

realtimepublishers.comtm

The Definitive Guidetm To

Identity Management



Archie Reed

Chapter 4: Implementing Identity Management	70
Planning—Where Do I Start?	70
Strategic and Business Justification.....	71
Return on Investment and Other Business Goals	73
The “Do-Nothing” Choice	74
Technical Goals	76
People, Policies, Processes, and Platform.....	77
Legal and Compliance Considerations	78
Core Infrastructure and Implementation.....	78
Interoperability.....	80
Requirements for Interoperability.....	80
Namespace Management	81
Maintaining Namespace Integrity.....	82
A Unique Identifier.....	83
Provisioning and Process Workflow.....	84
Setting Scope	85
Requirements Gathering	85
Buy vs. Build	85
Planning the Development Effort	86
Developing the Solution	87
Deploying the Solution	87
Sustaining the Solution	87
Account Management	88
Customer Service and Support.....	90
Physical Resource Management	92
Implementation Specifics.....	92
Implementation Scope	92
Team Composition.....	93
Migration and Interoperability	94
Pilots, Proof of Concepts, and Development Environments.....	95
Resiliency and Load Balancing	95
Training.....	95
Summary	96

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 4: Implementing Identity Management

Identity Management solutions have taken many guises as it has become a popular term, with many vendors claiming their solutions meet the criteria to be called such. Identity Management is a new and rapidly evolving market that has not achieved the level of maturity whereby we can say definitively what an Identity Management solution “must” contain in terms of functionality and services. Rather, as we have discussed in the previous chapters, the breakdown of Identity Management terms and components allows for flexibility, which in turn, makes implementations of Identity Management solutions unique to each organization.

Identity Management implementations have historically been undertaken as part of an organization’s security initiative or as a set of components built primarily on existing security infrastructure. However, although the implementation of Identity Management in an organization is strongly tied to security requirements, the strategic drivers should be, and are, at a higher level, tied to business requirements. The reality is that the security component is only a small part of Identity Management, and that much more process and technology lies beneath the surface. This chapter is about how you can go about implementing Identity Management in your organization.

Planning—Where Do I Start?

One of the most important aspects of any project is the methodology you employ to actually plan and implement a solution. For my own projects, I often use what’s known as the 4DS planning methodology, which Figure 4.1 illustrates.

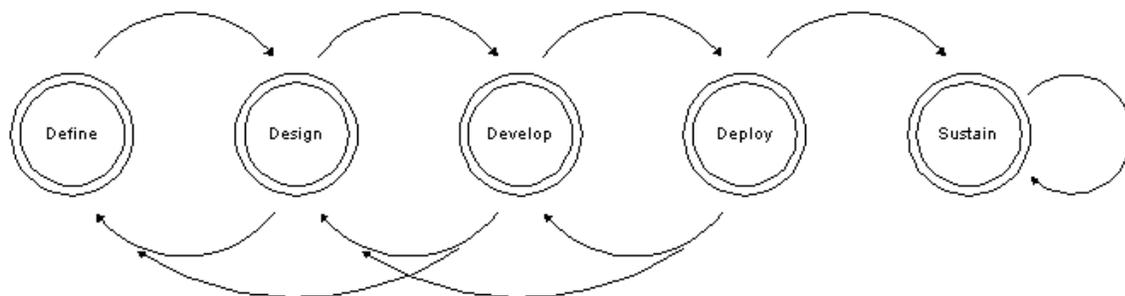


Figure 4.1: The 4DS project-planning methodology life cycle.

This book isn't designed to describe this particular methodology in great detail, and many organizations already have a methodology or even project management specialists. However, for the purposes of this discussion, the 4DS process provides a framework, so let's take a few moments now to discuss the basic steps and terminology associated with this concept so that we may refer back to it later in the book.

- **Define**—Determine the scope and deliverables that you want to provide and in what environment. Ensure that all must have, may have, and desired functionality is clearly defined and prioritized and that any expectations of vendor products is agreed upon and documented.
- **Design**—Set down the details of what you plan to deliver, then document and create a higher-level project plan.
- **Develop**—Create the code and identify the tools you need, and deliver a detailed project plan. At this stage, you should also be ready to pilot or run your project through a quality assurance (QA) or testing phase. This part of the process is essential—you must QA or test what you are developing throughout. Does it meet the needs you defined earlier? Does it match documented requirements, and do vendor solutions meet expectations? This testing also includes validating your delivery and deployment scenarios.
- **Deploy**—Deliver the solution according to your plan.
- **Sustain**—As with any product, you need a plan to sustain or maintain the product through its various life cycles, including new deployments or updates.

This standard progression and loop cycle is used by most project management methodologies. As with many projects, you might notice a loop effect as you go through the definition and design cycles. This effect is a result of the fact that as you learn more about what you plan to deploy, you might change your definition of what you plan to deploy. Thus, most of this book focuses on understanding the Identity Management solution space, and this chapter focuses on defining and designing your implementation project. Keep in mind that you can always step back should you realize that the project isn't going in the right direction or if new information comes to light that changes its perspective. As all good project management specialists and developers know, the costs of change increase the later you introduce those changes. Let's start to work on your reasons to justify Identity Management in your organization, and how you can begin planning.

Strategic and Business Justification

This section is about identifying the pain points in your organization, then identifying the parts of the Identity Management bundle that can minimize the pain. Finally, we'll explore how to provide a strategic and business justification for the implementation relating to those discoveries.

 Many Identity Management deployments flounder or fail because the business need has not been clearly enough defined such that there is executive ownership. In addition, there is commonly not enough staff that are experienced with the product, and potentially too much complexity to make the deployment successful. Before you can successfully deploy an Identity Management solution, you must identify and mitigate these issues.

Support for an Identity Management initiative may contend with the need for immediate delivery of new and focused services. The reason is that it is often difficult for organizations to move beyond tactical requirements of specific organizational units.

It is also the role of the business to support the development of this service according to standards, such that there are no cross-departmental issues that could cause it to fail at any point. There are many factors that can influence those views, primarily around the ways in which budgets are deployed, including geographical, commercial, functional, divisional, discretionary, and emergency. Using these demarcation points, you can identify stakeholders for your discussion and the related pain points that result from disconnects between them.

There are serious consequences to a business that refuses to support such a cross-organizational initiative. For example, one of the key initiatives that many organizations continue to work on is SSO, which we have discussed previously. SSO is essentially the ability for a user to be authenticated once using a name and password or some other means, and given that authentication, be able to access all of the corporate resources such as applications, data, and network resources, without having to authenticate again in any given session. Over the past few years, this solution has seen a shift in its required functionality from internal access to organizational resources, Web-based or otherwise, to the need to support such access from an intranet, extranet, and the Internet. To be successful, this type of solution mandates the requirement for the organization to work together, specifically all of the application “owners” of internally and externally facing solutions in order to create something that is integrated and valuable.

Of course, the reality of SSO is that it is complex. However, it is this type of technology that makes Identity Management components such as directory services such a compelling solution, as many of the SSO solutions available today require some form of directory-based management to be put into place.

In addition, management of SSO access controls requires a flexible and extensible model that can allow an organization to manage not only who has access across systems, but also who has granular controls around which components are accessible, when they are accessible, and so forth. This model is usually referred to as policy management. Most Identity Management solutions are moving toward this model to manage resources, including SSO, as well as provisioning, administration, and so forth.

So the important thing to remember is that with all these components using policy-based concepts, it is vital to ensure that you either consolidate those policy concepts or ensure consistency across any implementations. At this point, you will face a decision as to whether you will implement best-of-breed technology or a consolidated solution. These solutions are designed to integrate with other application services, but not necessarily each other. While there is ongoing consolidation in the industry, standards will allow these solutions to interoperate to some degree (we will discuss this development in detail in Chapter 5). Beyond that, tools such meta-directories allow the management and movement of data between such Identity Management solutions as well as the applications under management.

