

realtimepublishers.comtm

The Definitive Guidetm To

Identity Management



Archie Reed

Introduction

By Sean Daily, Series Editor

The book you are about to enjoy represents an entirely new modality of publishing and a major first in the industry. The founding concept behind Realtimepublishers.com is the idea of providing readers with high-quality books about today's most critical technology topics—at no cost to the reader. Although this feat might sound somewhat impossible to achieve, it is made possible through the vision and generosity of a corporate sponsor who agrees to bear the book's production expenses and host the book on its Web site for the benefit of its Web site visitors.

It should be pointed out that the free nature of these publications does not in any way diminish their quality. Without reservation, I can tell you that the book that you're now reading is the equivalent of any similar printed book you might find at your local bookstore—with the notable exception that it won't cost you \$30 to \$80. The Realtimepublishers publishing model also provides other significant benefits. For example, the electronic nature of this book makes activities such as chapter updates and additions and the release of a new edition possible in a far shorter timeframe than is the case with conventional printed books. Because Realtimepublishers publishes our titles in “real-time”—that is, as chapters are written or revised by the author—you benefit from receiving the information immediately rather than having to wait months or years to receive a complete product.

Finally, I'd like to note that our books are by no means paid advertisements for the sponsor. Realtimepublishers is an independent publishing company and maintains, by written agreement with the sponsor, 100 percent editorial control over the content of our titles. It is my opinion that this system of content delivery not only is of immeasurable value to readers but also will hold a significant place in the future of publishing.

As the founder of Realtimepublishers, my *raison d'être* is to create “dream team” projects—that is, to locate and work only with the industry's leading authors and sponsors, and publish books that help readers do their everyday jobs. To that end, I encourage and welcome your feedback on this or any other book in the Realtimepublishers.com series. If you would like to submit a comment, question, or suggestion, please do so by sending an email to feedback@realtimepublishers.com, leaving feedback on our Web site at <http://www.realtimepublishers.com>, or calling us at 707-539-5280.

Thanks for reading, and enjoy!

Sean Daily
Founder & CTO
Realtimepublishers.com, Inc.

Introduction.....	i
Chapter 1: The Who, What, Where, and When of Identity Management	1
Defining Identity Management	1
Identity Management Challenges	3
From the Intranet to the Internet	5
The Benefits of Identity Management	8
Data Management Issues	9
More than just a Technical Issue	10
Functional Aspects of Identity Management	12
Account Life Cycle Management	13
Profile Management.....	13
Workflow	15
Provisioning and Decommissioning	16
Delegated Administration	17
Self Service	18
Password Management and Synchronization	18
The Four As	20
Authentication.....	20
Authorization	20
Access Controls	20
Auditing and Reporting.....	21
An Introduction to Identity Management Standards.....	21
Legal Drivers	22
Summary	23
Chapter 2: Identity Management and Security	24
Risk and Trust.....	24
Authentication.....	27
Password Policy Management	28
SSO and Related Solutions	30
SSO Basics.....	31
Policy Evaluation	39
Access Control.....	39
Hierarchical RBAC.....	41

Auditing	42
Forensics	42
Accounting.....	42
Policy Management and Enforcement	42
Privacy	43
Federation and Federated Identity	43
Summary	45
Chapter 3: Identity Management Applications	46
Self Service	46
Provider Self-Service	46
Enterprise Self-Service	47
Password Management	47
Password Reset	48
Password Synchronization	48
Single and Similar Sign-On	49
Network Operating System-Based SSO	49
Web-Based Access Control SSO	50
Overview.....	51
Agent-Based vs. Proxy Model for Web-Based Access Control Solutions	53
Web-Based Access Control Features to Consider	55
The Future of Web-Based Access Control	56
Client-Side SSO	57
Overview.....	57
Client-Side SSO Features to Evaluate	57
Client-Side SSO Summary	58
Enterprise SSO Tools.....	59
Overview.....	59
Enterprise SSO Features to Evaluate	59
Summary for Enterprise SSO Tools	61
Password Synchronization SSO.....	61
Password Propagation SSO.....	62
Provisioning Solutions	62
Provisioning Features to Evaluate	65

Security Implications	65
Configuration and Management	65
Integration with Existing Infrastructure and OSs	65
Auditing, Logging, and Alerting.....	66
Scalability and Fault Tolerance	66
Agents vs. Connectors	66
Summary for Provisioning Products.....	66
Meta-Directories	67
Smart Cards and Tokens	68
Portals	69
Summary	69
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
Mapping Out the Workflow.....	86
Choosing a Product.....	86
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
Customer Service Through the Web.....	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
Chapter 5: Identity Management Standards.....	97
Relevant Standards Bodies	97
Directory Services.....	99
DSML	100
Web Services	100
SOAP	102
WSDL	103
UDDI.....	104
tModel.....	106
Security	106
SAML	106
WSS	108
Federated Identity and Standards.....	108
The Liberty Alliance Project.....	109
Microsoft Passport	109
Liberty, Passport, Both, or Something Else?	110
Trust	111
Workflow	112
BPEL.....	112

Provisioning	113
SPML	113
Biometric Standards.....	114
BioAPI	114
X9.84—Biometric Information Management and Security for the Financial Services Industry	115
XML Common Biometric Format	115
CBEFF	115
Smart Card Standards	116
Summary	116
Chapter 6: Identity Management Technologies and Trends	117
Consultants.....	118
Professional Services	118
Infrastructure Help	119
The Risk Management Factor.....	119
Solution Vendors	120
Emerging Identity Management–Related Issues	121
Federated Identity	121
Challenges to Federated Identity	122
Context-Sensitive Identity Management.....	123
Identity Theft	124
The Keys of Identity	126
Intrusion Detection.....	128
Intellectual Property Theft	128
Content and DRM.....	130
Regulatory and Compliance Issues.....	131
Identity Management Appliances	131
Software Licensing Enforcement.....	132
Advanced Biometric Applications.....	132
Identity Management Resources.....	133
Summary	135

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 1: The Who, What, Where, and When of Identity Management

Welcome to *The Definitive Guide to Identity Management*, the most concise and practical guide available today to explain the concepts of Identity Management. This chapter will introduce, *at a high level*, many of the concepts and terms used in the field as well as discuss basic and advanced scenarios in which Identity Management is a fundamental requirement. Although this chapter deals with a lot of abstract ideas, it is important for the reader to obtain a good grasp of the key concepts and terms, as they will be used throughout the rest of the book.

Defining Identity Management

Let's begin with a high-level definition of Identity Management. The essence of Identity Management as a solution is to provide a combination of processes and technologies to manage and secure access to the information and resources of an organization while also protecting users' profiles. Identity Management can provide the capabilities to effectively manage such processes both internal and external to an organization—for employees, customers, partners, and even applications, and, correspondingly, anyone or anything that needs to interact with an organization.

Because of the increased interest in Identity Management in the past few years, numerous analysts and commentators offer their views of the definition and related market, as the following quotations show.

Digital identity comprises the electronic records of identity information—including names or unique identifiers, credentials, addresses, entitlements, and other data—held by identity domains about network entities, or principals.

—The Burton Group, August 2002

The notion of “Identity Management” as a business issue is taking hold: Identity Management is often sold purely as a security solution, but organizations are realizing that it also encompasses user experience, business efficiency and business agility. Organizations are starting to realize this and develop Identity Management strategies and incorporate them into their enterprise architecture plans.

—Giga Information Group, November 2001

Identity Management encompasses the integration of products such as directories, single sign-on and provisioning applications into a unified framework for managing user information and access rights across multiple systems and business contexts. Enterprise interest in Identity Management is increasing not just because it improves security. Identity Management also addresses critical business issues and delivers a quantifiable return on investment in four key areas: user productivity, IT management efficiency and help desk cost avoidance, application development agility, and security audits and policy compliance.

—Giga Information Group, September 2002

The focus of Identity Management is on user provisioning—the creation, maintenance, and termination of user accounts and management of credentials in support of authentication and access control.

—Hurwitz Group, 2001

You will find a wide array of acronyms and terms applied to Identity Management. Here are a few that I have come across:

- Identity Management—IM, IdM, IDM
- Identity and Access Management—IAM
- Secure Identity Management—SIM
- Digital Identity—DI, DID
- Identity and Security Management—ISM

As there is no clear winner or distinction among these, I will stick with the complete term Identity Management as appropriate throughout the book.

Given these guiding definitions and array of acronyms, within the scope of this book, Identity Management solutions are viewed as primarily a tool for:

- Defining the identity of an entity (a person, place, or thing)
- Storing relevant information about entities, such as names and credentials, in a secure, flexible, customizable store
- Making that information accessible through a set of standard interfaces
- Providing a resilient, distributed, and high-performance infrastructure for Identity Management
- Helping to manage the relationships to resources and other entities in a defined context

Entities are also often referred to as objects. An Identity Management store (often, but not specifically, a directory) provides these capabilities by storing information in a structured form that can maintain relationships between objects while making it convenient to query, retrieve, manage, and update that information.

An Identity Management solution should also support the *extended enterprise*, which represents business partners, customers, and suppliers. For a true representation of the relationships of a business, all these factors must be taken into account. In addition, this type of relationship management means that access to the enterprise may occur through intranets, extranets, and the Internet. This accessibility includes direct connections, proxied connections, firewalls, wire-line and wireless connections, virtual private networks (VPNs), and so on. Thus, Identity Management is a requirement in the fundamental and widespread functions of any business.

Your *digital identity* depends upon a number of factors:

- Who you are
- The context
- Your profile

A digital identity is often dependent upon the context because each of us plays many roles throughout our daily interactions. The context defines your interactions with the digital world as an employee, a consumer, or a subscriber to services. In addition, our identity is closely related to our *profile*—that is the information, tools, preferences, and resources we need in order to perform in specific roles.

Identity Management Challenges

Identity Management does create some security challenges, however. After you create a centrally controlled identity solution, you also create a focus for any security attacks.

Another issue arises when an incorrect identity is able to be used. In other words, the information accessed or provided is inaccurate. Perhaps a user is using the right identity in the wrong context: you are trying to authenticate to your company's intranet using your personal username and password for your Internet service provider (ISP). Identity can also be dangerous when it is the correct identity but someone else uses it improperly. One of the goals of a comprehensive Identity Management solution is to ensure that the right context is used at the appropriate time.

Today, employees who are with a company for more than 3 years are commonly considered long-term employees, and consumers who shop on the Web have the ability to move from one site to the other, and will if they find a better deal elsewhere. This roaming nature and high rate of turnover creates a significant issue for organizations in terms of knowing who they are dealing with and ensuring that that person is allowed access to what they need, when they need it, and that access is blocked if they are not allowed. In the case of employees, it can sometimes take many months for the right access to the right systems to be granted such that they can be productive.

It is likely that you hold an employee ID card for your job, shop on the Internet at several stores using various logon IDs, possess numerous forms of "identification" (such as a driver's license, passport, or birth certificate), and have numerous credit or debit cards, and so on. The number of tools that you have, and must use, to demonstrate your identity to others can be significant, and seems to be increasing rapidly. If I consider my own situation, I can easily see that I possess many identities, as Figure 1.1 shows. I might use a combination of these, depending on the circumstances or context.

VisaCard	MasterCard	AmericanExpress
8432657986156482	1319298387981257	134655218164158
LotusNotesID	SocialSecurity	AAA
4452286419473789	555261655	558164919767
USDriversLicense	AustralianDriversLicence	UKDriversLicense
C4436733	E79598	R27652
AustralianPassport	EECPassport	USVisa
T5468332	GW669124	XYZ2Y555
HomePhone	HealthCare	HealthClubCard
+1(415)555-9931	91478912657	73283
RetailCreditCard	DiscountStoreCard	LibraryCard
9625872192526	275478442195	1394725631685
VideoStoreCard	FrequentFlyer	Pager
41473464953	BZ485537	18885556537
WorkEmail	PersonalEmail	CellPhone
name@company.com	plugh@emailco.com	+1(415)555-8397
CheckAccount	SavingsAccount	Mortgage
2551862125	8155212452	2525395721
CarLoan	EmployeeNumber	StudentID
172748864	CA15896	0576812

Figure 1.1: The various evidence of our many identities.

As this figure shows, I have traveled to a number of places around the world, increasing the number of national identities as well. This figure also illustrates that, as an individual with many identities, I also have many different and varied relationships with organizations, governments, and businesses: as an employee, as a customer or consumer, as a citizen, as a foreign national, and so forth. These relationships are known as *identity context*, which is an important concept that will be raised consistently as we work through this Identity Management guide.

As the previously mentioned issues illustrate, there are many factors driving the adoption of Identity Management solutions—these challenges are faced not only by the enterprise, but also by consumers and governments. As with many organizations, governments have their own policies about what identity data they require of individuals within their borders. Governments have policies about how that information is shared across government agencies, if at all. Similarly, they might have policies about whether the information can be shared outside the agencies. The same goes for the employee and customer data of businesses and other organizations. So we can see that at least some Identity Management components are vital across the vast group of corporate and government entities worldwide.

Challenges abound not only because this set of requirements and disciplines is new to those who are trying to implement Identity Management solutions, but also because the solution space is evolving rapidly in terms of scope and capabilities. Identity Management solutions have historically taken many guises and are commonly accepted as a specific part of enterprise security, or as a set of components primarily built on the security infrastructure. The reality is that the security component is only a small area within the Identity Management borders, and that much more process and technology lies beneath the surface. In later chapters, we will dig deeper into the specifics of the disciplines that are involved in creating an Identity Management solution.

In the earlier days of computing, circa the 1970s, protections would be provided through simple physical limitations. The mainframe was in the building, and to get access, you had to be in the building. Generally, there was a crowd of people who would know whether you belonged in that space. As networks evolved, from PCs on LANs to the Internet and even wireless networks, the physical nature of security became impossible to manage.


From the Intranet to the Internet

In a cartoon by Peter Steiner that appeared in the July 5, 1993 issue of *The New Yorker*, (Vol. 69 no.20), a dog says to another dog, “On the Internet no one knows you’re a dog.” This quote epitomizes a core part of the Identity Management challenge. How can anyone be sure who they are dealing with? Today, with advances in auditing, tracking, and profiling, Web site owners and corporations can create profiles of individual habits and interests, allowing for them to form a loose identity for each user of their sites.

These advances, however, ignore the original premise of the quote, which is that you are largely anonymous when surfing the Internet until you use an identity to identify yourself to a site. Doing so could be as simple as connecting from a specific computer or system, to being as advanced as using a complex series of passwords and certificate credentials. Thus, the issue of anonymity is another *identity context* wherein someone might access the resources of an organization and have the ability to perform certain actions without identifying themselves. For example, being able to browse an online store catalog and select items to be placed into the online shopping cart is possible without identifying yourself specifically to the site. However, if you want to purchase something, the site will require more information, introducing a different identity context. In addition, when you identify yourself and provide the necessary information, more compliance requirements exist around what information can and will be shared to complete a transaction. The Web site needs to know your credit card details, your address for shipping, and so forth.

In contrast, other sites might require registration (the creation of an identity) before they allow you to browse. For example, many premium content sites such as entertainment (music and movies) and research sites will not let you see content without at least registering, and sometimes not even without a credit card being processed.

Consider the situation in which registration is required but not validated. Perhaps the site designers want merely to collect some statistics about when and how often you access the site. However, many users often register using false names and if required, false physical or electronic addresses. How valid is this identity? The answer depends on the identity context, and how important the information really is. Concerns about privacy and a desire to work anonymously unless absolutely required to divulge one's identity often make people carry out this type of interaction, presenting another challenge of an Identity Management solution. This example opens for discussion the area of trust and the degrees to which each party (individual, government, or organization) trust each other.

 The concepts of trust, privacy, and anonymous access are broad, and sometimes nebulous, requiring much deeper review. I will offer a detailed discussion in Chapter 2.

Identity Management ensures that an identity derives from an authoritative source and that the creation of that identity is monitored and audited. Identity Management also ensures that an identity is secured—that is, it prevents others from tampering with that identity and continually validates the authenticity of that identity. And finally, Identity Management allows identity to be shared effectively, ensuring that information is provided in a timely, accurate manner while protecting privacy.

Identity Management solutions allow for

- Personalization
- Scalability
- Portability

Each of us can keep track of 5 or 10 things about a number of other people. Because we know some basic facts about those people, we know we can trust them on some level. Beyond that, it becomes arduous for most individuals to track, let alone be able to enable others to work together. Identity Management allows us to preserve a large-scale level of trust. For instance, within a company of, say, 50,000 employees, it is rarely possible to know everyone, and the only way to trust that someone is from the same organization is to work within some common framework. Because Identity Management solutions allow us to store and secure basic facts about an individual, we know we can effectively share those facts, making our identity portable across contexts and organizational boundaries.

These solutions allow us to

- Create a clear and unique identity for each user
- Simplify and rationalize the context related to that identity
- Define policies and security based on profiles

Identity Management solutions provide a simple mechanism to make sense of growth and complexity, ensure consistent configuration of all systems when users are added, deleted, or modified in some way, and map authentication, authorization, and access control across independent semantic systems (such as a Lotus Notes database, an Oracle database, or a Lightweight Directory Access Protocol—LDAP—directory).

Identity Management is about efficiently managing a definitive identity for a user and ensuring that users have fast, reliable access to information and applications in a secure manner. It encompasses the four As, namely

- Authentication—Proving who the user is
- Authorization—Determining access rights and user privileges
- Access control—Managing means of access
- Audit—Reporting and audit controls

Interestingly, many believe that such a solution requires a single, central store of all this identity information in order to be effective. Such is not necessarily the case, although it certainly makes things easier to manage technically. In Chapter 2, we will discuss the concept of federated Identity Management, which is a concept that supports the idea of sharing the right identity data across security boundaries such that intra- and inter-company activities and processes can be developed and utilized.

