systems). They all have a reliance on the availability of an underlying identity directory/database (as well as a policy server). You might use other related technologies such as eProvisioning, meta-directory processes, and self-service to manage the user data present in the directory to ensure data integrity.

> Having a high level of data integrity is vital when using Web-based access control solutions. They can be used to grant or deny access to very sensitive data based on an employee's management level, for example. If the incorrect management level is assigned to a user in the underlying user database (for example, as the result of an incorrectly configured meta-directory process), there is a very real risk that sensitive data might be exposed to an unauthorized user.

Being able to rely on an external shared security system allows applications to abstract the security sub-system from their application to this centralized authority. In this way, based on the definition in Chapter 2, Web-based access control systems can be seen to be providing true SSO as opposed to similar sign-on.

The key to keep in mind is that the Web-based access control system provides a central trusted security infrastructure. All participating Web servers and applications integrated implicitly trust it to provide all the security services they require. Although this might be of significant benefit particularly for in-house developed applications, it might not always be the best solution or in fact be possible to externalize all security functions.

Consider for example an employee self-service portal integrated with PeopleSoft. This kind of product usually relies on internal security (for example, PeopleSoft roles) to provide role-based access control—it is not possible to delegate the role-based access control externally from the application. It is important in this situation that the Web-based access control system can handle this and pass an identifying piece of information into the third-party application to identify the user. The authentication can be delegated to the Web-based access control system, but the roe-based access control then needs to be managed within the target application.

Web-based access control systems are particularly powerful in the customer-facing and extranet environments because of the focus on Web access to provide products and services. They are also proliferating in corporate intranets as result of factors such as the increasing reliance on Web-based corporate applications, increased portal deployments, their relative ease and cost of deployment compared with enterprise SSO tools, and the increasingly flexible integration options available.

Agent-Based vs. Proxy Model for Web-Based Access Control Solutions

Web-based access control solutions can be split into two distinct models—agent-based and proxy, as Figure 3.1 shows. The predominant technology is the agent-based model in which an agent (for example, NSAPI plug-in under Sun/iPlanet's Web server, ISAPI filter under IIS, and so on) intercepts all HTTP requests and performs authentication, authorization, role-based access control and token management.

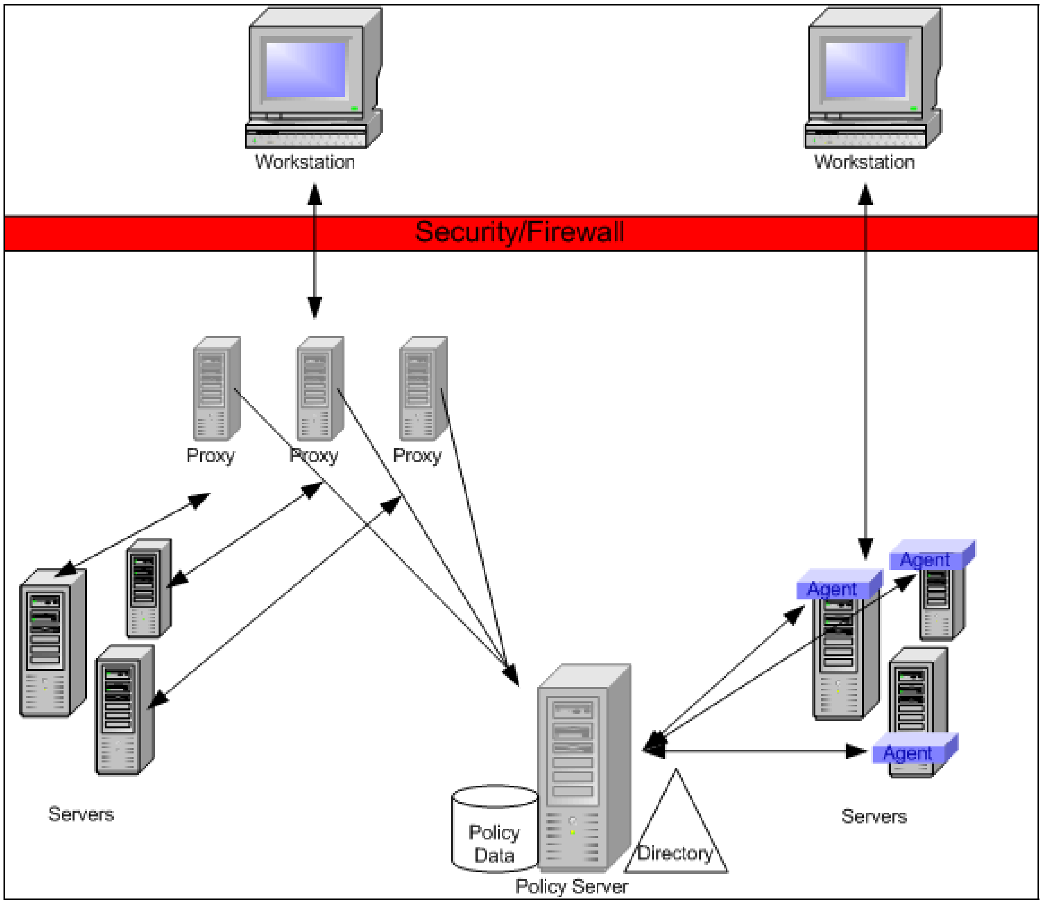

Figure 3.1: Agent and proxy-based Web access models.