☞ Identity Management solutions are complex deployments requiring involvement from many parts of the organization and careful identification and management of organizational issues. Despite the upfront costs, you must examine the capabilities of your in-house staff carefully. To mitigate these issues, you might seek the assistance of experienced Identity Management service organizations to lessen the impact of unplanned-for issues. Chapter 6 will provide a list of resources including such service organizations.

Thus, Identity Management *must* be driven by business needs. Unfortunately, there is no one single approach to an Identity Management implementation. The unique and specific requirements and priorities of an Identity Management solution for each organization negate such a possibility. So all organizations will need to identify the commonality of the solutions presented here that apply to them, and implement the customizations they require. We have discussed a number of goals throughout the previous chapters, and the following list provides some common business projects or goals that you can use to improve the effectiveness of an Identity Management project proposal:

- Regulatory and compliance pressure around management of employee and customer data, in particular personal or private information.
- Mitigate consumer concerns about misuse of personal and confidential information
- Liability for lack of due care in the protection of personal information
- Need to improve “hire and fire processes”—improve speed, accuracy, and cost structure
- Support access to business solutions regardless of location and type of end user (for example, customer, supplier, employee)
- Decrease costs by allowing self-service of information
- Decrease management overhead and costs
- Decrease development costs
- Reduce the risk of incorrect information being used for business processes

Return on Investment and Other Business Goals

Unless senior management has identified Identity Management as a critical requirement, there is a need to present some form of justification for the investment. Commonly, this justification takes the form of a write-up along with a ROI calculation. A ROI shows the costs or impact of specific projects and focuses on driving to specific numbers to show decreases in costs or quantifiable increases in productivity.

The goals of an organization generally focus on maintaining the status quo unless there are guaranteed, and sometimes significant, returns of at least some of the following:

- Minimizing the cost of the infrastructure
- Minimizing the cost of supporting the infrastructure
- Improving employee productivity
- Increasing the business functionality of existing systems
- Creating competitive advantage
- Increasing customer or partner satisfaction
- Increasing sales
- A new initiative or partner program

As we have discussed, Identity Management is comprised of several functional components that can be implemented singly or as a complete Identity Management initiative. At this stage in the Identity Management life cycle, most organizations find that justification and implementation is easier if they concentrate on specific solutions rather than a general one.

The “Do-Nothing” Choice

One of the challenges faced by this type of project that can have a significant affect on an organization is what is called the “do-nothing” choice. An organization can choose to ignore the potential advantages and cost-effectiveness of Identity Management solutions or to embrace them. As such, there are two primary directions that an organization can take at any point in time. Pay now or pay later. This concept is a simple one that can be emphasized through a graphical representation, such as the one that Figure 4.2 shows.

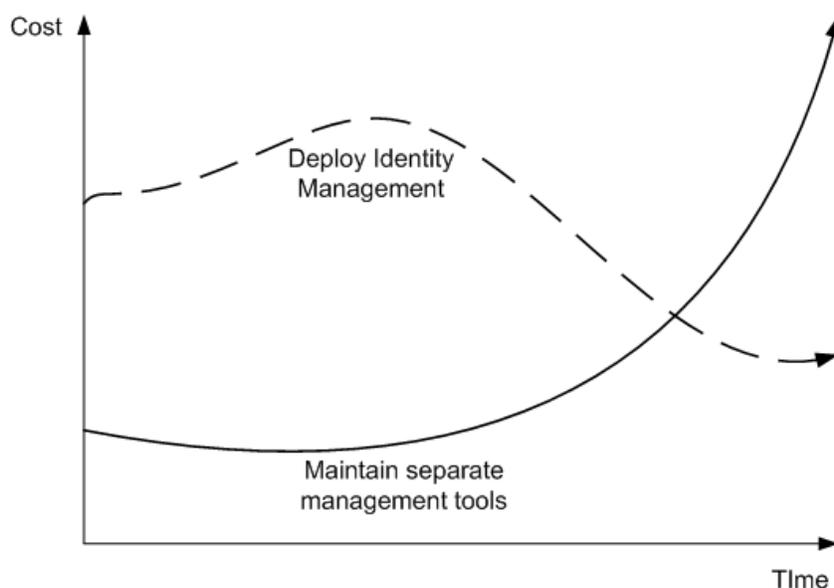


Figure 4.2: An illustration of the Impact of deployment costs over time.

The graph in Figure 4.2 provides a pictorial representation of the costs associated with a decision to implement Identity Management solutions or not, and can help encourage a decision.

Obviously, there is more up-front cost to begin these projects (indeed any broad projects), and the cost benefits are only seen later. This demonstrates a fishtail effect. However, unlikely it may seem, it is possible that over time the costs of an Identity Management system may increase. The point of the minor up-tick in the graph for Deploy Identity Management option is to reinforce the need to review and re-examine your deployment over time, as recommended at the beginning of the chapter around project management concepts, and ensure that you have the optimal solution in place.

Choosing not to implement an Identity Management strategy, the costs over time will increase with each application or service your organization might deploy. Costs are incurred with each new creation of data, the costs of either maintaining synchronization processes or managing the data independently of other systems, and finally, the unseen costs that are produced as a result of the data being inconsistent with other related corporate data, over time. Also, over time the costs of maintaining and managing older, legacy or heritage systems increases. The reason is that over time the systems routinely become more out of step with processes and data, as new solutions are introduced, and as such, the time spent in the care and feeding of each solution increases.

Certainly the *raison d'être* for this book is to introduce and even justify Identity Management to organizations; however, the “no choice” option introduces a potential counterpoint. It could be argued that the assumption that Identity Management is an eventuality for every organization is incorrect. Is it possible that some organizations are more efficient and cost effective with their current tools? In some cases the answer to this question may be yes. Is an Identity Management solution important for every organization? In some cases the answer to this question may be no.

In the research paper “Social Analyses of Computing: Theoretical Perspectives in Recent Empirical Research,” Rob Kling discusses some of these issues. In particular, he addresses the various perspectives that can influence individual and organizational views of technology. One important point that is brought out is that those who support certain goals for an organization (such as employing a new technology solution) often incorrectly assume that everyone has the same goals and motivation. This being the case, it might seem a bit closed-minded to assume that an Identity Management solution is a universal necessity among organizations; however, by now, you should have some very clear and concise reasons to deploy an Identity Management solution in your organization.

Technical Goals

Secondary to the business goals of implementing Identity Management are the technical goals. Where the business and technical goals intersect are your best bets for gaining support for this new deployment (that is, you must align your technical goals with your business goals). The following list provides key technical goals and requirements:

- **Security**—Many organizations believe they have a security solution in place, yet they often do not implement a complete solution, or worse still, fail to keep up to date with the latest security tools and mechanisms. However, most organizations are looking for ways to increase their security and understand that security is a rapidly evolving area in which an organization must be concerned about protecting not only its data and resources but also its reputation. Identity Management solutions can provide many mechanisms to help ensure that security settings are maintained across the network. Involve the security team and discuss whether the existing services are secure enough. Also, consider using the Identity Management project as the reason to perform a security audit on your network and resources to determine whether you need to change your existing security policy or, as some companies might find, more than one set of policies. Identity Management can help mitigate the following key areas within the security realm:
 - Physical and system/service access
 - Data theft
 - Data encryption
 - Transaction fraud
- **Manageability**—Organizations will want to minimize the number of administrators required to perform a specific task and the associated costs. Maximizing resource usage and minimizing resource costs are always important to any organization.
- **Availability**—Most organizations will want to ensure that their network services are available whenever the business requires them. Availability should also be a goal of your Identity Management project so that the current environment is disrupted as little as possible. This step includes maintaining the required access controls and other security settings.
- **Scalability**—Ensuring that a solution can scale to meet the needs of a whole organization requires that the big picture be defined upfront. Two levels must be considered for such a deployment: What is the scope of internal accounts and resources that require Identity Management? and similarly, What, if any, is the scope of external accounts and resources?
- **Integration**—When reviewing Identity Management applications, there are two important mechanisms to consider:
 - What systems can the Identity Management solution manage today?
 - What happens if a new system is introduced or the Identity Management solution does not have an immediate connection to a system? How easy is it to add the ability to manage a new system?