The Benefits of Identity Management

The following list offers the primary goals and advantages of implementing an Identity Management solution for an organization:

- Reduce total cost of ownership (TCO) for all systems (reduce administration, Help desk, and technical support costs)
- Reduce management overhead
- Provide competitive advantage through enabling automation and streamlined optimization of business processes
- Improve customer and employee service, and maintain the control and confidentiality of customers, suppliers, and employees
- Reduce time taken to enable new employees to get access to required resources within the organization
- Reduce risk of incorrect information being used for business processes
- Reduce risk of ex-employees retaining access to organizational resources
- Support legal and compliance initiatives around employee and customer data (for example, the United States' Health Insurance Portability and Accountability Act—HIPAA, the European Data Protection Directive, and the Canadian Privacy Act)

Done correctly, Identity Management solutions will support many security initiatives as well, including:

- VPNs
- Public Key Infrastructure (PKI)
- Single Sign On (SSO)
- Lookup services such as White Pages and Domain Name Service (DNS)
- Controlled access to corporate data

Identity Management solutions can also supports many profile-management requirements, including:

- Customer satisfaction by ensuring the consistency of customer information
- Profile management allowing for personalization of Web sites and applications
- Network management
- Directory Enabled Networking (DEN)

Finally, Identity Management solutions will enable organizations that undertake development to decrease those development costs, as the solutions

- Provide consistent and standard identity data to and for applications
- Often provide for a standard access mechanism (for example, APIs, standards) for access to identity data

To illustrate these benefits, consider an example from the healthcare industry. Most hospitals or care centers have the following issues:

- Multiple locations, partners, and providers
- Disparate and disconnected admission systems and—worse—separate and disconnected outpatient systems
- Different interfaces between those other internal systems such as those used for clinical, financial, and administrative functions

The result of this environment is that information from previous treatments might not be found when a patient is admitted; payment histories are not maintained; and demographic information might not be consistent. The implications of such shortcomings could be, at worst, fatal.

Electronic patient records, which allow access to patients' histories online, are an essential tool for clinicians. Without a permanent patient record, electronic medical records are not feasible. However, such a tool is incredibly difficult to implement when there are too many disparate systems that cannot maintain a patient identity between them. In the United States, when you add HIPAA-compliance requirements to this scenario, the situation becomes a considerable identity crisis. HIPAA requires the creation and maintenance of a permanent patient record, with availability of information to care givers and with security constraints to preserve confidentiality. Hospitals must comply to stay in business. As you can see, an Identity Management solution is needed to overcome this identity crisis.

Data Management Issues

After you realize the benefits of Identity Management, it is critical to realize that every application your organization decides to use has the potential to give rise to the creation of a new set of identity data. Every time this new data is created, there is a decrease in the organization's ability to guarantee that the information being held is accurate.

Consider how many projects have the need to gather and maintain information about the project's users, then define some form of authentication and authorization process around that information. Whether it is an in-house Web application, a remote access VPN solution, or a third-party application, there is usually significant effort expended to gather the relevant data, and even more effort expended to manage that data.

Unfortunately, although architects and developers often justify parlaying the immediate needs of an individual project against the delays in creating an enterprise-ready solution, the costs increase over time. Because it often occurs that the new application is not the “owner” of the data it needs, there will always be another place for people to go to update their information. Worse still, if the new application incorporates update or identity functionality within the solution, there is the risk of alienating or confusing users. There will either be more time spent updating the same information across multiple systems, or there will be the expectation by users that by updating information in one system, it will be reflected across other systems using the same information. Either way, there is a cost to the organization that cannot easily be quantified.

More than just a Technical Issue

Within an organization, a good Identity Management strategy goes a long way to realizing these goals, which should be near the top of any IS manager and CIO’s project list. (Increasingly, an Identity Management solution should top the CEO’s list as well.) Compliance and regulatory reasons abound when dealing with data about individuals. In Chapter 2, we take a deeper look at these concerns, but for now, consider that Identity Management is definitely not just a technical issue or a technical solution. For that reason, understanding how an Identity Management solution can enable these capabilities is not only vital for those with a technical background, but is also essential for those operating with a business focus.

So, although Identity Management is often looked at as being a purely technical solution, the primary focus for developing Identity Management solutions are most definitely business issues and deserve an overriding business focus. The issues surrounding a successful implementation of an Identity Management solution revolve around the following business areas:

- Conformity of project to business goals
- Data ownership or stewardship
- Data integrity
- Data usage
- Security
- Political concerns
- Legal issues
- Compliance issues
- Support of business process

Given all the positive things that Identity Management solutions can make available, let's look at the main reasons why an Identity Management initiative is most often overlooked or fails:

- Lack of understanding—either of the needs and benefits or the technology and business relationship
- Lack of senior management buy-in
- Lack of security processes and procedures, or lack of timely security involvement in the project
- Lack of enterprise planning groups and supporting budgets
- Perception of corporate solutions not allowing business units to quickly and easily maneuver in the marketplace
- Geographical isolation creating support, development, and network connectivity issues
- Traditional type stovepipe organizational structures, sometimes related to political issues such as empire building. (In the past, companies were organized along functional lines, commonly referred to as *stovepipes*; one department handled order processing, another handled billing, and so on. The computer systems that supported these individual business processes were not usually designed to integrate with other department systems.)

As you can see from this list, there is much commonality between Identity Management projects and other enterprise-level projects that organizations attempt to deliver today. It is important to realize that the delivery of an Identity Management solution is not a simple project that one department can take on and immediately provide enterprise-level benefits. Identity Management is one of the ultimate matrix projects, requiring input and resources from many different areas and levels within, across, and potentially from outside the organization.

Functional Aspects of Identity Management


We will discuss the process side of Identity Management as well as the specific security issues throughout the book, but for now, consider the following concepts as parts of Identity Management solutions, and again, remember that concepts apply across employees, customers, partners, even applications:

- Account life cycle management
 - Provisioning and decommissioning
 - Delegated administration
 - Self service
 - Password management and synchronization
- Access and authorization controls
 - Single or similar sign on
- Auditing and reporting

More comprehensive Identity Management solutions consider the needs and integration requirements for:

- Federated identity
- Web services integration
- Policy-based management and enforcement

Until recently, the focus for Identity Management–type solutions has been specifically on the enterprise and business solutions. The need for a similar set of solutions to help support inter-organizational Identity Management is also there. The rapid rise of Internet-based commerce, with both organizations and individuals, has given support to the concept of *federated identity*. Although Internet access is often considered anonymous, the requirements to enable trade and interaction through interconnected electronic commerce demands some form of identity solution that can scale across organizational boundaries. The concept of federated identity is defined as being able to extend account profile and access management to third parties who need to access resources in your organization, and similarly, being able to project your identity or identities that you manage (either as an organization or individual) to others.

 This concept can get complex, and begs the question of privacy. Critical standards, deployment options, and commercial support have, arguably, been growing significantly in recent years, and we will discuss federated identity solutions, and the question of privacy in Chapter 2.

Consider also, that as federated identity becomes a reality (for example, through the Liberty Alliance Project—see <http://www.projectliberty.org/>), the need to provide the following functionality becomes a natural progression for a complete and dynamic profile-management solution:

- Presence (status, availability, and so on)
- Personal preferences
- Mobile services (location)
- Digital Rights Management (DRM)
- Privacy, compliance, and legal issues

The question is, do these federated identity solutions require Identity Management, or do they support it?

The answer is both, and that goes to show the potential complexities of discussing Identity Management. These solution spaces are all advanced in terms of use and requirements of Identity Management. Throughout the book, we will be looking at some of these; however, most will be discussed in Chapter 6 dealing with Identity Management technologies and trends. For now, let's discuss these key areas and why they are essential components of not only an Identity Management-specific solution, but any enterprise solution.

Account Life Cycle Management

The concept of account life cycle management is that you can manage the state of an account, whether it is a user, system, or service account, for the complete span of importance for that account. Thus, even if you delete or disable the account, there may be requirements for maintaining an audit history of its actions as well as actions taken against that account. The key parts of the account life cycle management process are:

- Provisioning and decommissioning
- Self service
- Delegated administration

Remember that this part of the Identity Management puzzle applies regardless of the access required. Similarly, there is a fundamental need for profile management within the scope of account life cycle management.

Profile Management

Profile management provides a way to manage identities and distribute that managed information to external databases, directories, and applications throughout the enterprise, and potentially beyond. This process facilitates the self-management of user profile information and the automated replication of accurate profile data to key enterprise systems.

Accurate user profile information inevitably relies on many updates to a user's profile, making it important to determine where definitive information exists and build each element into a single central user profile. The goal is to create an environment in which when a definitive user profile is created for a user, any subsequent changes to that profile are automatically applied in accordance with existing or defined policies and rules.

Profile management, therefore, must address security-related requirements such as establishing and utilizing a unique identifier for each account. Using Identity Management tools such as provisioning applications, meta directories, and directories let you automate these processes, increasing administrative efficiency and effectiveness while reducing operational costs. This provides a platform from which to easily add new services, introduce Web services, and enable collaboration with external systems and organizations. Table 1.1 provides the key components of profile management.

Profile Management Component	Description
Creation and management of unique user profile identity	Nearly every organization holds multiple pieces of data on system users, but which data is the definitive data for a specific user? Usually the definitive user information is distributed across numerous systems and applications, necessitating building a unique definitive user profile by integrating subsets of data from different user records. The challenge isn't just to build the user identity, but to ensure that any changes to the user data at source are synchronized across all systems in accordance with organizational policy.
Self-management of user profile information	User profiles can contain sensitive information as well as less sensitive attributes (such as phone number, email address, and location) that can be directly managed by the user. Identity Management enables organizations to establish policies as to who can manage which data. An Identity Management store ensures that all attributes are subject to access rules determining who can read specific attributes and who can add/delete/modify attributes. By enabling users to manage some of their own data, you can ensure accuracy, remove administrative overhead, and save administrative cost.
Automated replication of user profile information across key enterprise systems	User information need not be held in one central repository. With the user profile being managed within an Identity Management store, the user profile content can then be automatically distributed across multiple systems and locations, ensuring that the latest data is available wherever it is required. This also increases the overall system performance and efficiency, reduces network bandwidth requirements, and saves on operational costs.

Table 1.1: Key components of profile management.

Workflow

Support all these aspects of account life cycle management generally requires the use of some form of workflow. Workflow is fundamental in order for an Identity Management solution to fulfill its role within existing and any newly established processes. There are many examples of a workflow solution; for example, the process of document editing and approvals before publication, resource provisioning, and bug tracking.

To broaden the example of document management, consider authors or writers working on creating new or updating existing documents, reviewers or QC (quality control) experts ensure the quality and suggest or request changes. As a result, a document might bounce back and forth between several key members of a team, with a final step being approval to publish. The final approval to publish outside this control group may come from someone identified as a team leader, project leader, or be a member of an approvals group who has the capabilities to approve the publication action. Many organizations offer this type of solution based on their Identity Management solution. Microsoft, for example, offers SharePoint Portal Server, which handles much of this kind of management based upon the identity already being in Active Directory (AD) and the permissions assigned. Similarly, Documentum offers its enterprise content-management solution with workflow capabilities.

These examples make use of workflow to manage specific processes. Now consider the need to manage the processes around the creation of the identity that these applications make use of and you begin to see why workflow is an integral part of an Identity Management solution. This process of creating identity within an organization may be simple, and essentially relates to the need to gather enough information such that the identity has enough context within the organizational bounds. The same applies to Web sites.

Workflow supports the situation in which approvals are needed, such as a manager approving certain resources be provisioned for an employee or requiring an individual to reply to an email before the user can get access to a Web site, which is a common practice when signing up for a Web-based site. These events are out of band for basic workflows and might require advanced capabilities in terms of timing out (if the manager or individual does not respond in a specific time), and potentially escalating to higher-level managers or alternates, according to a defined flow, or even initiating a completely separate workflow process. Similar workflow requirements exist if the process of account management requires that certain events take place in a certain order, either in parallel or a specific sequence.

Workflow engines direct and monitor the processes for managing changes and distributing them through to connected systems according to set policies, which can potentially be quite complex, allowing for both automated and manual intervention in order to progress the workflow. Furthermore, a workflow engine needs to be able to deal with conflicts through a similar manual intervention. Finally, to be successful, the workflow engine needs to understand the identity of the users within the system in order to know the identity of the appropriate individual or group that is needed to deal with manual processing or authorization steps within a workflow or process. Let's look at the specific components of account life cycle management in more detail.

Provisioning and Decommissioning

Provisioning is an extremely hot topic in the industry today partly because vendors position their solutions in the context of both Identity Management and security. Provisioning streamlines the process for giving employees, contractors, partners, and customers fast access to information resources—and for improving security by de-provisioning access when they leave.

You will see that many vendors and even analysts have taken to calling this component of Identity Management *eProvisioning*. The distinction being made is that such solutions deal specifically with computerized or electronic systems, as opposed to more physically based requirements. For example, consider the “provisioning” of business cards, a desk, or office space. These are commonly outside the scope or control of most electronic systems, however, as many eProvisioning solutions can satisfy this type of requirement through the use of defined workflows and manual intervention, eProvisioning is generally a marketing term more than a real distinction.

It is important to note that such provisioning solutions are at times difficult to differentiate from meta-directory services due mainly to the fact that both provide provisioning capabilities. However, meta-directories are more likely to be the core component of advanced provisioning, while the broader provisioning solutions also provide functionality not traditionally offered as part of meta-directory services—namely workflow and business process management, delegated user administration and self-service GUIs, and advanced security auditing and reporting. Like most identity-related projects, implementing a provisioning component is as much political as it is technical, requiring organizations to undertake time-consuming tasks such as data cleansing and process definition; often across a diverse group of stakeholders.

The classic case in which provisioning is essential is that of the new employee who cannot be effective until he or she has the necessary resources to perform the job. When the new employee joins a company, there are typically a variety of services he or she will need to access to do his or her job. Employees today typically require email accounts, access to enterprise portals, CRM, enterprise resource planning (ERP) and self-service applications, remote access networking services, firewalls, and more. In many companies, the process for managing user access to these applications and services is very labor intensive. Employees (or their managers) must request accounts, an account administrator responds, enters the employee identity information into an application, sends a set of initial credentials to the user, and after some period of time, sometimes weeks, access to the application is gained. This process is typically repeated for each application with a different group of administrators, and repeated again when an employee’s responsibilities change or when he or she leaves the company.

User provisioning is about automating these processes ensuring that, for example, as soon as a new employee is entered onto a Human Resources (HR) system, the employee's data triggers an automated process in which an email account is created, an ID badge is generated, the NOS administrator is notified, and subsequently a NOS account is created. This automated process creates the following benefits for an organization and user:

- The cost of provisioning a new user/subscriber drops dramatically and accuracy improves as individual application managers no longer need to reenter information about users into their administrative environments.
- Users can be set up with a default list of accounts and account privileges based on their job responsibilities, contributing to a well-defined and understood security policy.
- Accomplishing enterprise user provisioning in a timely fashion helps ensure that new employees are productive in the shortest possible amount of time.

Provisioning activities can be automatically initiated when a user's status changes. If we apply the new employee example to circumstances in which the user leaves the organization, the user details can be immediately updated preventing user access to any of the systems, ensuring security is watertight. In cases in which employees leave an organization, it can take months to manually remove them from all systems, creating a major security threat. Provisioning can therefore be cost justified with this type of example.


Delegated Administration

Delegated administration is an area that has become increasingly important when dealing with partners, customers, and employees. Delegated administration begins with the ability to define which accounts have the ability to perform certain managerial actions (such as creating new accounts) or managing specific functions (such as changing an account password).

Thus, given the ability to delegate the actions or effort of administration, the goal then is to provide an environment wherein this task is undertaken in a secure and responsible manner. To do so, requires comprehensive access control models, which we will discuss shortly.

Most administrators understand the concepts of roles in this type of environment. When a complex operating system (OS) is installed, there is often a default or predefined "administrator" account that has administrative capabilities. This account is usually used to configure the system. Part of this process is generally to create other accounts and grant them rights on the system (such as the ability to access the file system, run programs, and so on). This is part of the security model of the OS. Consider then that an Identity Management solution should provide the ability to extend this type of model across systems and applications, even across businesses. By defining an administrative model that can work this extensively requires delegated administration to scale and an access control model that is flexible enough to embrace unknown products.

Another aspect that needs to be offered is the ability to support temporary administrative capabilities based on conditional data in an account profile or system, or specifically, time-based data. This idea relates to the concept of *access controls*, which we will discuss shortly.

 It is important to consider that any actions taken within the system must also be securely logged, backed up, and able to be audited at any time. This allows you to not only see the actions -that were undertaken, but who was responsible, should there be any issues with actions undertaken within the system.

Self Service

The extreme or ultimate case of delegated administration is self service. This is the ability for an individual account to actively manage its own profile without requiring the intervention of Help desk or support staff. Such an arrangement can have a further and significant impact on cost basis for your organization.

Self service could allow for the individual to request access to other systems or services; however, self service is, in general, focused on giving individuals the ability to manage their passwords across systems. More advanced solutions allow the user to recover from a forgotten password through various means such as challenge/response questions. As an example, you might be familiar with institutions asking for your mother's maiden name to validate your identity. This method can be implemented within a delegated administration or self service application.

Password Management and Synchronization

From a user perspective, one of the biggest frustrations is the requirement to have a different password for every system to which they require access rights. Password management assists with addressing these problems. It can do so through a single-sign on solution, wherein a front-end application, agent, or service manages credentials on behalf of the user. When access is required to a specific system, the front-end application, agent, or service then passes the appropriate credential through to gain the required access. This mechanism can also manage password changes such that they are consistent, according to a chosen policy, across systems. Alternatively, this might be managed by a back-end service that ensures through password management that a user can maintain a common account name and password across disparate systems.

Password synchronization solutions come in several forms. One solution is to implement a top-down enforcement of your password changes through a system that can also implement password policies. This is generally in the form of a password change application, often implemented as a secure Web page that users must use, that then fans out changes to other systems. This does not necessarily create a central repository of identity information for use by other applications, but it can. A common issue that many enterprises who have implemented Microsoft Windows infrastructure face, as opposed to those with Internet-facing applications, is that there is already a mechanism through the Windows clients to change passwords. This needs to be identified as the password change mechanism, allowing for password changes to be intercepted, then propagated, or the ability for users to change passwords on the client needs to be turned off and another application interface used.