Although these agents are quite powerful and fairly simple to implement, there are some major downsides to this approach:

- The overhead to manage the deployment and upgrade and maintain the agents becomes prohibitive as the number of Web servers increase.
- The agent typically places extra load on the Web platform hosting the application (depending on the complexity of the role-based access control policies, this could be as much as 15 percent).
- The plug-in is another component that interacts with the Web server and application providing a possible failure point. For example, a complex URL might not be parsed correctly or cause an invalid action to take place on the Web server.

The proxy model functions in a more centralized fashion. All requests are first directed to a proxy server rather than directly to the end-user application. The proxy server then refers to the policy server to determine the authentication, authorization, and role-based access control requirements. After the appropriate steps are taken to authenticate and authorize the user, the user's request is then passed on to the destination Web application. Although the proxy model will not suit all implementations, there are some significant benefits to this approach:

- No extra load is added to the Web servers that are hosting the protected content and applications.
- No need to deploy, manage, and upgrade agents.
- Greater stability of the end-user Web servers, and no added complexity when Web servers or applications are upgraded or modified.

> ✎ As a result of the added flexibility that the proxy model provides, most of the other vendors have plans to provide the proxy solution in the near future.

Web-Based Access Control Features to Consider

One of the first Web-based access control features to consider is integration with your existing infrastructure and OS. Some of the Web-based access control systems provide integration with particular vendor applications, portals, application servers, and OSs. This may impact (in a positive or negative fashion) their suitability in certain environments.

Some of the Web-based access control SSO vendors provide additional features that may integrate well into your Identity Management environment. These various Identity Management features include delegation, user self-registration, and user self-management (including password management). The big players provide solid features in this area and a close examination of these products is warranted in any evaluation. The following list highlights additional features offered by Web-based access control SSO vendors.

- Auditing and intrusion detection—All the products provide some form or auditing, though some are better than others. Entrust GetAccess provides a centralized storage of activity logs. In addition, both Entrust GetAccess and RSA ClearTrust offer a form of intrusion detection by monitoring log files and reporting suspicious behavior such as attempted password cracking.
- Session management—All of the products set some form of token in the user's browser to manage SSO and session management (idle and session timeouts, for example). The cookies are set as non-persistent cookies for security reasons; however, this means that exiting your browser will destroy your session with the Web-based access control system. The cookies are encrypted and can only be decrypted by the agents or proxies. In most products, the encryption is based on shared secret. Although unlikely, it is possible that this could become compromised and user impersonation may take place. Regular changes to the shared key are vital, so look for products that enable the key to be changed. Entrust is unique in that it creates a unique key for each user session, so the risk of the key being compromised is greatly reduced.

- Scalability and fault-tolerance—Performance and scalability are important factors when evaluating Web-based access control systems. The major players all scale horizontally very well and provide automatic failover features (as do some of the other players). It is also important to evaluate how the products work with any load-balancing you might already be using. Some Web-based access control products might keep sessions open between components and have problems (or reduced performance) if subsequent requests are directed to a different server.

> ✐ If you are interested in pure throughput, review the statistics Mindcraft released (http://www.mindcraft.com). Be aware, however, that every 6 months or so one of the vendors will put their product through the testing suite and likely leapfrog the other vendors. It would be interesting to see a full test of all vendor products at a specific point in time to provide a valid comparison. As a result, consider pure throughput performance as one of the lower-priority considerations, unless one product is a long way behind or ahead of another.

- Value add and extra options—Some of the products provide extra components that might make the choice a compelling one for your organization. Entrust has a mobile access server component that allows access from WAP-enabled devices. As multiple channel access becomes more important, this kind of product could become important. Oblix has the ability to expose identity data and programmatically manage the product using SOAP and components called Identity XML. This standards approach and flexibility are an added bonus. RSA Clear Trust (through SmartRules) and Netegrity SiteMinder (through e-Telligent rules) provide extended rules for managing role-based access control that are powerful and flexible.

The Future of Web-Based Access Control

The Web-based access control space will continue to evolve as companies fight for market share and survival. It is really a fight for the Identity Management space as well. The big vendors such as Sun and IBM have shown that they are very interested in the area of Identity Management and have re-aligned their organizations and products to help target this area.

The current market leaders will work hard to highlight their strength, knowledge, and experience in this field as well as add value in other related Identity Management fields through product evolution, partnerships, and perhaps acquisitions. At the same time, application server vendors will be entering this field more and more. All these vendors are players in the portal space, which could be argued as being a component of Identity Management (at least a consumer of identity data). It makes sense as they add and enhance functionality (such as security modules and personalization), that vendors will start to provide general Identity Management functions and more specifically Web-based access control. The next 2 to 3 years will see some major changes in this entire industry.

Client-Side SSO

As mentioned in Chapter 2, a client-side SSO solution relies on proxy-based sign-on using a client-side secret store. Some of the vendors in this area include Passlogix, Novell, and Digital Persona.