Table 4.1 shows the general focus of the goals of an Identity Management project.

Goal	Implications for the Identity Management Implementation
Security	The project must improve or have a minimal impact on security policy; perform a risk assessment to identify any potential threats and take the appropriate countermeasures
Minimum disruption to the production environment	If possible, maintain users' familiar environment during and after the implementation; at least, provide for ease of use through common interfaces
No degradation of system performance	Maintain or improve expected performance
Minimum administrative overhead	User accounts should be seamlessly migrated; if possible, users should be able to retain their passwords; administrators should visit client computers only a minimum number of times; new permissions for resources should require minimal setup
Maximize "Quick Wins"	The enterprise should obtain access to key features of the new platform as soon as possible

Table 4.1: Goals for and implications of an Identity Management project.

People, Policies, Processes, and Platform

The implementation of Identity Management into any organization must be preceded by a close look at the organizational processes that surround the actual applications, resources, and services for which you want to manage identity. Over the past few years, the term *business process re-engineering* (BPR) has gained some notoriety and, dependent on the organization, can have good or bad connotations. The obvious goal is to minimize negative or costly impact to your organization, but to truly make use of any new system or service requires some change. Regardless of whether you use BPR or some other term, the requirement of change exists.

In addition, there is no reason to introduce an Identity Management solution if there is no intention to actually use the service. An Identity Management solution cannot and will not solve your identity problems simply because you implement it. The case of "build it and they will come" has never been much of a truism in business. You must invest time into reviewing how it will operate within your environment, what parts will be impacted, and what processes require change.

Consider the following list as key areas to review when considering an Identity Management project. As vital to many projects as they are, an Identity Management project requires as much, if not more, investigation in all of these areas:

- **People**—People are the most important part of the equation. Whatever you are trying to do in your project, you will be dealing with many different people.
- **Policy**—Policies define how the organization believes it should operate. They are high level, and should be created based on the needs of the business. In some cases, a policy might even be defined and enforced by an entity outside your organization. Additional examples would be the Department of Trade and Industry (DTI) regulations for business in the UK, the Securities and Exchange Commission (SEC) regulations around US financial services companies, and the Federal Communications Commission (FCC) regulations around US companies such as radio and television broadcasters. In any of these cases, your organization is required to meet some form or level of compliance with those regulations.
- **Processes**—Processes define the way that an organization will enact policies. Policies define general entry and exit criteria from the process, and the various high-level steps required to enable that process. These steps might include some form of exception rules and handling. Related are procedures, which would possibly add too many P's to this discussion. Procedures are given to an individual, team, or workgroup that will need to perform actions to complete the processes and enact policies. These actions are generally in the form of a very specific task list.
- **Platforms**—Platforms are the systems and services that the rest reside on and use to fulfill the needs of the business. Hardware, software, and middleware make up this part of the equation.

Legal and Compliance Considerations

As we've discussed throughout Chapters 1 and 2, legal issues can drive a successful Identity Management implementation. Without care however, legal and compliance requirements can create significant roadblocks.

Core Infrastructure and Implementation

Aside from the functional components of an Identity Management solution, the essential component of any Identity Management solution is an understanding of the identity store. Arguably a directory (X.500 and LDAP) is the most widely accepted store of identity information, however, databases are also often used. The key is to acknowledge that the store, whatever it is, needs to be populated with accurate information and the Identity Management solution should not only manage that going forward, but also be able to solve the life cycle management around that identity data.

Common data in the identity store might include profile information such as names, passwords, preferences, groups, access rights, access policies, and so forth. Importantly, the identity store does not only deal with what we might consider user data, but also must store information of system resources and applications to relate security models between them and provide context for a common security model, as Figure 4.3 shows.

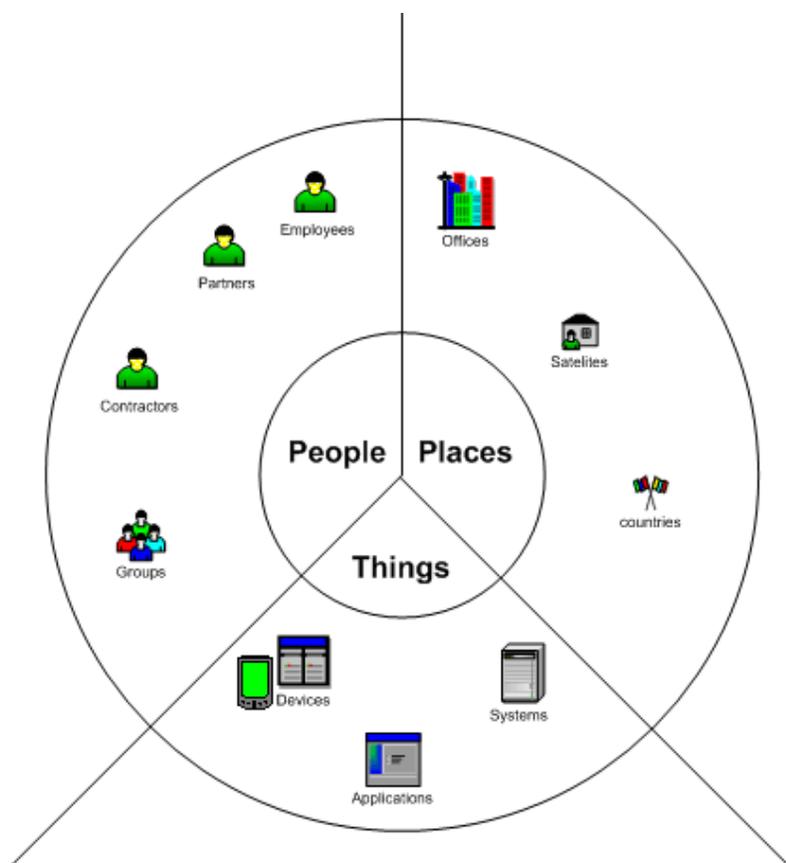


Figure 4.3: Systems, services, and data in the Identity Management solution.

When reviewing the core infrastructure of your Identity Management solution, review carefully how the system manages changes in the applications it manages. Meta-directory solutions have extensive connector solutions for dealing with this type situation, and new application solutions provide numerous connections out of the box with similar abilities to create customized connections when required. As noted earlier, the primary difference is whether your requirements lead you to a top-down, controlled solution favored by the applications but doable with all solutions, or a cross-application back-end solution supported more by meta-directory-like solutions.

 Refer back to Figures 2.1 and 2.2 in Chapter 2 to refresh the Identity Management concepts in your mind.

The identity store also needs to be able to draw identity information from a variety of systems: human resources and accounting applications, email directories, and Web server registration databases. This encompasses more than just being able to read identity information from other systems, including the ability to identify the changes that occur in these other systems. For this reason, the identity store must be closely coupled with interoperability services to achieve this goal. An Identity Management solution can bind identity data to the organization of information that is located in an organization's multitude of directories, databases, and other data repositories.