A similar method is to utilize directory solutions to manage account passwords in a central store (for example, a directory) and a synchronization mechanism (for example, a meta-directory) to propagate the password to all the related accounts across disparate systems. This method significantly reduces administration costs, improves user productivity, makes it easier to rapidly deploy new services, and increases security as there are fewer passwords that can be compromised and password synchronization across all systems is automated. Finally, these mechanisms may be used in parallel.

The most common issues faced in this space are:

- Password resets and support or Help desk calls are a major and increasing cost
- Password policy is enforced on a team-by-team or system-by-system basis
- Support staff are spending too much time resetting expired or forgotten passwords
- Password are regularly shared, or worse, compromised
- Lack of standards on how passwords are created, stored, and even replicated through corporate systems

Password management exists today as one the most prevalent issues for an organization's administrators and Help desk staff. Recent analyst reports have established that nearly 66 percent of Help desk calls are related to password management issues, and the cost per call is between \$20 and \$30. The annual cost per user is estimated to be \$230. This, therefore, represents a significant cost for today's typical organization. User populations whether end-user employees or customers continue to grow, increasing everyday the complexity and costs associated with maintaining passwords, providing service quality and service level agreements (SLAs) to users, and ensuring ongoing protection of corporate assets. Consider the business requirements described in Table 1.2 to see if this situation is familiar in your organization or application space.

Business Requirement	Description
Reduce the time support staff spends resetting passwords	The use of fewer passwords makes it easier for users to remember their password details and decreases the chance of passwords being compromised. As a result, administrative and Help Desk staff get fewer password-related calls.
Reduce the costs of password management and resets	The existence of fewer user passwords and the lower the chance for passwords to be compromised results in fewer calls to administrators and Help desk staff for password resets. This significantly reduces administrative costs and enables administrators to focus on higher-value activities.
Allow users to sign on to key enterprise systems with a single set of credentials (user name and password)	Enable users to have a single password that can be synchronized across all systems that the user is authorized to access. This improves quality of service for the user, reduces administrative costs, and increases security.
Increase the security of the enterprise through consistent enforcement of password policy	The automated synchronization of password details for all users ensures that the organization has a consistent and effective password policy applicable at all times, reducing the risks for security to be compromised.

Table 1.2: Password management business requirements.

The Four As

We defined the four As earlier in this chapter. The first three are traditional pillars of a security solution, while audit is not often considered specifically as it can have a broader context. In the case of Identity Management, all these components are important.

Authentication

Authentication is the basic process of validating that someone or some entity is who they claim to be. This process is broken down into several methods of challenge and response:

- Something you know—Account names, customer ID number, password, PIN
- Something you have—Bank card, driver’s license, passport
- Something you are—Fingerprint, retina, DNA, signature

That process can take many forms, and may even utilize combinations of these methods. The most common authentication solution on computer systems today is account name and password based. Identity in the electronic world can be even more complex than in the real world. Electronic identities are electronic counterparts to driver’s licenses, passports, and membership cards.

Authentication may be required once or many times depending on how integrated your system or systems are. In a more real-world example, airport security in many places around the world requires that you show some proof of identity, such as a passport, several times as you move around various sections of the airport. Similarly, a computer system may “challenge” you to provide some proof several times as you move about the system to make use of applications and services.

Authorization

Authorization is the process of determining whether an identified and verified account is permitted to access resources. Authorization is generally a basic check of whether the account is active and in good standing, and is based on specific data points within an individual system.

Access Controls

Access controls are a broader set of policies within an Identity Management system that define rules around what an account holder is allowed to do within the scope of that system. This type of policy set can be far reaching and make use of data points such as time of day. Unfortunately, applying access controls can also be a complex undertaking and highly prone to error because of the lack of cross-system standards, such that administrators are required to specify access control lists (ACLs) for each user on each system individually. Identity Management solutions allow for these policies to be defined at a high level outside of specific systems, then through translation, be applied as appropriate to each individual system.

In Chapter 5, we will take a look at emerging standards around access controls. For example, a standard introduced by the National Institute of Standards and Technology (NIST at <http://csrc.nist.gov/>) known as Role Based Access Control (RBAC <http://csrc.nist.gov/rbac/>) has seen some interest, but little commercial success. As a result, most Identity Management vendors have implemented their own custom authentication and access control models.

Auditing and Reporting

For some time there has been a need for organizations to be able to log and report on all events within their organizations. This is particularly important when dealing with customers, but not exclusively so. As a result, events such as account creation, modification, and deletion need to be logged. As previously cautioned, it is equally important to be able to make these logs accessible for audit to determine exactly which events took place within your environment. This, in turn, can allow an audit to determine who has access at which level to which systems.

An Introduction to Identity Management Standards

Although we will consider the bulk and depth of the Identity Management standards in Chapter 5, many bear introduction at this stage so that we can refer to them throughout the book. If we consider that directories formed the basis for early identity solutions, Identity Management standards have been around since the early 80's. We could argue the point, but as an example, X.500 has provided a mechanism for representing identity around the world, in a replicated and secure system since 1984 and through several revisions. Although successful, especially in government and educational installations, widespread commercial success was, it can be argued, elusive. In the 1990's, the rise of LDAP heralded a requirement for and resurgence in identity solutions; however, LDAP gained only a modest acceptance in application developments and did not solve all the problems of Identity Management. As a result, numerous new efforts have been initiated to support Identity Management.

Under the auspices of Organization for the Advancement of Structured Information Standards (OASIS at <http://www.oasis-open.org/>), several efforts have found a home. OASIS is a non-profit, global consortium that drives the development, convergence, and adoption of e-business standards, including:

- SAML—The Security Access Markup Language is intended to provide a session-based security solution for authentication and authorization across disparate systems and organizations through the use of XML expressions.
- SPML—The Service Provisioning Markup Language is a proposed standard for managing the process of provisioning of accounts across disparate systems.
- XACML—The eXtensible Access Control Markup Language is an XML specification for expressing policies for information access over the Internet. XACML is intended to define the representation for rules that specify the who, what, when, and how of information access. Access control, which is often called *rights management* or *entitlement management*, determines who can look at something, what they can do with it, and the type of device they can look at it on.


- **WS-Security (Web Services Security)**—In June 2002, the original owners of WS-Security (IBM, Microsoft, and VeriSign) passed the WS-Security to OASIS. The intention of WS-Security is to provide support, integrate and unify multiple security models, mechanisms, and technologies, allowing a variety of systems to interoperate in a platform- and language-neutral manner. The WS-Security specification defines a set of standard Simple Object Access Protocol (SOAP) extensions (message headers) to allow the implementation of integrity and confidentiality in Web services applications. WS-Security provides a foundation for secure Web services, laying the groundwork for higher-level facilities such as federation, policy, and trust.

In terms of Identity Management in a large-scale effort, especially focused on Internet solutions, several efforts exist from major organizations or groups in the industry to supply various degrees of identity data and related capabilities across distributed networks, including:

- **Microsoft Passport**—Microsoft Passport is one of the largest existing identity infrastructures with a claim of more than 200 million account entries. This is an example of a monolithic and centrally controlled Identity Management solution.
- **Liberty Alliance Project**—The intention of the Liberty Alliance Project is to allow distributed or federated identity services for authentication and authorization and beyond, to allow for cross-system interaction through a single logon. Released based largely on the SAML work from OASIS, the second phase is intended to provide a more extensive solution for expressing more complex security policies between organizations, focused on levels of trust.
- **AOL's Screen Name Service**—AOL has defined a service that combines the screen name sign-ins of AOL sites (America Online, CompuServe, AOL Instant Messenger, Netscape, and NetBusiness) as well as signed partners into one unified authentication system, with a total of more than 175 million accounts.

Like many single-sign on solutions, the goal of these solutions is to eliminate the need to remember multiple names and passwords, specifically while browsing the Web. To do so, requires that data is stored and managed securely as well as being able to be securely passed between sites (or businesses).

The potential issue with AOL and Microsoft's solutions is simply the fact that the data is owned by those companies. These certainly fit with the goal of minimizing the places where information is replicated. The issue most organizations have is the loss of control over a customer's or user's data.

 As previously stated, Chapter 5 provides a more in-depth discussion about these standards and services and their implications on data management.

Legal Drivers

A significant driving force behind Identity Management projects are mandates and laws by governments around the world. Legal drivers can impact your auditing policies as well as have a broader impact on the development of standards across the world. In the United States, examples are HIPAA, which affects the privacy of individuals' identity data as related to health care, and the Gramm-Leach-Bliley Act of 1999, which is intended to protect similar data in relation to financial transactions.

In October 20, 1999 the United States Federal Trade Commission issued the final rule to implement the Children’s Online Privacy Protection Act (COPPA) of 1998. The main goal of the COPPA is to protect the privacy of children using the Internet. Publication of the rule means that, as of April 21, 2000, certain commercial Web sites must obtain parental consent before collecting, using, or disclosing personal information from children younger than age 13.

The European Data Protection Directive applies whenever personal data is processed wholly or partly by automatic means and to certain forms of manual systems. In this latter situation, the legislation will apply only where the data is held as part of a structured filing system. Interestingly, the directive notes that “The right of a data subject (individual or otherwise) to obtain access to data held concerning them—and rectification of any errors discovered therein—is one of the key elements of any data protection regime.” This is very similar to the United Kingdom Data Protection Act, which has had a longer lifetime. The United Kingdom Data Protection Act originally defined in 1984 and updated in 1998, states “The Data Protection Act requires that appropriate security measures are in place to safeguard against unauthorized or unlawful access/processing of personal data.” Canada, for example, has a number of privacy and data protection acts in the form of the Access to Information Act and the Privacy Act.

We will look at these legal drivers in more detail in Chapter 6. The point for now is that many countries have specific requirements and government enforced policies about how data is handled, especially when it is shared in any way. When dealing with consumer information, you must consider the impact of both general government policies as well as those of countries in which you do dealings. This requires significant profile management to establish enough information to ensure that you are correctly managing the data about an account according to such national laws.

In the case of the enterprise, local policies must be considered in any effort to create Identity Management solutions, in particular, if you plan to work with any outside party where you provision on behalf of employees. An example would be an organization managing the provision of cell phone service or broadband Internet access from home for employees, which often require the exchange of profile information. Internal policies might exist for how this information can be exchanged, and furthermore, privacy, legal, and compliance issues likely exist as well.

Summary

Throughout this chapter, we have discussed at a high level the concepts around Identity Management. Moving into the following chapters, we will look at specific implementations and solutions to enable the practical implementation of Identity Management solutions including the relationships between identity and single sign-on, Web-based single sign-on, PKI, USB smart tokens, keys, smart cards, biometrics, Internet and intranet security, and VPNs and gateways. In addition, through Chapter 5 and 6, we will deal with the more advanced aspects of Identity Management, including presence (status, availability, and so on), personal preferences, mobile services (location), DRM, and privacy, compliance, and legal issues.

Chapter 2: Identity Management and Security

Chapter 1 discussed the basics of Identity Management. As observed, Identity Management is not a simple off-the-shelf solution—comprised of both technology components and business strategies and policies, it is essential to research and understand the many aspects of Identity Management to provide a true Identity Management solution. That is the goal of the following chapters: to delve deeper into the components required and available to support an Identity Management initiative.

Identity Management helps meet the key security management requirements that most organizations have today. The security requirements of an enterprise that provides access to employees is different than those of an Internet-based consumer site. In the case of the enterprise, regardless of its size, it is important that there exist some record of each employee—the employee's role and access levels across systems. In the case of the consumer Internet sites, the same information exists, but it is obtained with less concern for accuracy, and the information has different attributes and contexts and may be more readily shared across other sites. In this case, there may be more reliance on validating information through credit card companies, which is something an employer generally will not utilize. Despite these differences, there is a great deal of commonality across definitions of Identity Management frameworks. In this chapter, we will evaluate how an Identity Management solution is defined within the security infrastructure of these scenarios, exploring each of the components that have a vital role in protecting a system.

Risk and Trust

When evaluating solutions that enforce security, there is always compromise. Within the security space, this compromise is considered risk management. The reason is that generally the more security you put into place, the less usable the system. In line with that consideration is the acceptance that a system has a value to the organization, which must be secured.

Often the only way to calculate the risk is to use a qualified actuarial representative—essentially a statistician who computes risks and premiums, generally for insurance policies. Given that this resource is beyond the reach or reality of most organizations, the calculations are done by internal staff as they attempt to define ROI for a project. Calculating such value is different from organization to organization, and project to project, and can involve basic concepts such as the impact of having employees unable to work overtime due to system security breaches, the potential impact of customers (for example, a boycott), or even legal action against the company. Although calculating the value of more physical considerations is fairly easy, determining the cost of service abuse relative to corporate reputation and similar intangible assets can be very difficult. The point is that as you begin to assess the value of the assets that you are trying to protect, it is important that you utilize representatives from across the organization.

Perhaps a more appropriate baseline to begin assessing risk is to ask more generic questions that can be changed as appropriate for your specific situation, along the following lines:

- How secure is my infrastructure? Is sensitive data protected if disgruntled employees gain access to restricted systems or resources?
- How secure are my connections beyond my infrastructure? Can you ensure that your high-value online transactions are binding?
- How secure are my communications within and external to my infrastructure? Are confidential emails and files protected from interception by unauthorized employees, competitors, and malicious parties?
- Is there a plan to improve security over time?
- Is security actually improving over time?
- Can I transfer risk using different solutions (for example, outsourcing)?
- How does my security compare with that of similar companies in the industry?
- How will I respond to a breach in security?

The important thing to note is that understanding the level of risk you are prepared to accept relates directly to the level of trust you have in your systems and your relationship with other organizations and their systems. This concept of trust becomes very important due to the fine line drawn between fully securing a system such that it is unusable and securing it enough such that risk is mitigated but the system can be used to actually perform the task for which it was implemented.

Beyond this matter, you need to consider impact to your company or “brand”. In the case of any organization, there is risk if untrusted parties with whom you have no legally binding or enforceable agreements gain access to confidential business data, in particular customer or employee data.

The cost of securing a system, let alone many systems and their integrated applications, can be astronomical. Consider that the more complex a security solution

- The higher the potential cost of implementation.
- The higher the potential cost of administration and maintenance.
- The more chance that services or data will be unavailable when needed and someone will not be able to do his or her job.
- The more chance that security configuration will be overlooked or someone will not be able to do his or her job.

These truths eventually increase the risks rather than decrease them. This is called the law of diminishing returns.

Identity Management solutions help increase security and minimize the risk of systems by helping manage the lifecycle of a single identity and mapping that identity across multiple systems, principally reducing complexity and cost. A project such as Identity Management that plans to manage information about people and store organizational knowledge will have many security requirements and potential restrictions. As such, you should ensure that your organization has appropriate security policies, and that you are applying the appropriate level of security to the project itself. The optimal scenario for any directory services project is to involve security as part of the core team that will deliver the directory services solution. In this way, you not only gain a representative, or team, who understands the policy and can apply it to the project but also the potential to have the policy changed if there are any issues that are not met, cannot be met, or should not be met. The involvement of security should also be tempered with full interaction with the business representatives to ensure that functionality aspects are not overlooked.

The core nature of Identity Management is to support other networked services and applications. In isolation, an Identity Management solution is useless. As a result, the focus of any security analysis requires a great deal of investigation into the ancillary services to ensure that all potential risks are identified and dealt with in the networked environment.

As we discussed, security is largely about risk management. Once you have assessed your situation, there is a traditional trio of steps to be dealt with when defining and maintaining a security solution that will deal with possible threats to a system. These steps are known as PDR:

1. **Protect**—In this step, you define your levels of security around the system and the way in which you will implement them.
2. **Detect**—Despite all the attempts you make to protect a system, there will likely be a way around it, so you need to ensure that you implement monitoring and intrusion-detection into your solution.
3. **Respond**—To avoid a panic response to a security breach and to successfully deal with breaches of security, you must ensure that there is a step-by-step approach that those involved in the process can easily follow.

These steps define the traditional high-level approach to system security. Within each of the steps are a number of focused activities. To protect a system as well as have any chance of detecting a problem with it, you must understand the system. Seems logical right? Well, unfortunately, many installations of technical solutions are done without considering the aspects of security. It is important that you create a regular review of your environment, especially during times of change.

Let's turn to the specifics of each core security component of the applications managed by an Identity Management solution. To do so, we will begin with an exploration of authentication.

Authentication

Authentication is the core concept of Identity Management. Authentication lies on the outer perimeter of a security infrastructure and can take a number of forms related to who or what is trying to gain access to the system. As you can see in Figure 2.1, most security systems traditionally use the silo approach—each application maintains “identity” information about users, their rights, and some form of control to manage access to the application.