Overview

A user first logs onto a desktop using local or NOS credentials (or some other mechanism such as smart card or biometric device). The user then needs to gain access to an encrypted local store. This could either be automatically granted based on the user's successful logon or a secondary authentication mechanism may be employed. Although this process might seem a little redundant, the secret store will contain all IDs and passwords for the applications across the intranet and Internet. It is vital that this data is not compromised.

The client-side SSO software offers various options for capturing logons to different applications and systems. Some applications may be preconfigured by the vendor or the administrator, though client interaction is often needed to identify the application and configure it to record the logon attempt. Logons to all manner of systems can be captured into the local store for replay during subsequent access attempts. Applications such as client/server applications, Telnet sessions, intranet and Internet Web forms, and mainframe logon, to highlight a few, can be captured and replayed.

The whole concept is fairly simple on the surface. However, it does not attempt to resolve the issue of multiple authentications long term—it simply masks the problem. It is then difficult to make reducing and improving authentication systems a priority. There are also some quite complex issues to solve when designing a secure client-side SSO. In addition, there is generally an onus on the end user to configure and manage the product at the user's local desktop, and a corresponding increase in Help desk calls when problems occur. However, there are certain situations in which this kind of solution would work well, so it should not be dismissed.

Client-Side SSO Features to Evaluate

Most of the issues with client-side SSO relate to managing and securing the local store. Hence, this area is one to look closely at when evaluating any product.

Next, consider the location and management of the store. If the store is located only on the local machine, the solution is generally meant for a standalone user and not for a corporate environment in which end users may logon from different machines. There really needs to be a mechanism for the store to roam with the user. This is often accomplished with roaming profiles under NT 4.0 and Win2K. However, this in itself can be limiting and may not be secure. Other mechanisms such as locating the store in a central location can be good options. Many vendors allow you to locate the store in AD.

When products store their encrypted passwords in centralized locations and centralize their administration and configuration, they start to encroach into the enterprise SSO tools category. Novell's Secure Login is an example of this crossover, but is included in this client-side SSO discussion because it can be configured to have many of the characteristics of this product category. Examples of these features include the ability for users to add new applications for SSO, modify control settings on how the product behaves, and view existing applications and passwords that SSO has been enabled for (all these can be disabled by the administrator).

How do you manage the local store for factors such as backup and recovery (including key recovery)? Different products have various management functions to support this kind of operation? How does this fit in with your overall administration strategy?

The local store is a vital piece of the overall infrastructure—if it is compromised, access to all applications is then available to the intruder.

Another feature to evaluate is the private store's security. How is it secured if it is part of a roaming profile, a database, or a central directory? One product on the market, for example, allows you to integrate PKI and biometric devices with access to the central store. If you are going to implement client-side SSO, using additional security measures is highly recommended.

A third feature to evaluate is how a product handles password changes. Most products provide a method for intercepting the password changes on target applications (including the NOS). How do they handle prompting you for information? What happens if the password is disabled—what are the error messages to the end user? What happens if you change the password directly against the native system from another workstation—how are the passwords reconciled?

In addition, some products can be configured to silently change the password on your behalf. The benefit is that the user does not need to enter passwords thus increasing productivity. Also, the SSO application can enforce complex passwords that won't be as vulnerable to attacks, such as dictionary attacks. The real problem here is if the person attempts to logon from a workstation that does not have access to the SSO components—the user is effectively locked out of all applications. Think very carefully before implementing these kinds of features.

Finally, evaluate what level of client-side software exists? Microsoft Windows is shipped to load and execute the standard Microsoft Graphical Identification and Authentication (GINA) DLL called MSGina.dll. Microsoft allows for the replacement of the GINA DLL. Some vendors replace the Windows GINA logon code in order to provide the biometric sign-on. This makes the store more secure because the finger print is used to logon to Windows and unlock the password store, but the replaced components create a management overhead to deploy and upgrade.

Care needs to be taken because upgrading the OS might cause problems with the GINA.

Client-Side SSO Summary

Client-side SSO products will continue to play a part in the SSO landscape. However, to be truly applicable in corporate environments, they will need to increase the level of centralized management and administration, thus encroaching more and more on the enterprise SSO space. The market leader will be determined by who offers the widest range of application support, strong authentication integration, centralized management, and cross platform flexibility.

Enterprise SSO Tools

Enterprise SSO tools rely on network server proxy–based sign-on using a centralized secret store of some form as opposed to a client-side cache. These products have many common features with client-side SSO tools, and in fact, some products may be able to be placed into both categories. Some of the vendors in this area include BioNetrix, Computer Associates, Evidian, IBM, Novell, PassGo, and TrueSystems.

Overview

To access enterprise SSO products, users can logon to a desktop using NOS credentials or users can logon to the enterprise SSO after NOS logon. The user interaction with the SSO product can then be tightly controlled. This allows functions such as:

- Presenting a personalized desktop for users listing available applications
- Controlling which applications users have access to
- Auto-starting certain corporate applications for users
- Allowing multiple users to share a PC, sometimes in a kiosk mode in which the logon to the NOS or desktop is not part of the enterprise SSO

The enterprise SSO software can be preconfigured to intercept logons to certain applications and/or end users can add or configure logons themselves. The logon processes and handling of password expirations and other password management functions can be scripted. Logons to all manner of systems can be captured into the network store for replay during subsequent access attempts. As with client-side SSO tools, enterprise SSO tools can capture and replay applications such as client/server applications, Telnet sessions, intranet/Internet Web forms, and mainframe logons.