Interoperability

This part of the book will discuss the interoperability between the various Identity Management solutions and applications that you might need to deploy. In many cases, a vendor will actually utilize an existing or third-party directory for the storage of Identity Management information. However, managing such a solution can be difficult.

Requirements for Interoperability

One of the most common issues raised today is the level to which you can make various software solutions work together—share information and functionality between them to enhance your business. This functionality is one of the goals of an Identity Management solution; however, traditionally, vendors have worked to make their solutions your choice and have created integration solutions (products that include account management, data management, and security functionality) only when it is in their best interests.

Consider how this situation has evolved through Microsoft's Windows NT and Novell's NDS. Both provide security models, identity data management, and access control. Both companies have created capabilities to support migration from other solutions and interoperability if that is not possible. An example of interoperability is Novell with NDS for NT. Hybrids of these capabilities are also seen in products such as HP OpenView, Computer Associates' Unicenter, and IBM's Tivoli. These large suites of system and network management products utilize the underlying products as a source and a basis for their solutions, whilst at the same time providing integrated solutions that extend their capabilities and potential for sales.

So, what does all this mean? The existence of the solutions and even directories as identity stores only go so far in solving the problem of sharing data but not necessarily policy—remembering of course that a directory is not there to store all information and more important, enforce policies. Standard protocols do us no good if vendors do not choose to use them, but the standards do offer one part of the interoperability puzzle.

Let's turn our attention to the other requirements for interoperability, and how in many cases, there are still large gaps between those requirements and the reality of the market. There are essentially three layers that you need to consider for interoperability:

1. Management interface
2. Data definition and access
3. Information storage

Because it is likely that there will not be an immediate solution in all cases, you should review meta-directory approaches to allow you to consolidate data from various sources to provide a common definition across these layers. In effect, the data definition and access layer is the key.

One of the advantages of gaining standards-compliant software is that if there is a problem with interoperability, you have an immediate recourse and formal reference to use when dealing with vendors. True, as much as vendors might disagree with me, they often disagree with each other, finger point or outright blame the other side; however, standards keep us at least one step from having a completely proprietary set of solutions trying to interoperate. Of course, one of the key aspects of an Identity Management solution that needs to interact with and manage identities in disparate systems is to be able to deal with proprietary interfaces. Meta-directories have had this capability for some time; however, most Identity Management solutions now offer pre-written interfaces for standards-based and common proprietary applications and services. This functionality is supplemented through the ability to create connections through connector frameworks or adaptors.

Given that such is not the reality of the market, the solution that we have already reviewed at this time is the meta-directory option. Remember that while many vendors offer what they call a meta-directory solution, there will likely be differences across the level of functionality that they really provide relative to the definition given. In some cases, there will be extended functionality that will be useful to you that is not part of the definition. You can look to our definition of meta-directories in Chapter 3, but the reality is that meta-directory forms just part of the solution.

Namespace Management

Naming is a very difficult problem to understand and manage. Defining your naming strategy is one of those critical pieces of the project that is often left until the last minute in planning. After you start a naming standard it is very difficult to change, and an incorrect analysis of your situation can be disastrous. Let's consider in more detail what we really mean when we talk about namespace management.

When we talk about names and namespace management, there are several key distinctions that need to be made, and terminology that needs to be agreed upon. Naming a person in Identity Management products can have a number of different phases and definitions. It often consists of filling out fields such as first name, last name, initials, common name information, preferred display names, logon names, and email address(s). Providing a common and accepted naming standard is important within a corporation because it allows people to search for colleagues in a consistent fashion. However, simply choosing an approach, including components such as first name and last names, can run into problems in many situations, for example:

- People from different cultural backgrounds have different naming conventions
- People changing their name legally to a single identifier (does not fit the first name/last name mold)
- People with a single character first name or an identifier such as "Junior"

Sensitivity is needed when defining a standard to ensure that the standard works well but does not cause concern or embarrassment or introduce potential cultural conflicts. Self-registration sites on the Internet most often allow you to choose your own account name, but still usually prompt you for name components in order to register and display your name (with your permission) in a global address book of some form. Yahoo and Hotmail are examples of these kinds of sites. Having a user-chosen logon name and email address allows users to have some form of control over how their identity is registered and seen by others. This is a good example of self-service.

However, this setup does have its limitations, particularly in large user communities such as Yahoo and Hotmail. Logon names and email addresses constructed from known information (for example, first initial, last name, and some random or qualified iteration such as *flast2003*) are usually not particularly helpful when trying to search for someone. In addition, first names and last names are usually insufficient to *uniquely identify* you to others, and placing other personal information that would perhaps provide sufficient identity information could lead to privacy issues.

We are all known by our names in some form, even nicknames. Even use of digital certificates and biometrics map back to us as individuals that need to be searched for and contacted based on information relating to our names. Hence, within an Identity Management system, there is no way of getting away from developing a standard that caters to name clashes and different naming conventions. Generally, the best approach is to define a naming standard that meets the needs of the majority of your Identity community and be flexible enough allow a mechanism for sensitively handling exceptions to the norm. In large communities and in cultures in which name clashes are common, allowing people to register their common names without modifying them can make it difficult to contact the correct person. This makes it doubly important to ensure that your Identity Management solution incorporates other information that enables the correct person to be contacted. This information could include organization, office, job role, or phone number in the case of a corporation and street and home location in the case of larger “private” communities (assuming privacy concerns have been addressed).

Maintaining Namespace Integrity

Namespace management is not just about uniqueness or identifying a person in a single repository. It is also about maintaining names in disparate databases or directories. One account management system might have an 8-character limitation, whereas another may allow any number of characters. Some might enforce different naming standards (for example, *first last* vs. *last, first*). Also, names can and do change—people get married (and divorced) or simply legally change their names. Identity Management systems need to come up with a method for matching and maintaining users between systems and also enforcing naming standards.

Meta-directory and provisioning solutions can help to maintain integrity across disparate sources. However, implementing them can be difficult because each of the systems may have been managed separately for some time with varying levels of control. Some databases or directories may still have records relating to users that have left the company more than a year ago; others may be more up to date. Matching names and removing old entries is required prior to integrating automated account management solutions. This difficult and often time-consuming task is often affectionately referred to as *data scrubbing*.

Once the systems have been integrated (not a trivial task by any means), maintaining the integrity of the links can be quite difficult. Provisioning solutions usually record the account name from each system in a central repository (database or directory) that is used solely by the provisioning product. There is a record that identifies the users and all of their connected accounts. They then rely on any changes to account details in any of the connected systems being implemented using the provisioning system (admin interface or feed from an external source).

 Although many of the provisioning products have implemented some form of detection mechanisms, they still struggle to cope with changes to account ID and name fields that are carried out using the native tools.

Meta-directory products also usually have some form of central meta-directory database to maintain the mappings between disparate systems. The difference is that they are developed specifically to cater for changes in remote systems. However, problems can still occur if the key they are using to map users between systems (often an account name or email address—both usually based on a user's name) is changed. Directories and databases supporting change logs and notifications can be handled a little more smoothly, but other connected systems or flat file exchanges will usually break if certain name changes take place.

A Unique Identifier

An underlying unique identifier helps to keep track of an individual's identity if that individual's name (or account) changes. In fact, everything about an individual can change (except the unique identifier) and referential integrity between systems is maintained. This setup allows management of name spaces and enforcement of naming conventions to be managed in an automated fashion using products such as meta-directory and provisioning tools across a company or series of interconnected systems.

 Usually the best way to resolve the problem of mapping namespaces between disparate systems is to have some form of underlying unique identifier associated with an individual that is not tied to any one system. This identifier then becomes a "foreign key" between disparate systems that should "never" change, thus allowing consistent namespace management.