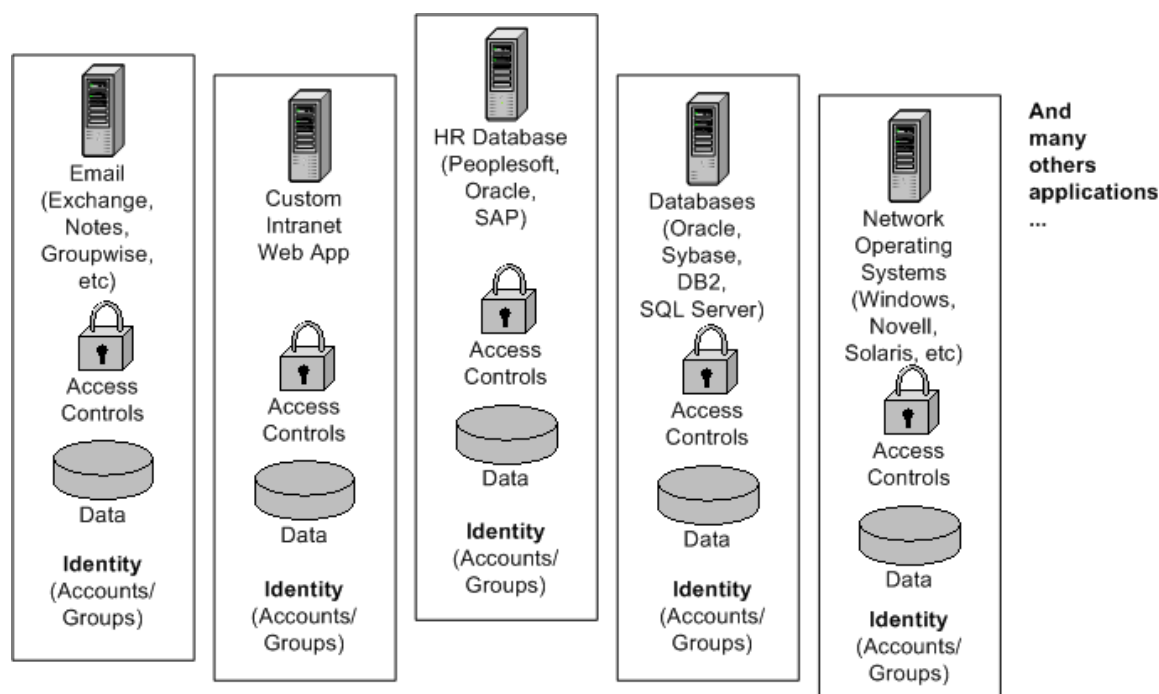


Figure 2.1: Silos of security and access information.

Authentication is the first thing that happens with any system, proving who the user is. The boundary of the system is the important thing to keep in mind as we move through this discussion.

Authentication can happen in numerous ways and requires some form of identification through the presentation of credentials to be validated by the system. At a conceptual level, authentication to a system for individuals can occur in a number of ways:

- Something you know—Traditionally, username and password, but may require the answer to specifically pre-arranged questions
- Something you have—Such as a time-based key device or token (for example, SafeNet’s iKey and RSA Security’s SecurID)
- Something you are—Considered to be primarily biometric measurements, such as retinal scans, fingerprints, and so on

Although these types of solutions are often used in specific situations due to complexity or cost or appropriateness, a system might enforce authentication to a specific service via several of the listed options. Indeed, the context of the authentication request becomes important. For example, accessing internal company resources may require simple password-based authentication from within the local network; however, when dialing in, authentication may only be possible using both the password and an additional key device control. Biometric solutions are potentially the greatest opportunity of identifying an individual; however, they are rarely be used in isolation to ensure security. For example, several vendors such as SafeNet and Digital Persona provide fingerprint scanners that act as tokens but require passwords or PINs to complete the authentication cycle. Chapter 3 will review specific implementations of vendor solutions, and Chapter 4 will cover potential issues with specific implementations. Two key drivers of Identity Management projects that deserve discussion here are password policy management and single sign-on (SSO).

Password Policy Management

Password management, which we discussed in Chapter 1, needs more explanation before we review password management applications in Chapter 3, specifically around the capability of password policy management. Password policy management is vital if that is all you are using to secure access to your network. Most enterprises enforce an account-naming standard. This common approach means that the account name is easy to derive and is therefore a minimal component of the authentication security.

That means that the password is the only real security you have. The traditional, almost comical approach to dealing with complex and multiple password management by individuals is to create a simple password that is easy to guess and/or to write down this password somewhere (for example, the ever popular sticky note on the monitor).

Password policy management becomes a significant issue without some form of top-down solution. Identity Management solutions generally provide for this type of thing, including the ability to define a consistent password policy across systems by coalescing the minimum and maximum capabilities of each system that is being managed, then providing a combination syntax and lifecycle constraints. Syntax deals with the format or composition of the password and ensures that it can be consistent across systems, using criteria including:

- Minimum and maximum password length
- Minimum and maximum alphabetic character counts
- Minimum and maximum numeric character counts
- Minimum and maximum punctuation character counts
- Exclusions (for example, specific words, variations of the account name)
- Consecutive character types
- Instances of any character
- Password uniqueness (for example, similarity check with previous passwords)
- Sequential character checking

Password Lifecycle

- Minimum and maximum days between password changes
- Password history count to enforce the number of times before the same password can be used again
- Number of failed logon attempts allowed before lockout
- Lockout duration
- Password reset questions (for example, what is your favorite color?)
- Any role-specific requirements (systems administrators have a different set of requirements than back office staff)

Remember that there are several goals to meet. Initially, the goal is to create a system in which the password-access mechanism meets a policy level that you are comfortable with such that attacks can be mitigated. Beyond this list of capabilities is the common requirement for auditing for specific events throughout the password policy management system. This requirement sounds simple but can be quite complex and is often not dealt with effectively by many systems. (This is related to the audit requirements discussed shortly.) For example, if the Identity Management system is primarily implemented to support a password management requirement, it is likely that the solution does not maintain each application access control layer OR its log collection (that is, each application is still accessed via its own UI and checks its own local security layer and reports failures to a local log). In this case, the Identity Management system may only enforce standard password changes into the local system without being able to access the applications' security logs. Thus, the Identity Management system will not identify times when local access fails causing a lockout on that system. Dependent on the solution, a SSO component would be expected to deal with the access layer at least.

In evaluating systems, you will find that some do not deal well with international characteristics on both technical and cultural levels. For example, technically some do not readily support internationalization and if they do, they have not been localized to all the countries that you may need to support. Culturally there may be preset questions that make no sense. For example, asking for the last four digits of a Social Security number makes sense only in the USA.

The key with password-based solutions is a reliance on encrypting the password in the store, securing access to that store, and ensuring that a validation request is also secured. Commonly, solutions use a hash of the password and a random challenge across the validation connection. Essentially, a system issues a challenge, the authentication service then hashes the challenge with the password and responds to the system so that it can validate the response against the stored password. There is an implicit trust in the security store, which has become standard practice within the enterprise. Moreover, since the beginning of dialup services through to fully featured Internet Service Providers (ISPs), users have trusted the providers with their password information.

There are various password authentication services available, such as

- Password Authentication Protocol—PAP is defined in Request for Comments (RFC) 1334 and is a rather simple and insecure solution that is rapidly decreasing in popularity.
- Challenge Handshake Authentication Protocol—CHAP is defined in RFC 1994 and has various derivatives; although usage of this protocol is also decreasing, CHAP still has reasonable use.
- Remote Authentication Dial-In User Service—RADIUS is a much more scalable solution, as is Terminal Access Controller Access Control System (TACACS). Both find their existence in dial-up solutions, especially in ISP environments.

Although it is unlikely that an SSO solution would support these protocols on the front-end (that is, for the initial authentication), there may be a requirement to support them against back-end systems.

SSO and Related Solutions

It is important at this stage to consider the desire for SSO as it is the basis for many of the Identity Management projects. Most businesses today are still attempting to implement some form of SSO, which is not a simple undertaking.

Surprisingly for many companies, employees trying to be productive in their daily work waste a huge amount of time in just such a state because of the new productivity services and systems being introduced that utilize separate user and security services from those already existing. Many employees spend large amounts of time obtaining access to services and applications. A number of studies exist around what the costs are associated with the silo approach to applications in today's businesses.

Studies suggest that the average user spends as much as 44 hours per year performing logon tasks. That is just over a week's effort for average employees, and given that it represents the time of only one employee, the problem is grossly inefficient when correlated across the number of employees in an average organization. Given an organization of more than 50 employees in this situation, a year's worth of productivity is lost just through access controls. Of course, there is always going to be time spent authenticating to systems; however, the promise of a SSO solution would cut down on such waste—based on the study numbers, the wasted time would be cut by a factor of four.

Similar issues exist for commercial Internet solutions, whereby a user is forced to manage numerous user names and passwords for different sites. In addition, users are often forced to re-enter credit card details and similar information to enable them to conduct business on those sites. A single solution to enable customers to move from site to site and continue to conduct business without having to bother with usernames and passwords is compelling to most commercial operators.

In this arena is where the potential of SSO begins to show. The combination of maintaining a single identifier and related password that allows access to multiple resources is powerful. There is also the factor that SSO helps in minimizing the need to remember multiple account names and related password and thus the security risks that occur when users are forced to write down that information in order to remember it.

As we begin to look at SSO, you should also note that whilst previous security risks are minimized, new risks become more prominent and need to be dealt with through a thorough review with your security group. The primary risk that is increased is the fact that there is now a single gate or access mechanism that needs to be broken to gain access to resources. Mitigation of this risk and other risks is discussed in the implementation discussion later in this chapter. However, to give a basic example, consider how you use Automated Teller Machines (ATM). To gain access to your account, you are required to present your card to the machine, which then prompts you for your PIN. This security solution is when dealing with simple account/password issues. By adding the requirement that the person accessing the system actually hold something physically, there is a combined protection mechanism.

SSO is also a common solution for remote access. Often remote access solutions are more complex than the simple scenario we painted for ATM access, employing smart cards or tokens such as iKey and SecurID, but also utilizing intelligence in the card or token itself. You might already use such solutions in your work, for example, if you use your building security pass not just to get into your office but also to access to your computer or your office remotely. Of course, if you forget your badge, this solution seems a little limiting.

SSO Basics

Each application requires a different logon account and password, and is generally managed through a separate administration interface. Effort is spent by each staff member in recalling this information, actually entering the logon information into each system, correcting mistakes, and attempting to maintain some sort of synchronicity between those systems. As a result, rather than matching a security desire for complex secure passwords, users are forced into trying to short-circuit the requirement by trying to select easy-to-remember passwords. Worse still, when mechanisms are installed to enforce secure password selection, users generally resort to using notes taped to the side of their computer screen listing the accounts and passwords they use. Doing so breaks multiple security tenets and makes the organization vulnerable to costly security breaches from both internal and visiting persons.

The same is true for administrators who must configure application services to utilize multiple security services to operate. The potential of an SSO solution is to allow for a comprehensive foundation to support enterprise-wide access for users to infrastructure services, while at the same time, enhancing the ability to provide *n-tier application solutions*. Although many are familiar with the client/server as a 2-tier architecture, many applications go well beyond this setup with many possible services and proxies, or additional tiers, between the user and an actual server or service the user wants to use. The importance of Identity Management is to ensure as much as possible that the right account and access information is in the right place across such architectures. This solution is possible by creating an environment in which all security and policy information is related through standards to a directory-based infrastructure supporting multiple clients, servers, applications, and services. Further, through a proper Identity Management solution, the administration of that account is much simpler when issues do arise. The costs of support for forgotten passwords can be immense, although hidden. Recent studies suggest that almost half of all service or Help desk calls are related to password or account lockout issues, and cost an average of \$80 each.

A number of products offer the promise of single logon. In the common security schemes, an identifier, such as user or application name, and a password is used to authenticate to a system. The reality of most SSO solutions today is that they offer a synchronization of user names and passwords across a defined group of systems.

A true SSO solution requires that all applications and systems stipulate a single source for security services. This includes the commonly referred to services of authentication, authorization, encryption, connectivity, and management. This is an extremely tall order for many application developers. Realistically, such a solution will not happen in the near future; however, by enforcing and representing such a model internally, vendors will be coerced into supporting such centralized services.

A common security threat to organizations occurs when users are given too many identifiers and passwords to remember—they often find the only way to retain the combinations is to write them down somewhere. As I have mentioned more than once, this occurrence is a significant security risk and provides one of the soft benefits for an Identity Management solution and related SSO requirements. Although you could place a value on some of the information, until there is an actual breach of security, many companies are not considering their exposure in these situations.

As I have previously mentioned, an SSO solution creates a potential security risk because it sets up a single point of entry relating to security. By having only one gate to guard, an organization might feel that it has less of a security risk. Such is not the case. What it means is that an organization can now dedicate its security resources to dealing with more complex problems rather than worrying about the yellow sticky note syndrome.

One of the many duties that engage administration staff is in defining and implementing security policies. In defining an SSO service, the obvious benefit is for the end user or client of the service. There is, however, cost savings to be gained through a comprehensive implementation of the SSO security model across a wide heterogeneous environment. The simpler and more standardized security model makes the administration model simpler and more consistent for administrators. More time can be spent on correctly defining policy and procedure than is spent on dealing with system limitations across multiple application and security environments.

Another common approach to SSO as well as the integration of policy controls is to utilize an enterprise security administration product such as IBM's Tivoli and Computer Associates' Unicenter. Such applications allow an organization to coalesce their various platforms and applications into a single managed interface, define rules to be applied across the enterprise, then distribute administration to selected staff in charge of application security.

The issue of a common mechanism to define and manage access control across systems and solutions is a long way from being solved. As a result, there will be, in the meantime, a need to utilize the best of breed solutions to implement SSO across existing platforms. In the short term, it is unlikely that there will be an enterprise-wide solution for SSO that works across legacy platforms as well as the new environments being introduced. This is protracted by the fact that many common application vendors are still waiting for a standard to emerge in order to implement their common sign-on solutions. Large-scale enterprise planning should look for solutions that minimize the number of logon identifiers and passwords that a user has.

In the early 1990's the Distributed Common Environment (DCE) received quite a lot of attention, and one of its offerings included a common security infrastructure. Despite the level of effort that went into engineering the solution, it did not gain the market penetration that IBM had hoped for. It is still around today in a number of large installations. Out of this effort, came an appreciation of work done on solutions such as Kerberos, SAML, and beyond. We discuss these solutions in detail in Chapter 5; however, for now organizations might want to push vendors into using this type of solution for an SSO environment.

Figure 2.2 shows the standard way in which a user signs onto a network operating system (NOS) to access other applications supported by that NOS.

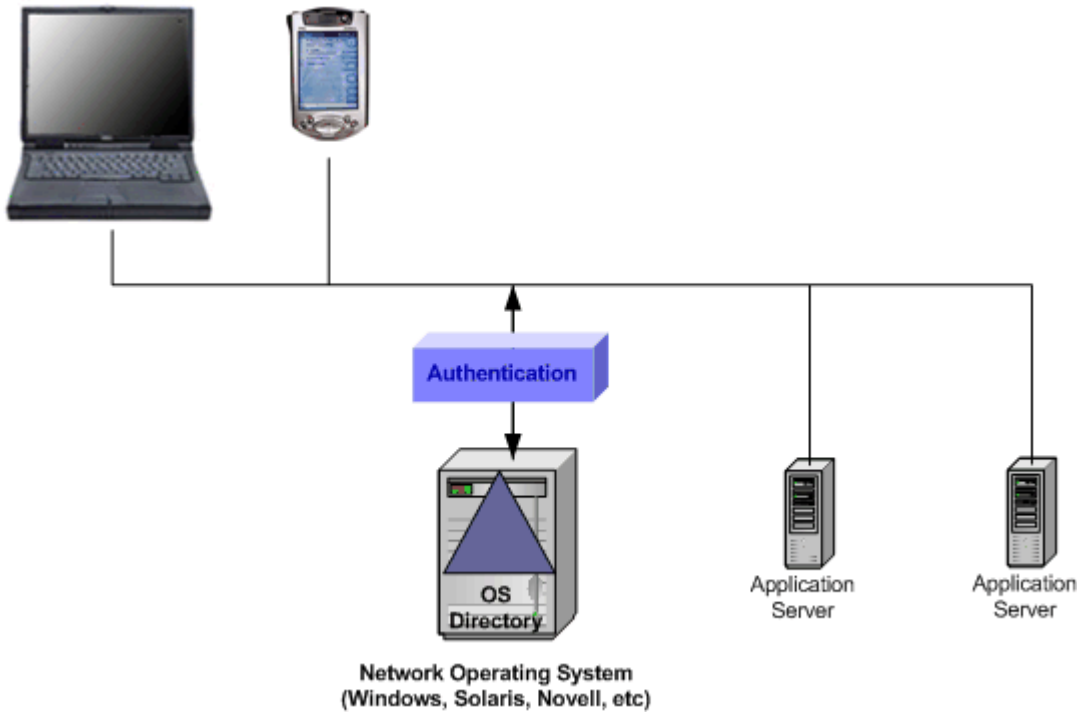


Figure 2.2: A NOS-based SSO solution.

Figure 2.3 shows a Web-based access control solution in which the Web-based authentication manager (WAM) authenticates users or defers authentication to a directory (or other source) and enables a session for multiple, heterogeneous applications.

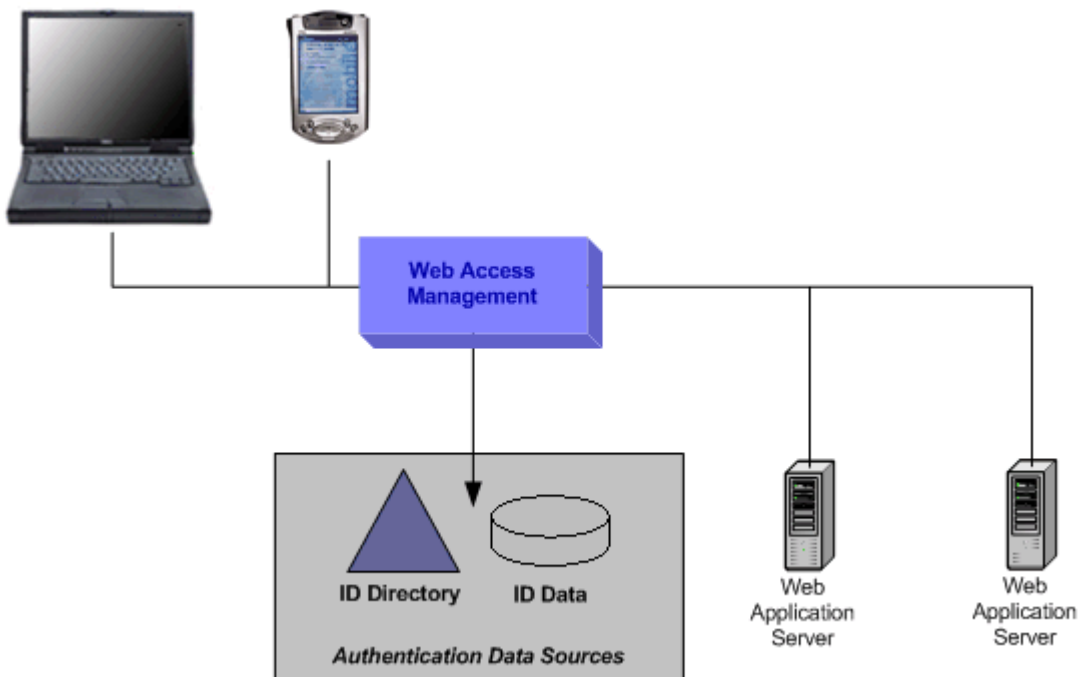


Figure 2.3: Web-based access manager SSO.