Also similar to client-side SSO, enterprise SSO does not attempt to resolve the issue of multiple authentications long term—it also simply masks the problem. Enterprise SSO implementations are generally quite complex due to the difficulty in handling the large variety of applications present in a typical organization. They often requiring complex scripts to be developed. Some of enterprise SSO product vendors offer simple drag-and-drop and wizard-driven configuration tools to ease some of this pain. Although such tools might be of help, the whole process is still difficult and time consuming to get right. Also, end-user interaction is still usually required at some point. User problems and frustrations will still be evident in the number of Help desk calls, though it will still generally be an improvement over client-side SSO or if no SSO is available.

Enterprise SSO Features to Evaluate

Enterprise SSO products are very complex and each of the vendors approach the solution in a slightly different manner. Before evaluating any of the available products, ensure that you have a very good understanding of your internal systems and an awareness of the security implications and user training requirements of each product.

There are major security implications with enterprise SSO products as a result of the fact that they manage passwords and accounts centrally and proxy user logons. Look for vendors with high levels of encryption associated with their central stores, controls on who can gain access to the stores and administrative tools, and which auditing and reporting capabilities are available (for both administration and end-user access to applications). Another useful feature that most vendors offer is the ability to seamlessly intercept password resets in the target systems and set difficult to remember and crack passwords. Apart from increasing the strength of the passwords themselves, nobody actually knows them (though this fact can cause problems if someone ever needs to access the application using the native authentication for some reason). Combining stronger authentication mechanisms such as certificates, smart cards, Biometrics and hardware tokens using products such as SafeNet's iKey is highly recommended to ensure that the security of the SSO account is not compromised. All the vendors provide features in this area that can be used to securely lock down and audit their enterprise SSO product.

Additional features to evaluate include configuration and management. As mentioned earlier, administering, configuring, and deploying enterprise SSO tools can be very complex. Taking this in mind, evaluating the relative strengths and weaknesses of the vendors in this area becomes very important. Is the initial configuration easy to accomplish? How easy is it to add new applications to the system and assign them to groups of users? What kind of policy management is available? Is delegation of administration available—how is it accomplished? How open and flexible is the architecture so that it can adapt to changing needs? What level of end-user interaction is required and how intuitive is the end-user interface? Does it support your primary applications and platforms or is there a large amount of customization required? How flexible are the password management features—do they detect expiration adequately and allow random strong passwords to be silently applied?

You also need to consider products' scalability and fault-tolerance capabilities. Enterprise SSO products become the central gateway to all corporate applications. Having the ability to scale to meet the needs of end users and having a fault-tolerant implementation is vital to the success of any enterprise SSO implementation. Most of the vendors offer some kind of support in this area, but it is important to look closely to see that it will suit your particular needs and integrate with your current infrastructure, including your load-balancing and failover components.

If the enterprise SSO system responds poorly or, worse, fails, productivity across the entire enterprise slows or comes to a screeching halt. Planning a fault-tolerant environment is absolutely vital.

Finally, evaluate how a product integrates with the existing infrastructure and OS. Enterprise SSO products will become major components of a corporation's environment. Thus, it is very important to evaluate how they will integrate with the current or planned infrastructure and OSs.

Summary for Enterprise SSO Tools

The main recommendation for evaluating an enterprise SSO tools is not to underestimate the complexity of an enterprise SSO deployment and management. Many deployments either fail outright or are only partially deployed. Like most Identity Management components, enterprise SSO implementations are not just a technology solution. Processes, procedures, security, and politics are very important, as is a very high level of corporate sponsorship. Evaluate your requirements carefully and set your scope small at first. Trying to solve all your authentication problems at once will be too difficult. Also, don’t lose site of the fact that consolidating back-end security and authentication environments is still something worth doing, even though it can be masked by enterprise SSO products. Doing so will help make your enterprise SSO less complex and easier to manage, thus providing more business value.

As with other Identity Management areas, changes are taking place quickly in the enterprise SSO space. Some vendors are bundling their products under an Identity Management banner, offering complementary (and sometimes overlapping) products in an attempt to provide a complete solution. Each suite of products offers some form or provisioning, meta-directory, enterprise SSO, and Web-based access control product. Although none of the vendors offers a complete Identity Management solution (or has a best of breed application), the combined products make a compelling option for some environments. However, these suites of products make it harder for best of breed applications to survive. Thus, as with other Identity Management areas, we will most likely see some attrition in this field in the next few years.

Password Synchronization SSO

Password synchronization SSO is rarely a full SSO solution by itself. Often it is a part of related products, such as centralized password management (resets), provisioning, and even enterprise SSO solutions. Vendors in this space include Blockade and PassGo. Password synchronization is often seen as weakening the overall security. Briefly, the way password synchronization works is as follows:

1. A series of authentication sources within an enterprise are identified to be involved in the password synchronization process.
2. Agents or plug-ins with the capability of accessing the credentials in the underlying security subsystem are deployed.
3. A relationship between each of the “secret store” plug-ins is established such that when a user changes one of the passwords in the native system, the change is propagated to all the related systems. The user IDs are usually the same in all systems, but don’t have to be.