Unique identifiers aren't perfect. Local administrators could still accidentally (or knowingly) change or remove the unique identifier field from a person's record and break the link. Also, some form of system and process needs to be put in place to create, maintain, and allocate the unique identifier. Social Security numbers (SSNs) are sometimes seen as a quick and logical solution for unique identifiers. However, privacy concerns exist with this approach, as the SSN is recorded in all systems and passed across the network regularly. In addition, if a company operates outside the U.S., this solution becomes unworkable.

Various approaches could be used to overcome this issue. Usually the best is to place the creation and allocation of the unique identifier under the control of human resources and make it an integral part of the hire and fire processes. If they need to ask for personal information to establish the employee (or contractor's) identity, this setup may be more acceptable to all involved. The ID would then be written into every new user's record in connected systems using some form of provisioning process and the namespace (as well as other attributes) maintained using meta-directory processes. Removal of all accounts associated with an individual can take place quickly, and reporting and control of accounts across a company becomes much easier. Figure 4.4 helps to highlight how this kind of system might work.

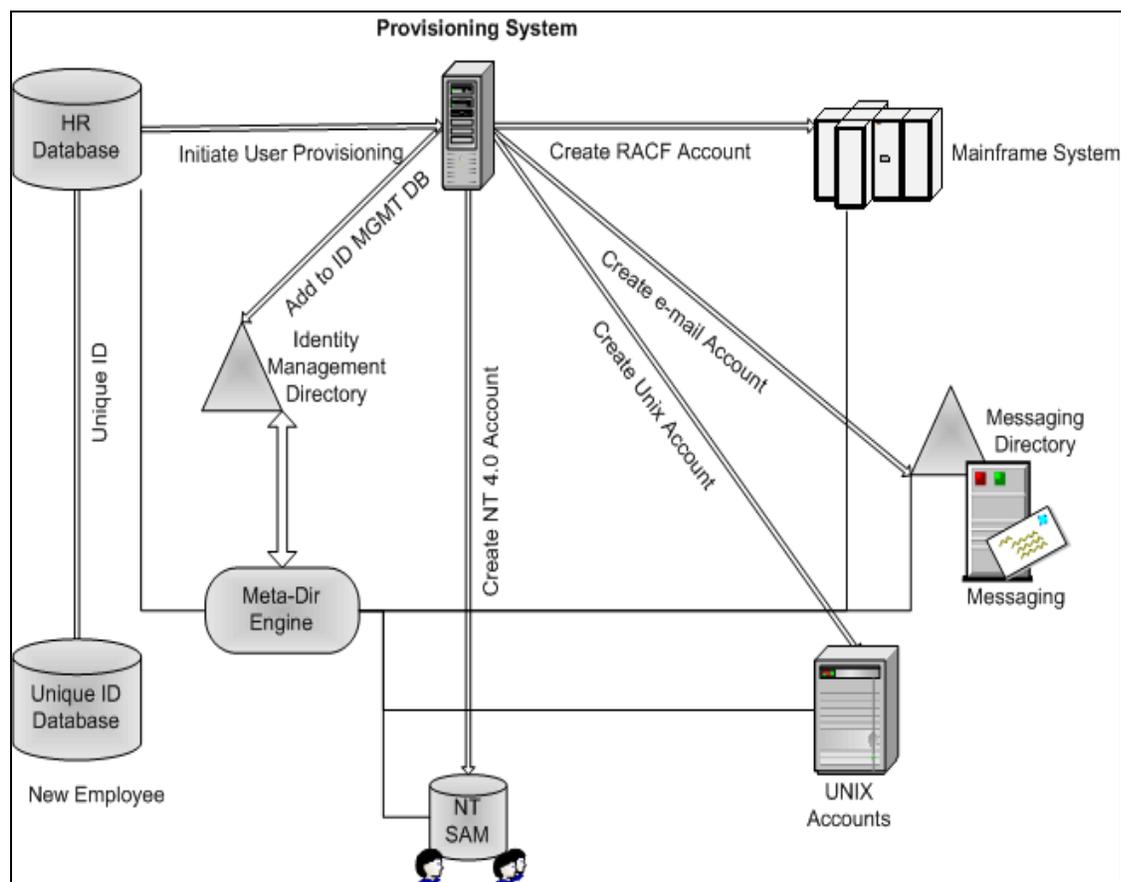


Figure 4.4: Identity namespace processing illustration.

Provisioning and Process Workflow

Provisioning solutions have the potential to form the backbone of an Identity Management system, so approaching this task with careful planning is vital. In addition, planning and deploying a provisioning solution should be undertaken as an overall Identity Management strategy. Planning just provisioning without thinking about account management, meta-directory, and role-based access control requirements could lead to inconsistent representation of user data and role definitions.

There are a large number of corporate problems that can be “solved” by provisioning solutions and workflow process changes. These range from the traditional hire/fire scenarios and enforcing naming standards to controlling role-based access to resources, provisioning accounts across every known system in the company, and integrating purchasing of hardware and allocation of office space. In addition, as mentioned in Chapter 3, many of the provisioning products encroach on the account and password management fields as well as provide meta-directory functionality. Hence, you could quite conceivably use a provisioning vendor to solve a large portion of your Identity Management needs.

Setting Scope

It is vital as part of the define phase (discussed earlier in the 4DS section) to set the scope of the project very carefully with any provisioning implementation. Without the correct backing and appropriate setting of scope, the whole process could lead to failure and recriminations.

The key is to set a roadmap for addressing many of the issues that are causing pain within your company. However, don't be afraid to set the scope to a subset of these areas to ensure success. Early success, even on a small scale, can inspire confidence and garner support for the more challenging tasks. Highlight the more difficult provisioning tasks as areas that can be addressed, but list them in an additional follow-on phase.

Requirements Gathering

As mentioned earlier in this chapter, identifying the business and technical requirements are vital to any successful Identity Management solution. It is also a difficult task because many parts of the organization hold a key to the puzzle. To make it more difficult, the different sections may have conflicting requirements. For example, the IT department might want to store and use sensitive pieces of information such as SSNs to make it easy to uniquely identify users across systems. However, Human Resources will most likely consider this action inappropriate. Balancing these conflicting requirements is a very important part of the process. Some of the groups that have a major stake in a requirements gathering process for provisioning include Human Resources, Security, and IT Account Administration. Be prepared to look at existing account management procedures and automated scripts as they often implement the business rules that may exist within a company. You might need to search hard to find good definitions of roles and resources required by people carrying out different work functions.

 Care must be taken when examining existing processes and scripts as they could be implementing incorrect business rules or taking short cuts that have the potential to cause security problems. Take for example the fairly common practice when creating accounts of *cloning* an existing account within the department the user is joining. Doing so ensures that the user has access to the appropriate resources. However, it is often done because there are no clearly documented user rights and roles required for a particular job category or function—something that needs to be defined before a provisioning solution can be deployed. Also, the person being cloned might have carried out several different job functions in the course of their tenure with the company and still be a member of privileged groups, thus granting a higher level of privilege to the new user than is necessary.

Buy vs. Build

Chapter 3 highlighted the overlap between “pure” provisioning solutions, meta-directory solutions, and account management and user self management. This overlap means that choosing a particular product or approach could strongly dictate the way in which other components of an Identity Management system are developed and deployed.

 Because of the complex nature of provisioning solutions, it is generally not as simple as buy vs. build—it is more like buy and build vs. build and build. All off-the-shelf products require extensive customization and often development.