Figure 2.4 shows how enterprise SSO tools manage SSO.

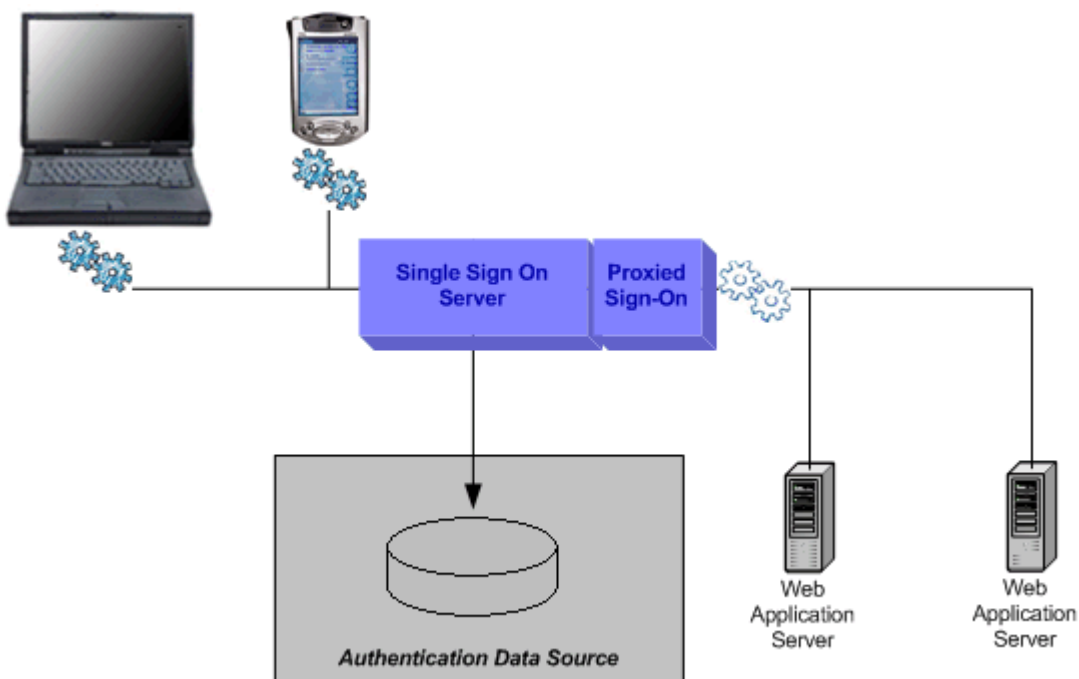


Figure 2.4: Enterprise SSO tools.

Although such solutions are popular, there are a number of issues:

- SSO tools require a “secret store” (encrypted, we hope) for passwords or other credentials in the network
- SSO tools require plug-ins in the applications to support pass-through authentication
- Can result in complex, proprietary solutions that few enterprises have deployed broadly

Figure 2.5 shows a client-side SSO solution that relies on proxy based sign-on.

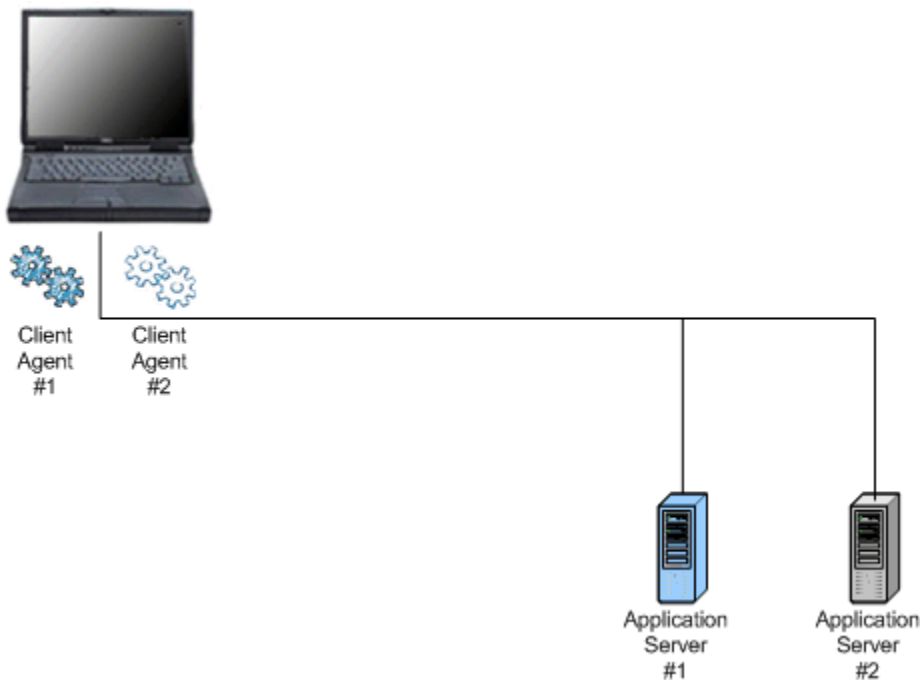


Figure 2.5: Client-side SSO.

Using client-side password capture software, the client program proxies user sign-on to NOSs, mainframes, and client/server applications. The considerations for this scenario are that it

- Requires a “secret store” for credentials on the client
- Requires significant scripting to implement
- Is best used in low-security situations or combined with stringent desktop security measures

Figure 2.6 shows a password synchronization solution.

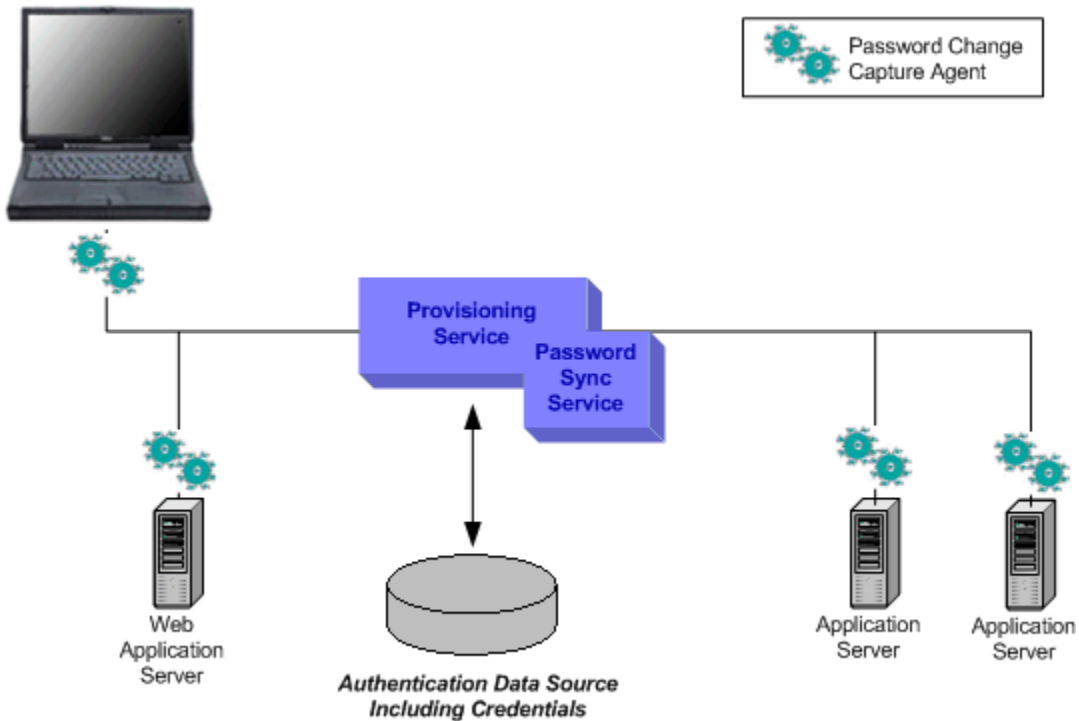


Figure 2.6: Password synchronization option.

The scenario illustrated in Figure 2.6 shows a password synchronization solution that provides a relatively transparent user experience wherein passwords created in any supported system are propagated to others. This is sometimes a custom project or dedicated software solution with the following issues:

- Password sync requires a “secret store” and plug-ins to supported systems
- Often unable to manage a consistent password policy across applications.

A similar solution is provided through password reset tools (see Figure 2.7), which propagate password changes made at a Web interface to supported systems. These solutions can manage password recovery, history, and expiration consistently. The only downside to this scenario is that users must be trained to use the password reset interface.

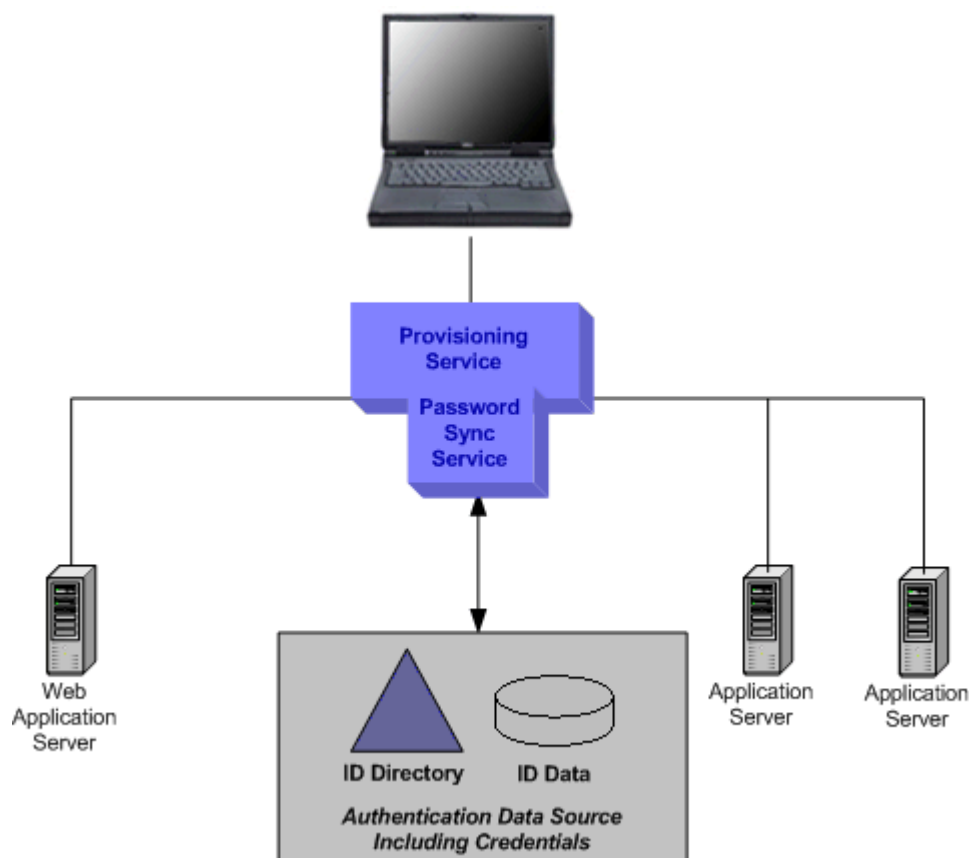



Figure 2.7: Password synchronization option 2.

The best alternative to this scenario is a meta-directory that can allow for the rules and policies to be easily defined within the provisioning system space. Given that all of these options are available, the choice of which solution to implement can be confusion. However, keep in mind that the goal is to create the right solution for your organization.

 Chapter 4 is about implementing Identity Management, and I will cover the methods to get to the right solution in more detail then.

Understanding these options is important in respect to understanding where the enforcement is done within your environment. In most of the examples provided, you will find that individual systems are still making authentication and authorization decisions within their own scope. This idea leads directly to understanding policy evaluation, and what it means to an Identity Management solution.

Policy Evaluation

It is important to understand where your Identity Management system will evaluate and enforce security policies within your system. The quicker you can evaluate the identity of who is trying to gain access to the system and determine the level of access allowable, if any, the quicker you can exclude that request from chewing up resources in the system. If enforcement can ensure that only valid access is gained at the authorization layer, the system will not expend extra effort. Another dimension to consider is how often credentials and access needs to be re-evaluated.

To improve performance of many systems, there is usually a policy to define how often the validity of authentication needs to be evaluated, and potentially for the user to be challenged again. Sometimes this is after a period of inactivity, but in highly secure environments, there is a need to ensure that the account used for access is still valid.

Access Control

Managing the means of access as well as providing clear capabilities based on attributes assigned to an individual or account is known as role based access control (RBAC). There are several fairly new standards to choose from, however, there are minimal implementations or compatibility with the standards to really make them useful. The National Institute of Standards and Technology (NIST) offers an RBAC reference model and The Organization for the Advancement of Structured Information Standards (OASIS) offers eXtensible Access Control Markup Language (XACML), an XML specification for expressing policies for information access over the Internet.

It is also important to note that few identity management players support a complete RBAC solution. The primary issue is that unlike a simple authentication model specific to an application, RBAC requires significant effort up front to design a model that works for an environment that is specific but flexible enough for an organization to live with. This can create significant changes to how an organization functions.

The initial goal of an organization is to deliver some form of a delegated administration capability. If you plan to deliver this, you must consider the ROI of creating a real RBAC solution. Chapter 4 will discuss the ROI of Identity Management including RBAC.

The NIST core RBAC offers a good overview of what is desired in an RBAC solution at <http://csrc.nist.gov/publications/nistbul/cs195-12.txt>. The NIST component defines five basic data elements:

- Users
- Roles
- Permissions
- Objects
- Operations

The whole model is defined in terms of individual users and permissions being assigned to roles. Within an Identity Management solution, these objects can be considered as follows:

- Users—An entity that uses the system
- Roles—A job function within the context of an organization
- Permissions—Approval to perform an operation on one or more objects.
- Object—Can be many things; for example, an entry in a target system (such as an account), a network resource (a printer), an application (a procurement), a policy (password policies), and so on
- Operations—Various and unbounded but including customer-defined workflow processes such as a password reset, the addition, modification, or removal (deletion) of user accounts, and specific data about those accounts; importantly, it should be possible to delegate these operations to other users

Delegated administration allows a chain of approvers to be identified to securely delegate capabilities (even roles) such as account provisioning to appropriate parties in the environment. Delegated administration allows the offloading of the responsibility for user management to those who know their users best, increasing administrative efficiencies and reducing the level of staff required at the central site. If an administrator has a delegable right on a user profile, he or she should be able to delegate that authority to another administrator. Similarly, the ultimate in delegated administration is to allow individual users to perform certain administrative tasks on their own accounts, the most finite example being password management. Delegated administration makes it possible to

- Decentralize administration by breaking down responsibilities among administrators by geographic location or area of expertise (account creation, password management, security, and so on).
- Delegation of responsibilities to authorized users (managers) who are best suited to assign and monitor the responsibilities of the users that they work with.

In general, when looking at Identity Management solutions, it should be possible to delegate all permissions, including the ability to

- View, create, modify, and delete users
- Change passwords
- Add or delete a user in a security group
- Approve or reject requests

Hierarchical RBAC

Hierarchical RBAC requires the support of role hierarchies, whereby senior roles acquire the permissions of their juniors, and junior roles acquire the user membership of their seniors. The NIST standard recognizes two types of role hierarchies.

- General Hierarchical RBAC—Arbitrary orders and relationships between roles serve as the role hierarchy.
- Limited Hierarchical RBAC—Restrictions are placed on the role hierarchy. Typically hierarchies are limited to simple structures such as trees or inverted trees.

Although General Hierarchical RBAC introduces potential problems of hierarchy loop detection and/or prevention, it is seen as the most useful.

In an RBAC solution, consider that occupants of the same roles at different locations in an organization will need access to different underlying systems. This allows the same role (for example, Development Engineer) to be given access to different systems based on differing values in the role occupant's profile. So while all development engineers need access to source control, it is likely that those in one office or working on one product may need access to a different source control system from those in another office or working on a different project. To solve this problem, a parameterized permission object can be used. A single permission Source Control Access might be used. However the mappings from that object into the connected systems (that is, source control systems) would vary based on a user's location attribute or on the project attribute.

The alternative to parameterized roles is to use scoped roles. In this approach, the roles are defined with a direct scope. If we consider our previous example, instead of having a single role of Development Engineer, there would be locally scoped versions of this role (for example, Application Development Engineer and Interface Development Engineer), and these locally scoped roles would be linked to locally scoped permission objects (for example, Application Source Control Access and Interface Source Control Access).

The tradeoff between the two schemes is that in the scoped roles model there will be more roles to be defined whereas the parameterized roles model has fewer roles but is more complex to develop and potentially more complex to administer (depending on how good the provided administrative tools are). It is worth noting that the two models are not mutually exclusive. That is, both can be supported at the same time and used in a complementary fashion. Also, there are no functional limitations associated with either model—both can be used to get the job done. So, when evaluating options, obviously focus on what best fits with your requirements.

Auditing

Reporting and audit controls are an important part of Identity Management. For example, HIPAA, discussed in Chapter 1, requires organizations that deal with personal data to track all access to that data. Thus, not only does a record need to be made of each access to a record system but also any data transfer, change, and deletion. Financial Services requires tracking and produces information that can be considered for forensic research.

Forensics

Forensics is the next step following auditing, wherein once something has been audited, there may be a need to dig deeper and potentially recover or reproduce events as they happened across systems. Identity Management solutions can compound the problems that they were intended to solve unless careful thought is put into the requirements of the system and the specifications. There is an expectation that once a system goes in that it will be able to consolidate and view activities across the applications it manages. This collides with the goals of monitoring solutions and a recent crowd of solutions with the goal of providing intrusion detection.