Users still need to enter their passwords when accessing each of the systems, but their password is the same each time. Although this setup makes it easier for users to remember their passwords (rather than remembering multiple passwords), there are some major downsides:

- The password policy needs to be set to the lowest common denominator. Thus, a system that is part of the synch process can only handle at most six characters and can only handle alpha-numeric characters (or words, only alpha). Strong password policies such as forcing users to employ punctuation can't be deployed.
- If the password is compromised, the intruder can gain access to all applications. This possibility is very real if access to some of the systems has to be in clear text.
- It is difficult to link up all the systems for which an enterprise might want to provide SSO.

> ✎ The recommendation with password synchronization products is to use them as "point" solutions or as part of a provisioning or password reset solution only—and then to do so with care.

Password Propagation SSO

As with password synchronization SSO, password propagation SSO is rarely a full SSO solution by itself. Often it is a part of related products such as centralized password management (resets) and provisioning solutions. I'll discuss password propagation in more detail in the following provisioning section.

Provisioning Solutions

Provisioning solutions are currently considered a large part of any Identity Management solution and have the potential to impact the broadest parts of your infrastructure as well as cross the boundaries into your partner networks. The leading vendors in the provisioning space are Business Layers, Waveset Technologies, and IBM. However, many other vendors are moving into this space very quickly, often leveraging or re-aligning existing products and marketing them as provisioning products. In addition, the meta-directory vendors are enhancing their products to be able to perform certain provisioning tasks. Clearly identifying your requirements is vital before attempting to choose and deploy a provisioning product.

As referenced in Chapter 1, provisioning solutions often incorporate other parts of the Identity Management framework, such as self-service and password management. With provisioning products, as noted at the beginning of the chapter, you run a risk of implementing one solution that can potentially clash with another.

Provisioning solutions are similar to SSO solutions in that they operate from the top down. Thus, the application manages all the systems under it. Administrative functions, from the essential add, modify, and delete to the more general maintenance and monitoring are under the control of the provisioning system. As mentioned in Chapter 1, provisioning functions can also include non-electronic tasks such as identifying a cubicle, connecting a network port, acquiring a PC, and the like. Figure 3.2 illustrates a typical provisioning architecture.

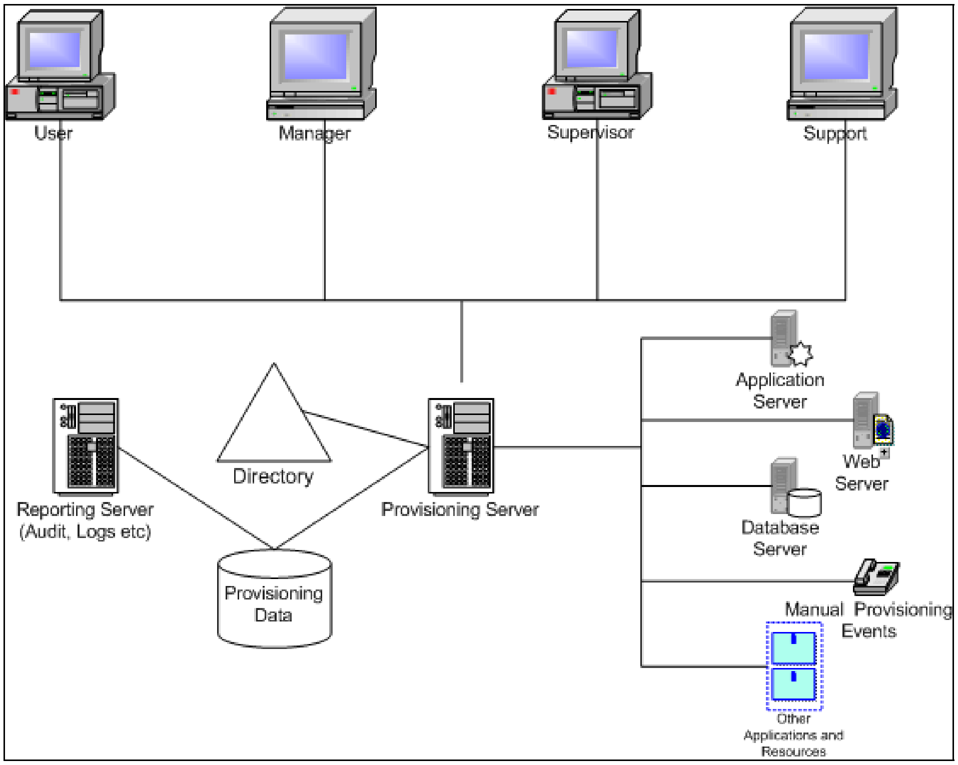

Figure 3.2: Typical provisioning architecture.