Many companies have developed some form of in-house provisioning solution that may enforce some of the business rules for creating and managing accounts. These are often Web-based administration tools used by administration teams to either tie together account creation processes, create some form of primitive delegated administration, or enforce naming conventions. Continuing to enhance these products could be a viable solution, particularly if they are coupled with a meta-directory product to help tie this front-end process to other internal systems. It may not necessarily be a traditional meta-directory approach that looks to synchronize disparate directories directly. Other solutions utilize a *message bus* architecture to transfer data and changes between different systems.

On the downside, building either from scratch or by enhancing existing in-house tools can be fraught with danger. The in-house tools could be a mix of old technologies and platforms, poorly documented and understood scripts, coupled with the occasional manual intervention. It might make more sense to replace the entire mix with something designed specifically to carry out this task.

Mapping Out the Workflow

Provisioning solutions involve a series of inputs and workflow rules. A single request to add a user can be routed through multiple paths, some of which may involve a manual work request. Think of provisioning as a series of business workflows; doing so can often help when mapping business requirements into programmable business rules. In fact, there are various commercial products and tools in the BPR space that might help to bring visual clarity to the planning process.



Providing a provisioning system can be seen as implementing BPR. In fact, stating it in these terms can often help garner support from senior management.

Choosing a Product

Chapter 3 listed a series of available products as well as some of their strengths and weaknesses. Using some of the information listed there may help you in choosing the appropriate product if you choose to buy. The key point to remember, though, is that this decision is not simply which product is best of breed. You need to examine your existing infrastructure, strategic relationships, workflow processes, applications, and requirements. If you have engaged a services organization to help you with an overall Identity Management strategy, it is possible that they may have a preference for a particular product. Care must be taken here as they may have a relationship with some of the vendors, and this relationship could color their viewpoint. However, if the products they propose meet all your requirements, then choosing a product they have experience with may be a positive approach.

Planning the Development Effort

If you have carried out requirements gathering and other planning processes carefully, you should have a good idea of what is required in the development area. It can often seem a little overwhelming when the sheer enormity of the tasks involved is clearly highlighted. Thus, it is important to set the scope in a realistic fashion early on. Enormity of work aside, it is important to ensure that a project manager helps to mould the development effort carefully as it could involve in-house developers and external contractors and consultants.

Services organizations can often be very helpful in this area as they may have been through this several times before and have a good idea of what is involved. If most of the work is being carried out predominantly by an external services company, ensure that in-house staff is targeted to oversee development and configuration of the system. If you plan to deliver and manage the system, training for the vendor product may also be necessary.

Developing the Solution

The development can be a hectic and furious process. Even though provisioning has been around for a few years, the products are still fairly immature. In addition, all companies have different business rules and workflow processes. These can be very difficult to implement using products out of the box. Often external processes or scripts need to be written or formal policy developed for interactions with the system. It is not uncommon for feature enhancements (including connectors, bug fixes, or custom development) to be provided by the provisioning vendor to support a given solution.

It is very important during this process that the development plan has regular checkpoints built in where the business rules being coded are validated with stakeholders. It is not uncommon for workflow processes being mapped to change before the solution has been deployed or incorrect requirements have been documented. Regular sanity checks help to avoid problems right at the end of the development cycle.

Deploying the Solution

Deployment is a particularly tricky part of the project life cycle. The provisioning solution, as highlighted earlier, has the potential to replace major components of a company's processes. Implement the solution in incremental stages and/or running the two systems in parallel can help mitigate risk. A pilot implementation using a subset of users is often a good plan as well. However, staged implementations or pilots can be a tricky proposition if existing in-house processes are held together with duct tape, so to speak. It may actually be safer to deploy the new system in one big deployment. Doing so will require a large amount of coordination between all parties in order to be a success. Ensure that you have a back-out plan as well that enables a fairly seamless rollback to the existing system (even if it is a straight manual process).

Sustaining the Solution

As soon as you have successfully deployed the provisioning solution (whether you have built it yourself or deployed a packaged solution), you will receive requests for changes. Ensure that you have planned post-implementation reviews and development tasks to meet immediate problem needs. Budgeting this need into the delivery costs is usually a good idea. Also, business rules change and enhancements will be requested. If you have not involved and trained internal staff to take over after any external consultants have delivered the solution, you will be calling on their services quite regularly (for a cost of course).

 If you don't factor maintenance and enhancement costs into your provisioning project, you run the risk of the system failing soon after deployment or of providing only partial functionality. Business processes are subject to regular change and you have to be able to evolve your provisioning solution to meet these changing needs.

Account Management

Account management covers many aspects of Identity Management and, some may argue, is a description of Identity Management itself. Although this idea might be true in its simplest form, previous chapters have highlighted the breadth of technologies and processes that constitute Identity Management. That is not to say there aren't major overlaps between components and technologies. Provisioning solutions overlap with meta-directory solutions, and both perform aspects of account management. This overlap is what makes deploying an Identity Management solution so challenging—finding the best mix of products and processes that meet your business requirements.

As mentioned previously, account management can't be looked at in isolation and needs to be part of an overall Identity Management solution. It may be sufficient, for example, to use the features of a planned provisioning product to meet your account management needs. As highlighted in Chapter 3, many of the provisioning vendors provide components such as password resets tools, user self management, user self registration as well as interfaces for administrators to manually make changes to accounts. However, often it is necessary to combine these kinds of tools with password synchronization and meta-directory solutions.

Aside from the implementation specifics, some thought needs to be put into what kind of account management is required and why. One of the key benefits that a good Identity Management solution can provide you with is the ability to track the digital profile of a person throughout the person's time with the company. To what level does there need to be consistent tracking and reporting?

There are various solutions available to meet your account management needs but, as discussed elsewhere in this chapter, you need to have the business drivers dictate the “depth” of your solution. It may be sufficient to only track a small number of accounts, and then, only the accounts and not the types of authorization these accounts have. However, increasingly, the requirements for account management have begun to dictate a much more stringent knowledge and tracking of accounts. This is often referred to as account life cycle management or “cradle-to-grave” knowledge of an employee's accounts and authorities.

You might need to solve questions about where best to store and how to track account-access information at a particular point in time. Generally, this capability is best left to the native applications and their auditing tools. However, if tracking of account authorization is not available, a repository that stores this kind of information may need to be established and linked to the identity store and the native account databases.

Apart from tracking system accounts, other pieces of information may need to be stored for industry compliance and legal reasons. Within the financial industry, for example, there may be a requirement to know information about an employee that goes beyond the common accounts such as OS, email, and mainframe. They may need to know information such as which training courses an employee attended in order to identify liability in the case of legal action. This drives a requirement that records in a training system be matched up with an employees' identity profile. You need to ask questions about whether you store information about the external source (training in this instance) in the identity store or provide some mechanism to link and then retrieve the data.

Keeping things separate is usually advisable. A unique identifier, as mentioned earlier in this chapter when referring to namespace management, can greatly help in this task as well. A unique identifier lets you use tools such as virtual directories to transparently access the data and present it as if it was present in the identity store, or to simply run a manual report that merges data from the identity store when required.

There are still some major obstacles to overcome in this area, though. How do you reconcile users who have left the company? They may still be in the training system but not in the identity store. How do you manage employees who leave the company and return at a later date? If you are relying on a unique identifier as the key to all your systems, if the employee receives a new one when they return, you end up with orphaned records. Keeping some form of archive or database of identity information can be useful to resolve both of these issues.

One of the biggest challenges is identifying the returning employee and re-activating their identity profile. An option is to use the Human Resources or payroll system to help track users after they have left. Most companies keep a record of every employee that has been with the company and simply mark them as inactive. If the unique identifier is stored with their employee records, it can be re-used in the identity store if an employee returns or can be used to map back into other databases at any stage on an ad hoc basis. Remember, no system is perfect and you can never guarantee 100% that a returning employee is matched back to his or her original record (someone may mistype an SSN, for example) and this needs to be highlighted to management. Also, manual reconciliation processes will need to be established to recover after a mistake occurs.