Identity Management solutions can only help if they are able to extract and divine operational information about various activities through audit and reporting capabilities. Aside from that, forensic data collection must span all relevant boundaries, especially in cases of federated identity.

Accounting

A final component of security is accounting. When charges are made based on access to resources, usually in commercial environments such as ISPs, ASPs, and so on, a mechanism is required that can track usage and feed that into some form of billing database. This type of requirement fades in and out in many enterprises who decide to charge-back internal system usage to cost centers or business departments in order to effectively manage costs. This should be a separate database from the audit reporting.

Billing records may be generated on the fly or may be derived from provisioning and usage information. It is important to maintain a consistent method for achieving billing for customer records and dispute resolution, as well as any audit requirements.

Policy Management and Enforcement

Moving on from authentication, authorization, and access controls there is the issue of how these requirements are enforced throughout the system. Consider a system as a large office building. Access is granted at the front door based on an employee badge. Assume for the moment that the employee is who they say they are. What happens if the employee quits or is let go, and the employee card is not taken away? Does that ex-employee still have access to the building? Can the ex-employee still get into the building? What can the employee get access to while in the building?

Privacy

Within commercial enterprises, there is a significant contention between the desire for personalization and privacy. For example, consider portals such as Yahoo, AOL, and so on. To provide any degree of customization based on desires of the individual requires that preferences and personal information be stored. The trouble with maintaining that information is that it may be potentially traded with other parties.


Although the government may change the levels of compliance required over time, the HIPAA privacy regulations are in effect April 14, 2003. HIPAA is a good requirement to systematically analyze because it provides a key example of legal regulation in place to protect specific customer's data—in this case, for healthcare patients. In addition, HIPAA has a broad-reaching effect to any organization that might have a need, or obligation, to have access to such customer data. HIPAA requires that protected health information be neither used nor disclosed without permission of the individual customer, except for healthcare treatment and payment and when required by the healthcare operations of a group health plan.

The issue of trust is key in understanding why HIPAA came into being. Because access to healthcare data has become available through electronic systems and the security around that data was inconsistent to the point of causing harm to consumers, the government stepped in to provide a legal framework for that protection, in effect forcing a trust model into the healthcare industry in the USA.

The importance of the government regulation is an example that if organizations begin to share customer or employee data without managing the compliance issues in some way, either technically or manually, then the governments will step in. In fact, there may in some regulation cases already in place bent toward supporting or confining the exchange of user data inter- or even intra-organizationally in many countries.

Federation and Federated Identity

The concept of federation is used when disconnected systems or enterprises need to interoperate with each other's concepts of identity. This has become a more specific use case for the concept of creating secure extranets. But what is federation? The Burton Group in August 2002 provided the following definition "Federated Identity Management [is] the use of agreements, standards, and technologies to make identity and entitlements portable across autonomous identity domains." The goal of federation is to enable transparent and secure exchange of identity information to enable disparate systems to interoperate at the security level.

 Federation creates risk. Federation requires breaks in the organizational border and can diminish any content control you may have in order to facilitate the movement of identity data across those boundaries. This requires that policies be strenuously defined outside the traditional technical bounds, and legal and compliance issues be carefully addressed.

The obvious extension to what we might consider an enterprise solution to a truly federated solution is the need to work across disparate enterprise domains (as opposed to the Windows domain concept). The reality is that the cross-enterprise concept or “solution” is still evolving. The issue with federated identity is that this type of thing has been tried before with varying degrees of success. Why is this “federated identity” thing any different? History shows that very tightly defined solutions (that is, tightly coupled systems) have some success but are either not very flexible or not very simple or are too simple. As the industry works through the convergence issues, the loose links established so far will help enable flexible solutions to evolve.

The first example of this that has drawn a number of vendors together on the same road is the Liberty Alliance. According to the Liberty Alliance (Liberty Architecture Overview V1.0, 11 July 2002):

The Internet is now a prime vehicle for business, community, and personal interactions. The notion of identity is the crucial component of this vehicle. Today, one’s identity on the Internet is fragmented across various identity providers—employers, Internal portals, various communities, and business services. This fragmentation yields isolated, high-friction, one-to-one customer-to-business relationships and experiences.

Federated network identity is the key to reducing this friction and realizing new business taxonomies and opportunities, coupled with new economies of scale. In this new world of federated commerce, a user’s online identity, personal profile, personalized online configurations, buying habits and history, and shopping preferences will be administered by the user and securely shared with the organizations of the user’s choosing. A federated network identity model will ensure that critical private information is used by appropriate parties.

The key thing to realize about federation and the way in which the standards are evolving is that there is still a considerable amount of work that needs to happen “out of band.” The out-of-band requirements are essentially the agreements that are set up ahead of time around a specific goal and physically signed and executed to ensure that there are resolution processes in place should something unacceptable happen during federated interactions. For example, what if account data, such as spending limit, is not updated by one partner in the process, which causes a financial loss to another party, who allows a purchase to be made or a service to be used based on that out of date information. Who is responsible? This is not something dealt with by current standards such as SAML.

SAML uses the communications defined through Simple Object Access Protocol (SOAP) and XML to exchange authentication and authorization assertion tokens between domains. In a general sense, domain A can undertake an authentication and assign that user rights within its own system. From that, domain A may assert to another domain what it has done. In this case, domain B might be willing to accept that assertion and allow certain actions to take place for the user within its own environment. For example, an online travel agent can assert that a person has authenticated with them and has bought a ticket. An airline may take this assertion and derive that the user has rights within its own system to perform some actions, such as pick a seat. Essentially this is a variation of SSO, in a federated model. This is the basis of the work done by the Liberty Alliance Project.

The level of success that Liberty and similar alliances may have is based on concepts we discussed at the beginning of this chapter: trust and risk. How much do you trust the assertion being provided and what or how much are you willing to risk based on that assertion?

Industry groups such as credit card companies deal with this type of situation by setting up a framework defining standards and principles within which “members” operate. Importantly, this includes resolution processes in the event of some failure. For federation, this type of activity is the goal of the PingID Network (<http://www.pingid.com/>).



The goal of the PingID Network is that members instantly benefit from access to standardized business operating rules and regulations, privacy policies, and dispute resolution procedures.

Summary

Chapter 2 introduced the remaining concepts that you need to be familiar with Identity Management solutions. As stated at the beginning of Chapter 1, the goal was to define the concepts and terms used in the field of Identity Management, and this has continued through this chapter. The importance of this is to ensure that before introducing the bulk of the technical solutions and standards available for Identity Management solutions, a common vocabulary is understood.

This foundation sets the groundwork for the review of Identity Management applications in Chapter 3. Remember that some of the concepts, and more importantly standards, are still being formulated, so applications that claim they offer certain functionality deserve close scrutiny if you plan to rely on and deploy them.

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 led 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	Oracle9iAS 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 role-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.

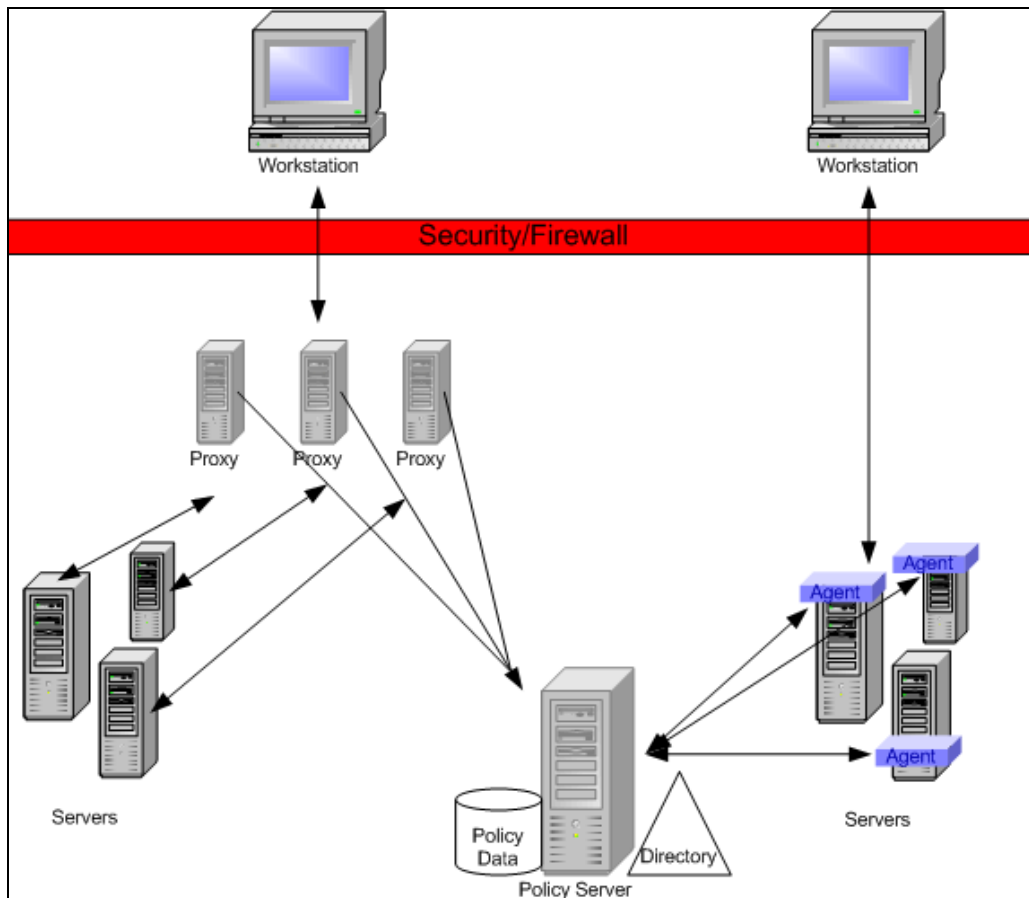


Figure 3.1: Agent and proxy-based Web access models.

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 of 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.

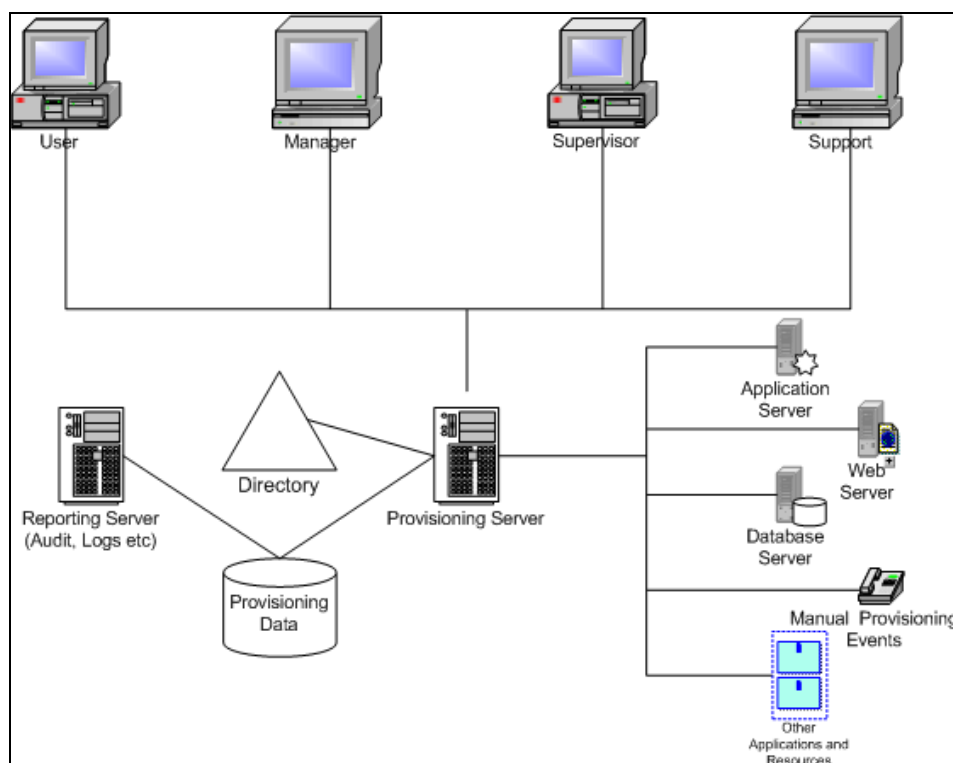



Figure 3.2: Typical provisioning architecture.

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.

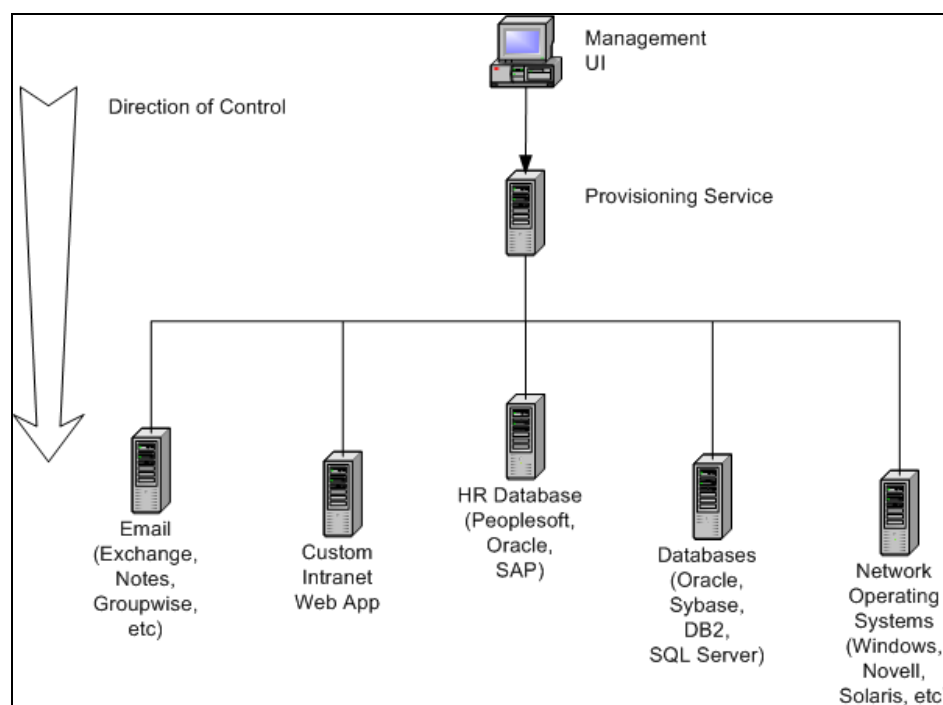


Figure 3.3: Provisioning top down solutions.

Figure 3.4 illustrates managed matrix solutions.

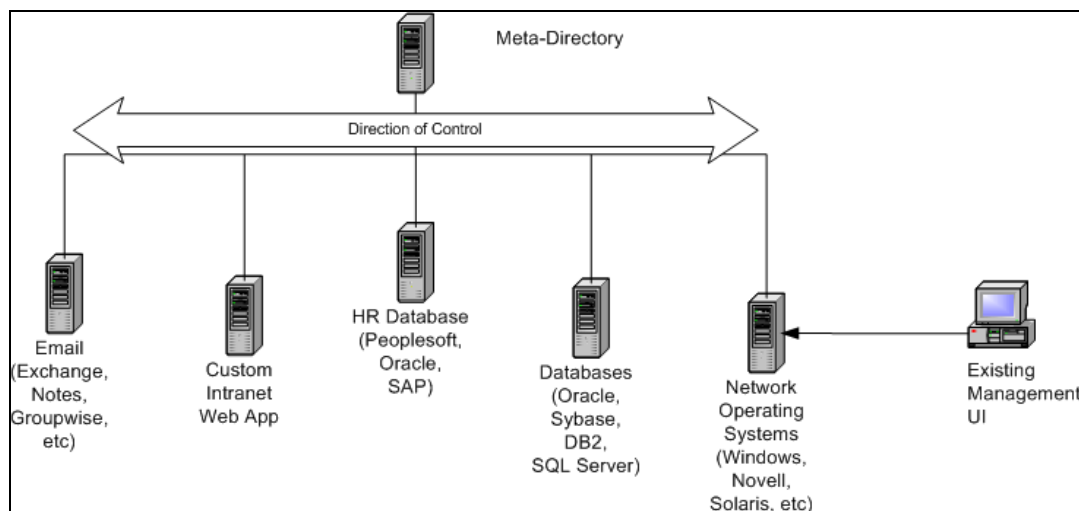


Figure 3.4: Meta-directory managed matrix solutions.

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.

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.

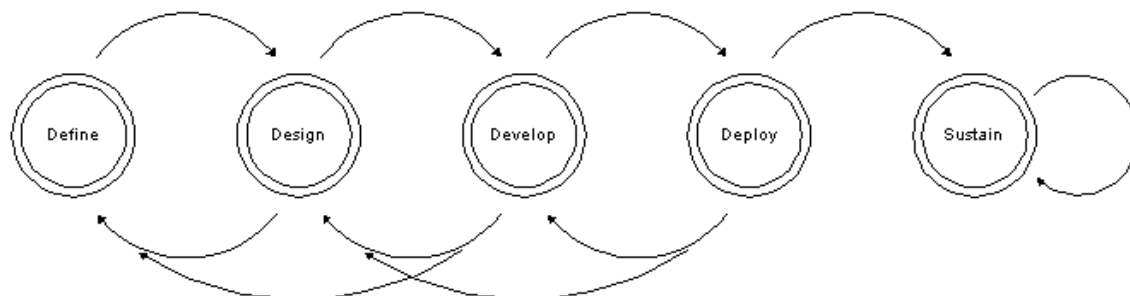


Figure 4.1: The 4DS project-planning methodology life cycle.


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.