To summarize how a typical provisioning system works, the following steps walk you through how the add, modify, and delete components tasks usually work. To add components:

1. A manager, administrative assistant, or systems administrator enters information about a new employee or contractor into an interface (usually a Web form).

> ✎ Most products provide the capability of kicking off the provisioning process by receiving a feed or some form of notification from an external database such as an Enterprise Resource Planning (ERP), Sales Force Automation (SFA), or Customer Relationship Management (CRM) system rather than having it entered manually in a provisioning interface.

2. The information is then routed using predefined internal workflow rules to an approver (this may or may not be bypassed if the data came from an ERP system, depending on the defined business rules).
3. After the appropriate person provides the approval, the provisioning server accesses target systems either directly or by connecting to an agent, and creates the users accounts. This functionality lets you provide consistent naming standards, linked accounts, consistent identity information, and the establishment of roles.

To modify components:

1. A manager, administrative assistant, or systems administrator enters information about a modification for an employee or contractor into an interface (usually a Web form). This modification could be a name change or correction, a department change, a change in access to a specific application, a suspension of account requests, or even a password reset request.

> Most products provide the capability of kicking off certain changes by receiving a feed or some form of notification from an external database such as an ERP system rather than having it entered manually in a provisioning interface.

2. This modification is then routed using predefined internal workflow rules to an approver (this may or may not be bypassed if the data came from an ERP system, depending on the defined business rules).
3. After the appropriate person provides the approval, the provisioning server changes details in its core database or directory, then accesses target systems either directly or by connecting to an agent, and carries out any requested modifications. This feature provides the ability to maintain consistent identity information throughout linked systems

To delete components:

1. A manager, administrative assistant, or systems administrator marks an employee or contractor for deletion in an interface (usually a Web form).

> A delete can be seen as a modification. Hence, most products provide the capability of kicking off deletes by receiving a feed or some form of notification from an external database such as an ERP system rather than having it entered manually in a provisioning interface.

2. This information is then routed using predefined internal workflow rules to an approver (this may or may not be bypassed if the data came from an ERP system, depending on the defined business rules).
3. After the appropriate person provides the approval (or the person performing the action has the appropriate delegation), the provisioning server changes details in its core database or directory, then accesses target systems either directly or by connecting to an agent, and disables or deletes the target accounts. This functionality provides the ability to remove accounts from the appropriate systems in a prompt and consistent fashion.

Provisioning Features to Evaluate

As mentioned earlier, provisioning products are very complex and each of the vendors approach the solution in a slightly different manner. Before evaluating any of the products available, ensure that you have a very good understanding of your internal systems and an awareness of the security implications and user training requirements of the product.

> ☞ Network Computing recently carried out an evaluation of provisioning vendors that is a useful reference. It is located at http://www.networkcomputing.com/1317/1317f2.html.

Security Implications

Provisioning solutions are often sold to organizations based on the product's ability to improve security by managing consistent policy and removing accounts after people have left. The solutions also have security implications because the agents or connectors have a high level of authority over your corporate systems in order to achieve their functionality. You don't want passwords stored in clear text or being passed in the clear between systems. In addition, the password reset processes can synchronize passwords between multiple systems and reduce the security of the end systems in the process. Ensure that you implement these components of the products with care. Use of agents or connectors is an area to examine closely. A later section highlights their security implications.

Configuration and Management

Deploying full-blown provisioning systems is a massive undertaking. You have to map out all the planned systems in advance, including all the nuances such as to which group a person needs to be added, where the person's home and profile server is, where the person's mail server is, and so on. All businesses change, and change regularly over time. Departments come and go, processes change. Thus, your provisioning product needs to be fairly simple to configure and modify. There needs to be capabilities to carry out bulk changes and adapt to new business rules.

Provisioning product vendors all can provide the basic—create an account in a target system easily. The differences start to show between the vendor products when you try to implement complex scenarios and integrate other pieces of external data. For example, say you want to create a user on a mail server but you want to take into consideration the capacity of the servers available and make a choice based on data in an external database. How does the vendor product handle this? Most of them offer such functionality, but how difficult is it to implement. Implementers are often faced with complex requirements such as this when planning and deploying a provisioning solution.

Integration with Existing Infrastructure and OSs

As with any deployment of this magnitude, understanding the infrastructure present within your company is important. Some of the vendors integrate better with some infrastructures than others and can make use of other related Identity Management products.

Auditing, Logging, and Alerting

Many different tasks and activities can be initiated by the provisioning systems. Keeping track of who is initiating them, knowing when accounts were created or removed, identifying when a process has stalled and why (and resolving the problem), and dumping reports about what access people currently have is very important. Provisioning solution vendors can not only audit what took place, but can give accurate views of what access end users have to the various target systems.

Scalability and Fault Tolerance

Provisioning implementations centralize many IT system processes, potentially creating a single point of failure. Thus, it is very important that you evaluate the ability to configure redundant components and scale to meet the needs of your deployment.

Agents vs. Connectors

Some provisioning solutions work in a predominantly connector mode. This means that the provisioning engine connects directly out to the target system and creates, modifies, and deletes. Other solutions work primarily in an agent mode, in which agents need to be installed in all the target environments. There are benefits and drawbacks to each of these approaches, so evaluate what works best in your environment.