Another area that many companies find difficult to adequately track is contractors. Is there a requirement to track them coming and going? If so, they need to be in the identity store and auditing database(s). There is usually a requirement to provision, maintain, and remove their system accounts in a similar way to employees, so they will most likely be there anyway. However, they may not be in the Human Resources and payroll system, so some other mechanism needs to be established to track them. This can be a particularly difficult area because the ownership of contractors within a company can be nebulous at best. You need to manage their life cycle with the company—they may start as a contractor and become an employee or start as an employee and convert to a contractor. The solution that manages your unique identifier, for example, needs to manage contractors and their movement throughout the company. Although the Human Resources or payroll departments may not like it, they are usually best equipped to take on this responsibility. Adding a separate table in the payroll database may be a simple solution.

 Care is needed when recording and managing information about contractors so as not to blur the line between contractors and employees. This mistake could lead to law suites over benefit entitlements.

When senior management backing is established at the start of your project, ensure that consistent management of contractor accounts is clearly listed as a key requirement. When Human Resources pushes back or hiring managers want to “just create an email account for a contractor” and bypass the established process, you need to be able to have the management backing to enforce the policies that enable appropriate tracking of accounts.

Customer Service and Support

Almost all organizations provide some form of products or services to customers and partners. Outside of SSO, this type of activity is often ignored by Identity Management implementations until it is too late, yet this is also an area where an organization can benefit significantly in both hard and soft ways—through actual cost savings to improvements in customer satisfaction. The potential for a company to provide comprehensive customer service and support is greatly enhanced through the introduction of a strategic Identity Management initiative. One of the key features that customers want to have is the feeling that the company knows who they are and what they want. This is extending the customer experience through the use of technology, and Identity Management supports this in several ways:

- Maintaining a single identifier for each customer from “cradle-to-grave” across applications, services, and similar
- Maintaining profile information on each customer
- Maintaining preference information on each customer
- Supporting secure transactions with customers
- Supporting self-care for customers

Most organizations have the need to meet these requirements for customer service, yet companies continue to implement customer support applications for separate initiatives across their organization. Consider that you have many internal customers, in the form of employees, contractors, and consultants. Most, if not all of the things we discuss here, can also be applied just as effectively to that group of customers.

What does Identity Management mean to customer service and support? Simply, all applications and services can be managed through a common solution, and customer data, policies, and security can be consistent across the various applications that are written to support customer-facing requirements. This includes holding and facilitating data access policies across disparate data environments.

Customer Service Through the Web

Today, a Web-based customer service site is an essential tool to facilitate and organize growth. Whether directly accessed by the customer over the Web or immediately distributed to customer service representatives over an Intranet or extranet, a Web-based customer service site has been described as one of the killer applications of the Web. This solution helps with cost reduction through minimizing the number of calls to the organization call centers requiring a physical presence as well as supporting the need for a consistent customer experience. It is often presented through a CRM or similar application, however, as discussed earlier, an Identity Management solution has the ability to provide Web-based customer service capabilities.

In terms of the directory service opportunity, the site must support the goal of comprehensive customer service by allowing customers the following capabilities:

- Allow customers to easily identify themselves to the site (SSO)
- Request information, goods, or services pertinent to them (self-service and self-service provisioning)
- Obtain information about their interactions with the organization (self-service)
- Open trouble-tickets if appropriate (self-service)
- Easily update their personal information (profile management)

The site should be personalized to the needs of the customer, and this requires some form of profiling. Profiling could include support for pro-active services.

For example, Web sites provide customized content based on such profiled information. Broad examples of this type of profiling and customized content are My Yahoo and My Netscape. You might also be aware that using your profile, these sites can target advertising and specific stories to you. Netscape offers a Web site specifically dedicated to their channel partners known as Insight. Using their technology, they maintain a directory of all participants. The interesting thing about this site is that they require partners to obtain a certificate from VeriSign in order to access the site content. Thus, access is not based on a username and password combination, but instead on having the password available to access the certificate to open it and make it available to respond to the site.

Beyond this type of setup, Web sites such as Amazon and Dell use information on you and the purchases you have made to selectively provide you with relevant information. In the case of Amazon, they offer you Book Recommendations based on who you are and what items you have already purchased. Whilst in many cases there is a database directly supporting the Web site, there are Identity Management methodologies behind the database maintaining identity information to support those functions. This Identity Management solution helps organizations to provide customers with focused attention based on the needs of the individual. The system that Amazon.com uses to make book suggestions is classified as a recommender system and is used in conjunction with Identity Management. Actually, this information is a set of historical data and preferences linked to a person's identity, and serves as an example for applications linking processes and data with Identity Management.

When a customer is interacting with someone for the organization, you can allow customer support and sales representatives to easily access all information about the customer given a single identifier for that customer. Commonly managed in a CRM application, this data is important throughout most organizations, and therefore has benefit if available in both front and back offices. When you make this data available through Identity Management processes, you can enable support for registration, maintenance, and customer communications, including

- Phone calls supported through call center lookups and caller ID
- Faxes
- Electronic mail
- Written correspondence, stored in a electronic document management system
- Sales transactions, stored in the sales database
- Physical visits, noted against the customer support database

Physical Resource Management

Physical resource management is a broad term that revolves around how you manage resources beyond accounts and security resources. In this case, you should be considering how you will manage the provisioning of resources such as

- Phones (both at desks and mobile)
- Pagers
- Desks and offices
- Hardware tokens (beyond the actual activation of the token)

In these cases, the process requires more than bit-switching, and physical interaction is required to provision the resource as discussed in Chapter 2. Managing physical resources is done through workflows that allow events to occur outside the ability of the Identity Management solution. All the Identity Management solution will know is that something should be happening. The key here in your implementation consideration is to ensure that the workflow solution can deal with timeouts and escalations.

Implementation Specifics

Implementation is the phase of an Identity Management project in which you need to deliver. What you deliver, in essence, is what you will be judged on by senior management, your business partners, and your end users.

 It does not matter how well you have engaged your stakeholders, gathered requirements, and planned your project—if you fail to deliver according to set expectations, the entire project will most likely be judged a failure.

However, if you have carried out adequate planning, requirements gathering, and setting of scope, there is a good chance you will have set yourself up for success. Successful implementation is important whether you are deploying a new interface for administrators, updating a synchronization process, or deploying a full provisioning, meta-directory and account management system. Remember, an Identity Management system and project could involve the deployment of several different products and systems to provide a solution to meet a company's needs; so careful planning of all the inter-dependencies is vital.

Implementation Scope

What is it you have set out to achieve? If you have promised the world, you are almost surely setting yourself up for failure. The best way to manage expectations is to break the implementation into multiple phases, each with discrete achievable deliverables. Doing so can sometimes be difficult to achieve because of the complex inter-dependencies present within an organization, but is still worth attempting. What you choose to deploy depends a lot on the purpose of your Identity Management solution. If you are providing user self-registration and management on an Internet site, your deliverables will be different than those of an internal Identity Management system.

With an internally focused solution, you might want to start off by deploying a basic white pages interface on top of your core identity store. Doing so will require certain provisioning and meta-directory interfaces to present and maintain the data so that it is a good test of the overall strategy. End-user self-service of certain attributes, such as phone numbers and other contact details, could also be a part of this step or a follow-on phase. This process allows you to establish a central store of user profile information that can start to be used by the company in application development and workflow processes and begins to establish credibility. You can progressively add more and more components of your Identity Management solution over time to bring functionality online. This expansion of functionality could include a full range of activities such as account (NOS, messaging, and the like) provisioning and account management (including password resets and synchronizations), complex meta-directory processes, SSO, and role-based access control systems. Each step builds a more detailed user profile that can be used to achieve the benefits of a well-planned Identity Management solution as highlighted in Chapter 1 (TCO, business processes, security improvements, account consistency, and the like).