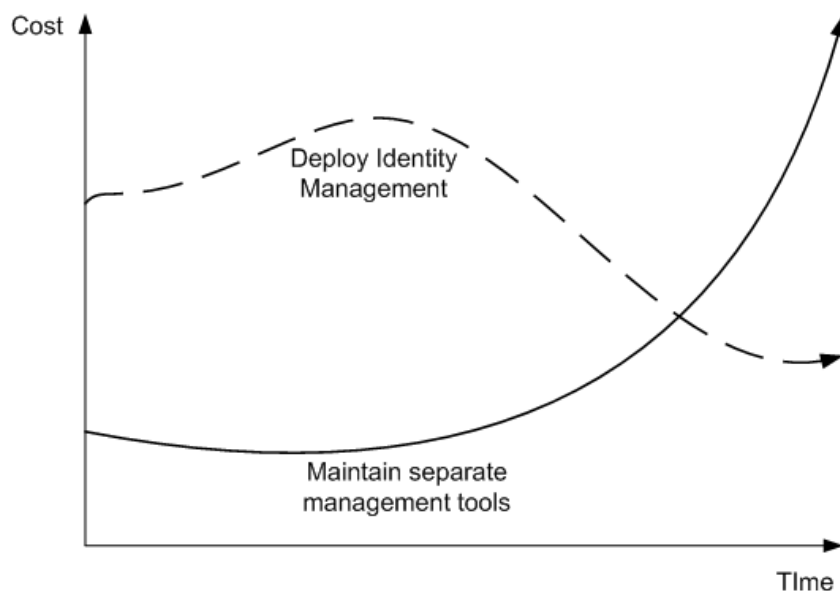


Figure 4.2: An illustration of the Impact of deployment costs over time.

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.

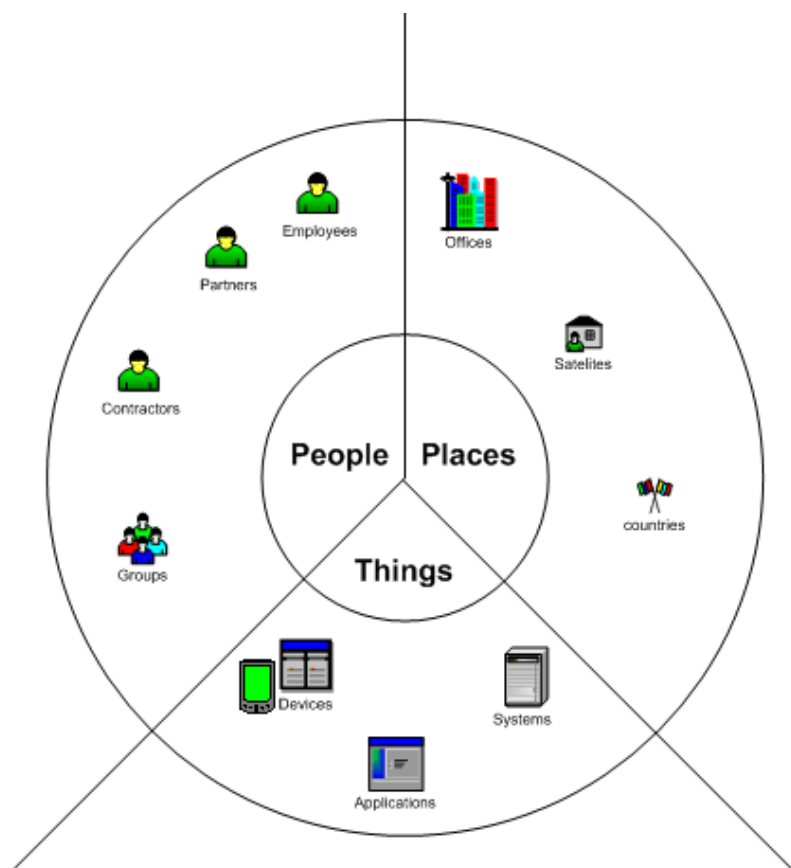



Figure 4.3: Systems, services, and data in the Identity Management solution.

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.

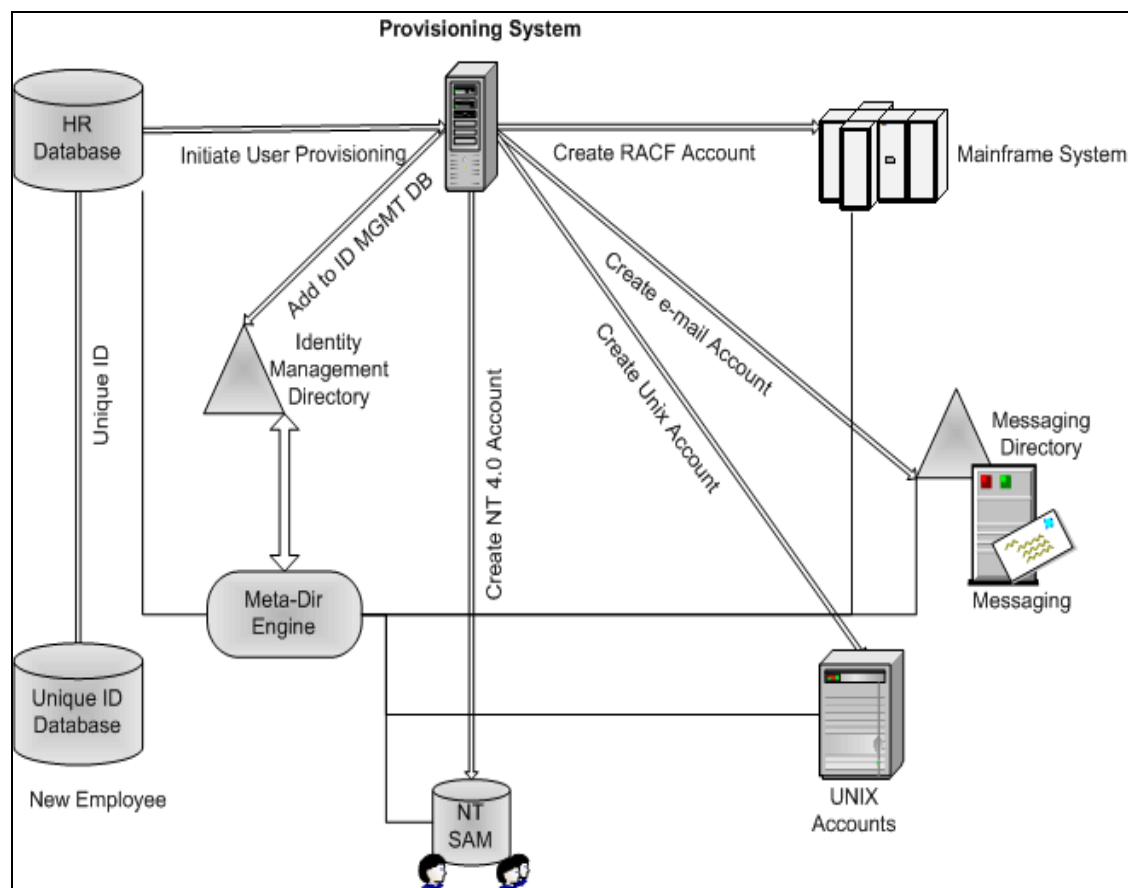


Figure 4.4: Identity namespace processing illustration.

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.

Chapter 5: Identity Management Standards

Chapter 1 provided an introduction to Identity Management standards—this chapter delves into the fundamental Identity Management standards that you should evaluate as you define your requirements for and plan an Identity Management implementation. As with many areas of focus, a significant amount of effort by many individuals and organizations has been devoted to defining and implementing standards around Identity Management. Standards defined by recognized groups and authorities provide key levels of interoperability and might be formally published and mandated or adopted through common use.

Although there has been an undue amount of duplication as well as contention between the standards bodies that are creating potentially proprietary solutions, this behavior appears to be diminishing. There is increased participation from organizations that actually use the resulting solutions as opposed to vendors who need to solve a specific interoperability problem.

The goal throughout this chapter is to determine which standards solve the challenges of your environment and are well supported. Let's begin by exploring the relevant standards bodies.

Relevant Standards Bodies

Over time, the dynamics of the following standards bodies might change, with equal potential for mergers or splits and new organizations being formed. Table 5.1 details the roles and responsibilities of each organization according to its own definitions as well as the key standards they “own” or “develop” as they relate to Identity Management.

A majority of the organizations listed here maintain some relationship to the concept of Web services. Therefore, following this standards organization review, we will discuss the key Web services model as it applies to Identity Management, then review the details of the key Identity Management standards that were referenced.

Standards Body	Role and Responsibilities
The Organization for the Advancement of Structured Information Standards (OASIS) at http://www.oasis-open.org/	OASIS is a private worldwide organization focused primarily on XML-based standards. A non-profit organization that has a large membership and has driven a number of popular and essential standards, including: Security Assertion Markup Language (SAML), eXtensible Access Control Markup Language (XACML), Directory Services Markup Language (DSML), and Service Provisioning Markup Language (SPML).
Web Services Interoperability (WS-I) at http://www.ws-i.org/	WS-I states that it is “an open, industry organization chartered to promote Web services interoperability across platforms, operating systems, and programming languages.” The key standard managed by WS-I is the Simple Object Access Protocol (SOAP).
The World Wide Web Consortium (W3C) at http://www.w3.org/	W3C is responsible for the Web Services Description Language (WSDL) specification.
Internet Engineering Task Force (IETF) at http://www.ietf.org/	IETF is a loose affiliate of individuals and organizations aimed at defining, maintaining, and evolving standards to support the Internet. The IETF is not a traditional standards organization, although many specifications produced become standards. Of particular interest to identity management-related activities is the Lightweight Directory Access Protocol (LDAP) standard.
The Open Group at http://www.opengroup.org/	The Open Group sponsors several sub-groups for identity management-related activities. Beyond the messaging and the mobile management forums are those relevant to identity management: the Directory Interoperability Forum (DIF) and the Security Forum (SF).

<p>National Institute of Standards and Technology (NIST) at http://csrc.nist.gov/</p>	<p>NIST is responsible for a wide variety of activities; specifically related to identity management are the Cryptographic Standards and Applications and Security Research/Emerging Technologies - Authorization Management and Advanced Access Control Models (AM&AACM). The NIST RBAC model is recognized as being one of the few standards initiatives of its type. A related standard around biometrics known as the Common Biometric Exchange File Format (CBEFF) is managed by the NIST Information Technology Laboratory (ITL) in conjunction primarily with the US National Security Agency (NSA) amongst other bodies. Derived and incorporating several biometric standards efforts.</p>
<p>International Standards Organization (ISO) at http://www.iso.ch/ and ITU Telecommunication Standardization Sector (ITU-T) at http://www.itu.int/ITU-T/</p>	<p>ISO is responsible for many standards worldwide as it is a standards network for 145 countries. The technical work of ISO is highly decentralized and based in more than 2800 technical committees, subcommittees, and working groups that have already published more than 12,000 standards. In relation to identity management, ISO with the ITU-T is well known for the X.xxx-based standards. Of particular interest to the identity management market are the X.500 through X.586 directory-related standards. Most PKI implementations rely on the X.509 standard.</p>
<p>The BioAPI Consortium at http://www.bioapi.org/</p>	<p>The BioAPI Consortium was formed in 1998. The most prevalent biometric standard outside governments is the BioAPI, which defines an open API for developers to integrate with biometric mechanisms in a standard way.</p>

Table 5.1: Standards bodies relevant to Identity Management.

Directory Services

Considered the core of most Identity Management solutions, directory services enable many of the previously listed standards. The key standards are X.500 and related standards, LDAP, and DSML. Although X.500 remains popular in large global organizations, government, and educational environments, LDAP remains the core for most Identity Management solutions that rely on directory services. There are many places to review the X.500 Directory, X.509 Public Key Infrastructure (PKI), and LDAP standards, but fewer resources available regarding DSML.

DSML

Originally defined in 1999, DSML v1 defined an XML-based document type for publishing directory schemas and exchanging directory data over any transport protocol. Unfortunately, DSML v1 did not find much success as it competed with LDAP Data Interchange Format (LDIF), a widely understood and widely adopted protocol. In addition, DSML v1 didn't offer any advances in functionality or suitability. However, accessing LDAP directories through firewalls and within secure environments has proved a limiting factor in directory deployments.

Despite the lukewarm adoption of DSML v1, version 2 was developed by OASIS and approved as a standard in May 2002. DSML v2 addresses most of the deficiencies of the first version and maps LDAP v3 operations to SOAP schemas. As a result, there is now explicit support for transports such as HyperText Transfer Protocol (HTTP), which for the time being allows for directories to be more easily accessed through secure firewalls.

However, even now, version 2 has seen little market momentum. Because of the lack of security inherent in the protocol, vendors have been slow to adopt this new standard. Therefore, in spite of the DSML and XML relationship, DSML appears stalled while other Identity Management-related standards have gained popularity.

Web Services

Web services are a business service provided by a software component and accessed through standard protocols and over public and/or private networks. The goal of Web services is to provide for loosely coupled communication between heterogeneous platforms, applications, and systems as well as allow for the dynamic assembly of new applications and services. For example, Web services help to enable the following types of data and process integration scenarios:

- Stock quotes and stock charting
- Credit card verification and payment processing
- Integrated travel planning
- Request for Quote (RFQ), bid process, auctions
- Moving data for a federated Identity Management solution

Table 5.2 provides a guide to the core Web services standards that relate to Identity Management from a protocol standpoint.

Area	Standard
Universal Data Format (UDF)	XML
Transport	HTTP(S)
Network	TCP/IP
Service invocation	SOAP
Service descriptions	Web Services Description Language (WSDL)
Publish and find services	Universal Description, Discovery and Integration (UDDI)
Authentication and authorization	SAML
Access controls	XACML
Provisioning	SPML
Web Services Security	WS-Security (WSS)

Table 5.2: Identity Management-related Web services standards.

Table 5.2 shows the basic Identity Management–related Web services standards, although there are many other supporting standards and components. The core of Web services functionality is based on the model that Figure 5.1 shows.

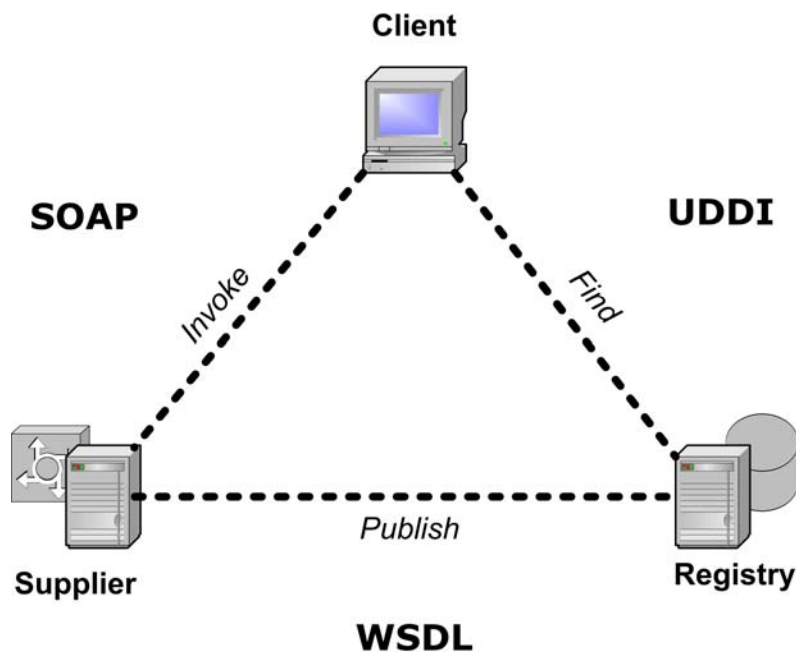


Figure 5.1: Basic Web Services model using SOAP, WSDL, and UDDI.

At the base, SOAP, WSDL, and UDDI make up the foundation of Web services architectures. Let's summarize these standards before we discuss the rest of the Identity Management standards.

SOAP

SOAP is a standard for transporting XML-based messages. Using TCP/IP and HTML as the basis, SOAP is a representation for remote procedure calls (RPCs—call and response). SOAP is a standard originally defined by Microsoft, and now maintained by the W3C. The SOAP specification defines a method for encoding data into an XML format and focuses on an envelope with headers and a body with message content. SOAP can be used with different transports, including HTTP(S). Figure 5.2 illustrates the basic SOAP document structure.

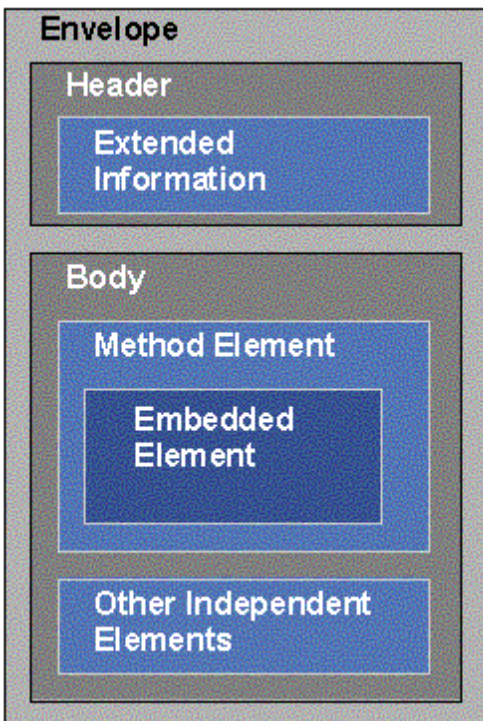


Figure 5.2: Basic SOAP document structure.

There are numerous SOAP extensions, some of which do not deal with Identity Management directly:

- XML Signature and XML Encryption—Draft proposal for public key–based signing and encryption.
- WSS—Defines how to attach signature and encryption headers to SOAP messages to provide quality of protection through message integrity, message confidentiality, and single message authentication. WSS also describes how to attach security tokens, including binary security tokens, allowing for interoperability with common existing security solutions.
- WS-Attachments defines a method for dealing with non-XML content in SOAP. Direct Internet Message Encapsulation (DIME) provides a mechanism for packaging pieces of data together. WS-Attachments then defines how DIME can be used to include attachments with SOAP messages and how to refer to those attachments within the realm of the DIME package.