Connector-based systems are simpler to configure and manage because there is no remote installation and management of software, and it is easier to target the creation of accounts on different mail servers based on rules (if server1 is full, connect to server2). However, this could lead to potential security problems if the target system does not support encrypted communications. If you are communicating with an agent, you can build in strong security without relying on the underlying application or OS environment. Realistically, though, a combination of both is generally needed. Evaluating your target platforms and security requirements is part of the solution consideration process, and including the agent and connector discussion is an important part of this evaluation.

Summary for Provisioning Products

One of the key decision points, the process of which we will discuss in Chapter 4, is determining how much of an Identity Management solution is necessary to support your business requirements. In the case of provisioning solutions, you will find a generally complex and costly exercise is required to deliver on the standard expectations. The cost of the product is only a small part of the overall deployment costs in complex environments. However, provisioning might be appropriate for point tasks such as big password-management chores. Companies developing full-bore provisioning schemes do not need point products but those that start with basic password-management products easily can move to provisioning. All but the most narrowly focused point-product vendors offer add-ons for account-provisioning tasks. Rather than have account management for each user under every circumstance, provisioning solutions often perform a subset of full-on provisioning. This subset limits the project scope and, therefore, the costs.

Meta-Directories

Another contender in the Identity Management market works behind the scenes—the meta-directory products. These products are advancing through the addition of workflow engines and customizable UIs, and they provide an interesting alternative to the existing password management and provisioning capabilities already discussed. The main vendors in the meta-directory space today are Critical Path, Microsoft, Sun Microsystems, Siemens, and IBM.

Meta-directories may be considered the forerunner for many Identity Management solutions. The goal circa the early 1990's was to integrate data from directories across disparate systems, whether LDAP-, NOS-, or X.500-based, generally focusing on user-specific or identity data. The term was first coined by the Burton Group in its February 1996 Network Strategy Overview document "Meta-Directory Services." According to The Burton Group definition, a meta-directory is a "directory that can integrate multiple directory services within an organization."

This definition quickly changed as more data was found to be in databases within organizations, and over time, meta-directories become Identity Management solutions dealing with data and directory integration. Unlike other top-down provisioning applications, meta-directories allow for the consolidation of critical enterprise data into a centralized repository, establish and enforce business rules for updating this data, then distribute any changes back out to all applications and systems. Meta-directories operate in two ways: as top down and managed matrix. Figure 3.3 illustrates top down solutions.

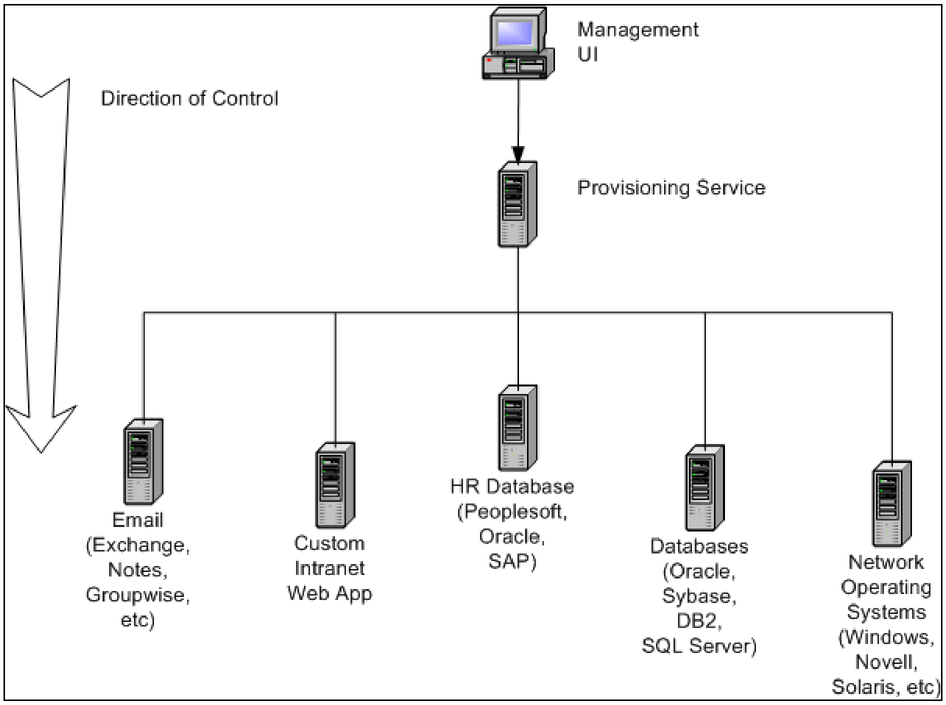
Management UI
Direction of Control
Provisioning Service
Email (Exchange, Notes, Groupwise, etc)
Custom Intranet Web App
HR Database (Peoplesoft, Oracle, SAP)
Databases (Oracle, Sybase, DB2, SQL Server)
Network Operating Systems (Windows, Novell, Solaris, etc)

Figure 3.3: Provisioning top down solutions.

Figure 3.4 illustrates managed matrix solutions.