Team Composition

You need to think carefully about the composition of your implementation team. What use (if any) will you make of external Identity Management services organizations? A lot of the questions around team composition are not all that different from those you ask for many other IT implementation projects.

A project sponsor/champion is required to manage business expectations. This person is responsible for working with the overall sponsors in the senior management team (senior management backing is vital as mentioned elsewhere in this book) to keep them abreast of developments and request support when working with business partners. In addition, this person is responsible for being a liaison between the core implementation team and the business partners and stakeholders. Consistent communication and feedback is required throughout the implementation phase(s) to ensure that expectations are set and met or that a change in requirements is dealt with in the appropriate fashion.

A project manager is required to manage overall project costs and deliverables. A technical team leader is a vital part of the overall team as well. The person targeted for this role needs to be able to work closely with the project manager to manage deliverables and work at a technical level to accomplish directly and/or guide a technical team to accomplish the necessary technical development for the implementation. The reason that this role is so vital is that the process of mapping complex and often conflicting business requirements and workflow processes to technical solutions can be extremely difficult. A business analyst can help in this process and should be assigned to the project at some stage as well. There will also be various technical hands-on development and infrastructure personnel required on the team.

 One of the key roles in an Identity Management implementation is a security expert. Centralizing the storage and maintenance of identity information has major implications on security requirements around this data as well as overall security policies in a company.

If the Identity Management system is used to provide role-based access control to important corporate resources, compromising the data in the store has major ramifications. Human Resources and legal representatives need to be accessible for similar reasons. Storage of certain information has privacy and legal implications.

External services organizations can provide a lot of value to an implementation. Most companies that attempt to deploy an Identity Management system for the first time generally doesn't have a lot of experience in this area. Some services organizations specialize in deploying Identity Management systems and can add a lot of value to your solution. Often they are involved in the planning phases and will continue on into deployment, which can help with continuity. In addition, if you purchase a particular vendor product, the vendor might have a professional services arm that can help with the technical side of the deployment. You need to be careful when engaging external and vendor services organizations. Some of the things to take into consideration include:

- If you choose to have the technical lead position and/or the project management positions filled by external organizations, ensure that you have a counterpart within your company dedicated to answering the external person's questions and overseeing assumptions and decisions.
- Be aware of conflicts of interest with vendors and vendor products, including partnerships and strategic relationships.
- Keep a tight reign on scope and deliverables to ensure that your organization doesn't set or agreed to extra tasks by the consultants that don't meet with your core requirements and scope.
- Ensure that there is appropriate handover of configuration and development aspects of the project. This is extremely important from the maintenance and future enhancements aspects. Business processes change all the time and it is important that internal personnel are able to carry out maintenance and customizations to ensure that the Identity Management system can adapt to the changing business needs. Continually having to re-engage external services organizations is a length and costly exercise.

Migration and Interoperability

As mentioned in the provisioning and workflow section earlier, migration from existing Identity Management systems and processes can be a tricky proposition. It is unlikely that the deployment of a comprehensive Identity Management solution does not involve the replacement in some form of existing processes and components. Native administration tools that are being used to create accounts or in-house automated tools could be implementing a form of primitive provisioning, account management, or meta-directory processes. It is extremely unusual that a "green fields" environment exists. The exception could be certain extranet or customer facing systems.

Take care to evaluate all the dependencies between the old systems and processes and the new ones. It is entirely possible that interoperability between the old systems and the new will need to be built. For example, the existing systems might be producing some form of unique identifier that is being used to link some of the systems. You might want to either utilize this current setup or replace it with another more suitable identifier in the new Identity Management system.

You might need to run the new system in parallel with the old system(s) to allow for fail-back in the event of a problem. Building these types of contingencies into your implementation is extremely important.

Pilots, Proof of Concepts, and Development Environments

Before deploying an Identity Management solution, you need to prove to yourself and management and sponsors that the system will work. To this end, you need to build a development environment and a proof of concept system. A proof of concept is often a good idea to ensure that you can validate the assumptions made during the design phase and prove to your sponsors that the solution is workable. An additional suggestion is to have the vendor(s) utilize this environment to prove their products work as “published.”

It is not uncommon for the proof of concept system to become the test and development environment. The development environment allows the initial system to be built and changes made without fear of causing problems within the production environment. Having “sandbox” links to test NOS, Human Resources, and identity store systems is required to ensure that the existing production environments are not impacted in any way.

A pilot is also a good idea. Ideally, a pilot will interact with a subset of production systems and be used either by a subset of end users or by a small number of the account administration team. This task is a particularly tricky undertaking because you might need to maintain parallel systems or synchronize systems during the pilot. Although it may be difficult, avoid continuing straight from the pilot to full implementation.

 Use the pilot as a final validation and learning phase, in which feedback from end users and administrators is evaluated and fed into the final product. Set a specific end date, and establish the expectations that the pilot configurations will be retired after this date if at all possible.

Resiliency and Load Balancing

Don't forget the importance of the availability and scalability of the infrastructure components. Ensure that single points of failure are eliminated where possible from the Identity Management solution, and sufficient resources are available to meet and process requests. It would not look good if a new Internet Web site registration system performed poorly or crashed at regular intervals. Many Identity Management systems have resiliency and load balancing built into their products. Use these where it makes sense, and other products such as layer-four switches and such to provide a complete solution.

Training

Existing staff will most likely need some form of training on the new Identity Management system. This training can be broken into two main areas—operational and end-user training. Operationally, the system will need to be kept running and recovered from failures. Processes around this important task need to be documented and handed over to the appropriate personnel. The physical systems and applications need to have corrective actions applied in the event of a failure. In addition, recovery from problems with data integrity is vitally important. Identity Management systems are by their very nature complex beasts, and unintentional changes to connected systems could cause major problems. For example, the incorrect setting of a flag in a Human Resources system could result in the de-activation of a user account or granting/restricting access from an application or important data. Detection and correction of this kind of problem needs to be built-in to the training and troubleshooting documentation.

End users could be users accessing an Internet site, business partners accessing an extranet, or internal employees. Internal employees could be administrators requesting/implementing changes to a user's profile or end users updating their own phone numbers or resetting their passwords. In all these situations, some form of training and documentation needs to be provided. This training could entail FAQs, system documents, hands-on training, or classroom-type sessions. Whatever is required, ensure that it is a critical part of the implementation plan or problems will occur.

Summary

The goal of this chapter is to provide a set of tools to enable you to justify and move toward the implementation of an Identity Management solution. As noted several times, this book cannot provide the complete solution that is immediately applicable to your situation because each situation is unique, but the tools are here to move forward.

Planning is vitally important. Business justification can take many forms; the key is to pick the concepts discussed in this chapter that most relate to the pain points in your organization. The key takeaways on the implementation side:

- Plan for a common store and format for Identity Management data
- Legal issues are a significant concern—ignore them at your peril
- Not all technical solutions will meet your needs
- Interoperability is tough and requires careful testing
- A unique identifier that is common to the Identity Management solution as well as other applications is essential
- Consider requirements both internally (employees, contractors, and so on) and externally (partners, customers) to your organization

Moving forward, it is important to understand where the industry is going and what other resources are available to support your initiative. For this purpose, Chapter 5 will look at the industry and the standards that are being implemented and proposed.