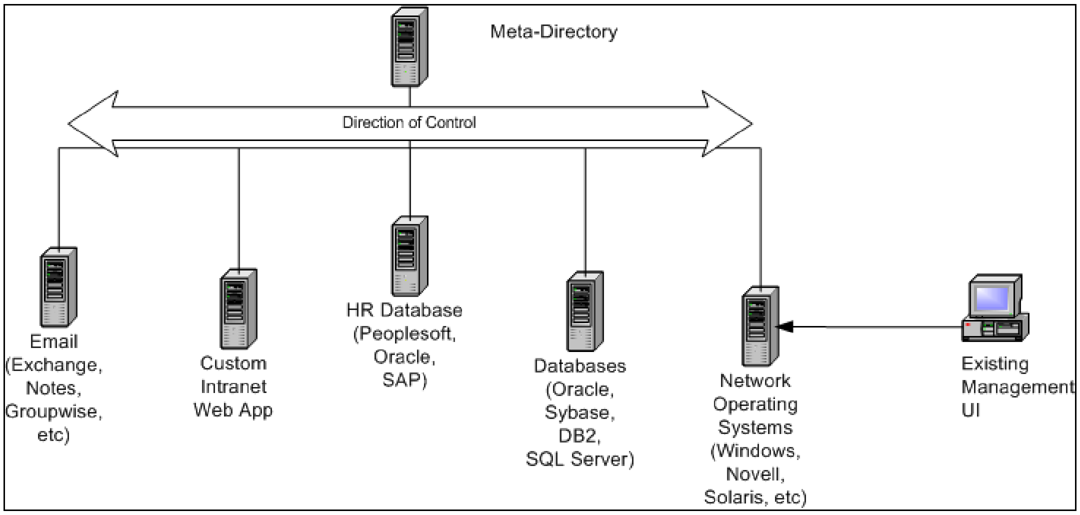
Meta-Directory
Direction of Control
Email (Exchange, Notes, Groupwise, etc)
Custom Intranet Web App
HR Database (Peoplesoft, Oracle, SAP)
Databases (Oracle, Sybase, DB2, SQL Server)
Network Operating Systems (Windows, Novell, Solaris, etc)
Existing Management UI

Figure 3.4: Meta-directory managed matrix solutions.

Sitting behind the scenes, meta-directories allow for the integration, and more important, standardization of processes and data, allowing you to maintain existing management products and procedures. Meta-directories can operate in a top-down fashion and support the requirements to manage disparate data from different parts of the business with minimal disruption. Because existing business rules can be defined in the meta-directory rules engine, then updated as the business migrates to new processes, meta-directory serves as a great solution when the top-down approach of many of the password management and provisioning solutions just does not work.

Smart Cards and Tokens

Hardware keys allow for less concern in the de-provisioning cycle, as they provide a physical and virtual connection with identity. By disabling the physical access capabilities provided by the hardware, you can stop access before the electronic access is required. Of course, this is not possible if the hardware solution provides access to a portable device, but this obstacle can be overcome by using devices that respond to wireless signals. We will discuss wireless options, including Radio Frequency ID (RFID), General Packet Radio Services (GPRS), and so forth, in Chapter 5.

In the case of authentication, tokens better support location-based authentication. One of the concerns around this type of technology is around what happens when such tokens are permanently or temporarily lost, stolen, misplaced, or otherwise. In most cases, the first activity is to disable the capabilities provided by the token.

Portals

Some industry analysts and vendors see the rise of the portal as the next point of convergence for Identity Management technology and more general application environments. Portal solutions require some form of identity and profile management capabilities to manage access, customized views based on roles, and personalization for end users. As a result, portal solutions provide their own profile management as well as interact in some way with other identity and security solutions—as noted in the previous discussion about SSO.

One logical set of progressions is that portal vendors will either partner with or become Identity Management vendors. When considering this tight integration path, be aware that vendors cannot remain on top of the Identity Management heap if they only support portal or Web access solutions. You need to consider the vendors that can solve this problem as well as manage identity and access across non-Web and legacy applications; otherwise, you simply introduce a schism in the management of your environment.

So if your company is implementing a portal strategy of any type, consider the implications of the portal vendor design carefully as there are potentially significant costs associated with ad-hoc deployments. If a portal insists on managing its own data or on a specific format of data in either directory or database, you essentially create another silo of data.

When considering a portal solution, like any other Identity Management component, consider that despite the intent of portals to embrace all other applications and services, there remains the distinct possibility that the integration points of portal vendors may not align with existing SSO, provisioning, or other Identity Management vendor solutions. Therefore, ensure that if you plan to use multiple vendors' products, they are compatible with your portal solution.

Summary

This chapter has reviewed the bulk of the Identity Management solution providers and analyzed the differences between their offerings. From this chapter, it is clear that there is consolidation of the various Identity Management component solutions into more robust and full-featured application suites. Although not fully there, there is a distinct shift toward single solutions, so consider your vendors carefully.

Chapter 4 deals with the process of proceeding to implement these solutions. The technology is evolving as well as consolidating. In past years, as the Identity Management market has evolved, perhaps the two greatest challenges facing the adoption of such technology were politics and education. Planning is essential both to succeed and deal with these issues, and that is what we will deal with in the next chapter.