- **WS-Policy**—Will describe the capabilities and constraints of the security (and other business) policies on intermediaries and end points (for example, required security tokens, supported encryption algorithms, privacy rules).
- **WS-Trust**—Will describe a framework for trust models that enables Web services to securely interoperate.
- **WS-Privacy**—Will describe a model for how Web services and requesters state privacy preferences and organizational privacy practice statements.
- **WS-Coordination**—Describes an extensible framework for providing protocols that coordinate the actions of distributed applications. Such coordination protocols are used to support several applications, including those that need to reach consistent agreement on the outcome of distributed transactions.
- **WS-Routing**—A simple, stateless, SOAP-based protocol for routing SOAP messages in an asynchronous manner over a variety of transports such as Transmission Control Protocol (TCP), UDP, and HTTP. With WS-Routing, the entire message path for a SOAP message (as well as its return path) can be described directly within the SOAP envelope. It supports one-way messaging, two-way messaging (such as request/response and peer-to-peer conversations), and long-running dialogs.

There are numerous other extensions being defined on top of SOAP, but this list should provide some clarity to the flexibility of SOAP as a basic solution for interoperability.

WSDL

WSDL descriptions express the programming interface and location of a service. Publication of a service is really any action that makes the WSDL document available to a potential requester. For example, emailing a WSDL (or a URL pointer to a WSDL) to a developer is publishing. So is advertising a WSDL in a UDDI registry for many developers. Figure 5.3 shows the basic WSDL document structure.

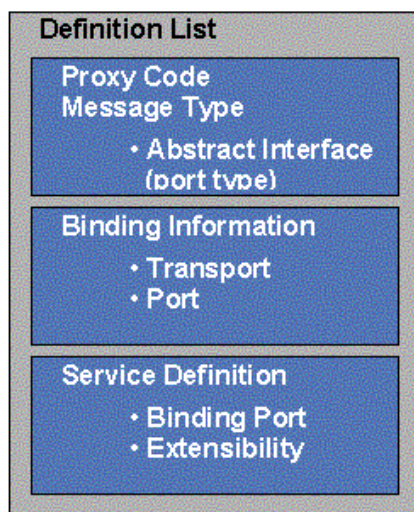


Figure 5.3: The basic WSDL document structure.

Likewise, discovery of a service is any action that gives the service requester access to WSDL for a service. The action might be as simple as accessing a file or URL containing the WSDL or as complex as querying a UDDI registry and using WSDL file(s) to select one of many potential services. Note the lack of specific security or validation around these activities, however. Listing 5.1 shows a simplified sample of a WSDL document.

```
<message name="getUserDataRequest">
  <part name="term" type="xs:string"/>
</message>

<message name="getUserDataResponse">
  <part name="value" type="xs:string"/>
</message>

<portType name="UserData">
  <operation name="getUserData">
    <input message=" getUserDataRequest"/>
    <output message=" getUserDataResponse"/>
  </operation>
</portType>

<binding type="UserData" name="b1">
<soap:binding style="document"
transport="http://schemas.xmlsoap.org/soap/http"/>
  <operation>
    <soap:operation
      soapAction="http://example.com/getUserData"/>
    <input>
      <soap:body use="literal"/>
    </input>
    <output>
      <soap:body use="literal"/>
    </output>
  </operation>
</binding>
```

Listing 5.1: A simplified WSDL document sample.

UDDI

UDDI registry provides a standard way to publish and find information about Web services:

- Find services by searching or by using a unique identifier
- Publish and find services using browser-based and SOAP-based interfaces

UDDI registries contain information about businesses, services, and service bindings as well as additional metadata for categorization purposes (Figure 5.4 shows high-level UDDI interactions). A Web service listing is created using WSDL and then sent to a UDDI registry. UDDI registries organize this information in a manner similar to most directory and phone book concepts (using “colored pages” as the basis). The UDDI business registry has the following three components:

- White pages—Business information including business name, address, and contact information
- Yellow pages—Service categorization (that is, categories based on standard taxonomies)
- Green pages—Technical information (that is, technical specifications and references such as interfaces and URL locations); when requesting a service, you use WSDL to electronically interact with the Green Pages section of that service’s listing

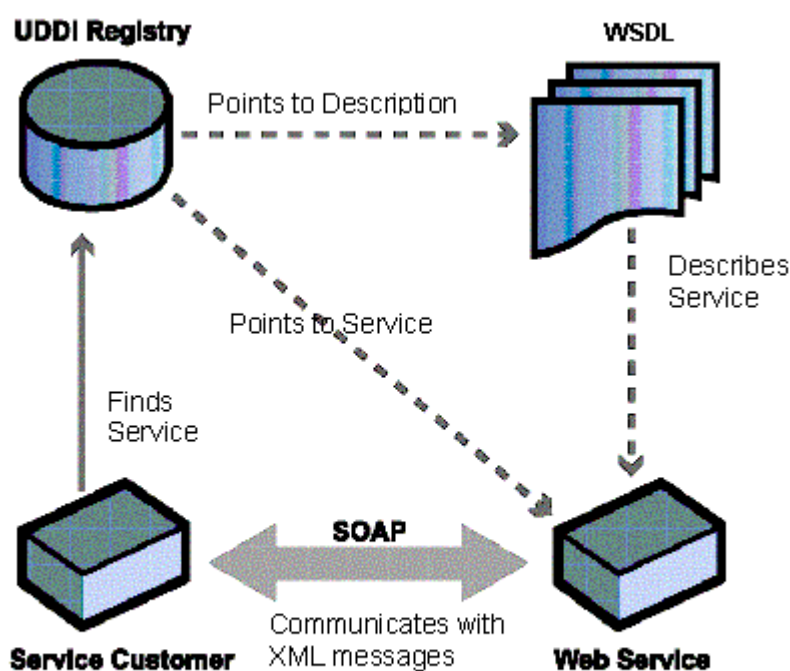



Figure 5.4: High-level UDDI interactions.


UDDI was originally developed by IBM, Microsoft, and Ariba, and is now managed by OASIS. With the stewardship for the standard having been moved to OASIS, work is now progressing on the next release.

 You can find information about UDDI versions 1, 2 and 3; supporting WSDL service interface descriptions; and tModel overview documents at <http://uddi.org/specification.html>.

tModel

Although the interface descriptions are important when looking for a service, perhaps more important is the concept of a tModel. A tModel is the technical fingerprint used to describe these interfaces. tModels provide a binding template, which allows you to determine whether you are compatible with a given service based on interface, behavior, or some other concept.

Free, public, interconnected UDDI servers are deployed today by Microsoft, IBM, SAP, and NTT. In addition, there are test registries you can use to develop and test deployments against. Companies such as Novell, Sun Microsystems, and Computer Associates are working on UDDI support in their directory products, and BEA WebLogic 7.0 includes an LDAP-enabled UDDI server that will allow for private or intra-organizational registries, supporting the goals of code reuse as well as full service access within an organization.

 For information about the LDAP schema for UDDI, check out the Internet draft on the IETF Web site at <http://www.ietf.org>.

Security

In the area of security, there are a couple of Identity Management–related solutions. In the following sections, we’ll explore SAML and WSS.

SAML

SAML delivers an XML-based authentication solution for Web services. SAML is designed to support the exchange of authentication and authorization information between disparate systems from Web access management to broader security solutions, leveraging the Web services standards that we discussed earlier (such as XML and SOAP). The goal is to allow transactions to be securely distributed across multiple organizations and Web services, while mitigating the complexities of differing authentication and authorization schemes.

In some cases, such solutions will have significant impact because the simple act of authentication and authorization is quite arduous; in other cases, authentication and authorization is only a small part of the problem. That is not to say that solving this problem is not important, but that authentication is not always the only problem being faced. Consider a company that partners with many third-party organizations and providers to offer a consolidated store-front for the purchasing of many different items and services. To initiate this arrangement, there is a significant amount of work to integrate the sign-on and back-end shopping processes. Being able to move customers from one site to another without requiring that they log on to every one of those sites is critical to the seamless shopping experience, but this ability assumes that all the work takes place at the first logged onto site. It is the back-office coordination of deliveries, packaging, and returns that must be considered in addition to authentication and authorization. Thus, the goal of SAML (and the Liberty Alliance Project) is to allow for easier integration of systems, enabling organizations to quickly develop basic but strategic alliances.

SAML is comprised of three parts:

- Assertions—There are three assertions: authentication, attribute, and authorization
 - Authentication assertion validates a user’s identity
 - Attribute assertion contains specific information about a user
 - Authorization assertion identifies what the user is authorized to do
- Protocols define how SAML asks for and receives assertions
- Binding defines how SAML message exchanges are mapped to SOAP exchanges; SAML can utilize multiple protocols including HTTP, Simple Mail Transfer Protocol (SMTP), File Transfer Protocol (FTP), and SOAP.

However, SAML is not a provisioning solution. There is an implicit assumption in the protocol that the correct accounts have been registered (that is, the identities have been established for all parties—source and destination) or that the initiation of SAML will call into play some dynamic registration. This then presupposes that Identity Management provisioning is in play. As such, there is also work on provisioning standards, the most prominent of which is SPML, which we will discuss shortly.

For reference, many Identity Management companies currently support SAML, including:

- Sun Microsystems
- Baltimore
- Oblix
- OpenNetwork
- RSA Security
- Crosslogix
- OverXeer
- ePeople
- Sigaba
- Entegrity

Many others have announced support and will likely introduce it to their products in 2003.

☞ OpenSAML is a set of open-source libraries in Java and C++ that you can use to build, transport, and parse SAML messages. OpenSAML is able to transform the individual information fields that make up a SAML message, build the correct XML representation, and unpack and process the XML before handing it off to a recipient. OpenSAML fully supports the SAML browser/POST profile for Web sign-on, and supports the SOAP binding for exchange of attribute queries and attribute assertions. It does not currently support the browser/artifact profile or other SAML messages involving authorization decisions. You can download the OpenSAML code at <http://www.opensaml.org/>.

Another resource is the SourceID Single Sign-On Toolkit. Although it doesn’t directly offer identity storage, retrieval, authentication, or authorization logic, it provides well-documented plug-in points with which the tool kit user can write short Java classes that bridge existing systems to the SourceID SSO kernel. You can download the toolkit at <http://www.sourceid.org/>.

WSS

WSS, sometimes referred to as the Web Services Security Language, specifies enhancements to the SOAP protocol and is intended to enhance message confidentiality and integrity through the definition of how and where to place security information in a SOAP message envelope. For example, SAML definitions could be incorporated into the WSS model, and the standard specifically calls out PKI, Kerberos, and Secure Sockets Layer (SSL).

Initiated by IBM, Microsoft, and VeriSign, WSS is now managed by the WS-I. Related specifications include the Business Process Execution Language (BPEL), WS-Coordination, and WS-Transaction.

Federated Identity and Standards

We examined the concept of federated identity in previous chapters. The rise of new distributed computing models has driven the adoption of federated identity and Web services solutions. This rise of the Internet has forced organizations to play in the wider arena of interoperability across organizations in order to optimize their value chains. This cross-organizational push has forced the adoption of proprietary solutions over time; however, the concept of federated identity allows for a standards-based solution to be developed that allows individuals or systems to better interoperate securely across organizational boundaries currently protected by security systems, primarily firewalls and virtual private networks (VPNs).

Because interoperability has historically been perceived and addressed as a data-level issue, the consideration of how access is gained and who or what has access has almost always been hard coded (that is, developers or vendors have predefined access control within the application by, for example, providing only administrator, manager, and user definitions). To create fluid and efficient interoperability requires that the security or identity components be automated too. Thus, the need to continue to build and manage internal processes around Identity Management are just as, if not more, critical than solving the federated identity problem. The bigger issue remains around policies, repudiation, and related aspects. Although PKI has driven many of these discussions already, the solutions available today do little to address privacy policies and trading-partner agreements that are essential to creating trust relationships. The difference is that with the experience gained from the PKI initiatives, new solutions and standards are making trust relationships easier to establish.

On the standards front, there are a number of efforts initiated to support the requirements of federated identity. Because these initiatives are moving fast, I'll briefly discuss them, then quickly move on to how you can determine which is best for you.

The Liberty Alliance Project

As introduced in Chapter 1, the Liberty Alliance Project (<http://www.projectliberty.org/>) “is an alliance formed to deliver and support a federated network identity solution for the Internet that enables single sign-on for consumers as well as business users in an open, federated way.”

Although the Liberty Alliance Project intends to solve multiple issues around authentication, authorization, and the related policy issues, the first release addresses the following requirements:

- Opt-in account linking—Enables a choice to link accounts across disparate organizations regardless of business type
- Simplified sign-on for linked accounts—Provides the ability to authenticate using a single account and navigate to other sites without authenticating again, utilizing linked accounts as required
- Authentication context—Enables organizations to designate authorization levels for specific customers, defining what the customer can see and do at a site
- Global log out—Provides the capability for customers to log out of all linked sites through logging out of the initial logon site
- Liberty Alliance Project client feature—Provides a client component for fixed and wireless devices that facilitates the use of Liberty version 1.0

 Sun Microsystems has released an “Interoperability Prototype for Liberty” that you can download from <http://www.sun.com/software/sunone/identity/ipl/index.html>.


Microsoft Passport

Microsoft Passport, now know as the .NET Passport, was introduced in 1999 and, as noted by Microsoft, “is a suite of Web-based services that help make using the Internet and purchasing online easier and faster.” .NET Passport is delivered as part of the .NET Services, which is a broad swath of services designed to provide the building blocks for the efficient development of user-centric applications. As the Microsoft Web site notes “.NET Passport provides users with single sign-in (SSI) and fast purchasing capability at a growing number of participating sites, reducing the amount of information users must remember or retype.”

Passport is delivered as a Web service, allowing developers to use the Microsoft managed authentication service instead of implementing their own. This factor is an important consideration in that while you might maintain local identity information for any reason, some subset of that identity data is held outside your control.

The areas most concerning both supporters and detractors are around liability, privacy, ownership, and regulation of the identity data. Microsoft has faced the European Union on these specific issues as related to the Passport design, and was forced to make changes. Although this situation has not significantly affected partners using Passport at this time, the issue of being able to meet your own organizations’ current and future compliance requirements bears careful consideration against any potential upside gained by using a widely available solution such as Passport. Although you cannot predict every future possibility, consider the introduction of HIPAA, which we’ve discussed in previous chapters.

As we've explored, HIPAA has driven many organizations to change the way in which they deal with privacy issues, often resulting in systems being removed or radically changed to support the mandatory requirements around patient data management and access. If you no longer own some of the data, this exercise becomes even more excessive. However, if you partner with Microsoft or implement solutions using .NET and Internet Information Server (IIS), you should consider integrating security access with Passport as well as maintaining your own data.

 Microsoft has released an SDK that allows you to integrate Passport into your own applications. The .NET Passport SDK is available as part of the developer resources on Microsoft's Web site (<http://www.microsoft.com>).

Liberty, Passport, Both, or Something Else?

One of the questions that will likely arise is whether to use the Liberty Alliance Project solutions, Passport, both, or something else? At a base level, these “standards” attempt to solve the identity requirement for authorization and to differing degrees, authorization. The goal of all the solutions is to enable federation of Identity Management for organizations, from internally integrated solutions to cross-organizational resource access, by minimizing the need to exchange sensitive data, but still securely share relevant data.

In theory, these solutions should allow for a single identity to be used for sign-on across all relevant applications, services, and resources. The logical end is seamless interoperability; however, as mentioned earlier, there is still a potential need to support registration across the disparate applications, services, and resources.

As noted, both the Liberty Alliance Project solutions and Passport are well suited to support consumer solutions; however, these solutions might be more than an organization requires. The Liberty Alliance Project has based a lot of their initial solution on the SAML specification, so while there are additional specifications by the Liberty Alliance Project, perhaps SAML is all that is needed for your situation.

For example, OpenSAML offers a basic SAML implementation through open source licensing. Alternatively, the Shibboleth Project (<http://shibboleth.internet2.edu/>), which is sponsored by Internet2, uses OpenSAML to advance its solution of “developing architectures, policy structures, practical technologies, and an open source implementation to support inter-institutional sharing of Web resources subject to access controls. In addition, Shibboleth is developing a policy framework that will allow inter-operation within the higher education community.”

The Shibboleth project's goals are very similar to the goals of the Liberty Alliance Project, and thus, require consideration especially if you do not plan to extend into commercial applications immediately. The common use of SAML provides some level of mitigation for interoperability in the future.

Although developing your own solution is one option, it is likely that vendors will provide comprehensive and interoperable support for the various standards around Identity Management, in particular those related to security. For example, the first company to demonstrate an interoperable solution using both the Liberty Alliance Project's solution and SAML was OpenNetwork.

OpenNetwork's solution works as follows:

1. As Company A's user signs into a DirectorySmart-protected Web service with their Passport credentials, they might want to access a second Web service hosted by a trusted business partner using SAML.
2. As the user attempts to access this SAML-based service, DirectorySmart passes on the required authentication and authorization information in SAML to the trusted partner, Company B.
3. The partner then uses this information to determine authentication and authorization to Web services, eliminating the need for an additional logon for the user.
4. Company A is then able to deliver a seamless user Web experience by joining Passport and SAML through the DirectorySmart interoperability bridge.

This solution is a good example of the need for and implementation of interoperability.

Trust

We have touched on the issue of trust several times. In the case of Passport, trust must be placed in Microsoft not only to manage and protect the data, but also to maintain the service availability. In the case of the Liberty Alliance Project, there is less of this concern, but the authentication service must still be available to work or there must be processes in place to deal with a failure of any of these areas. Because these considerations must often be enforced outside the automatic confines of system interoperability, they require out of band or manual process, legally binding companies to certain support levels and remediation processes.

At this point, organizations such as PingID become valuable. Aiming to provide a visa-like network of trust through standard and legal agreements, PingID is made up of members who want to trust for Identity Management purposes. Organizations such as the Liberty Alliance Project and Microsoft offer some protections, whereas SAML, of course, as a standard, provides none of this support. Furthermore, the level to which the Liberty Alliance Project solution and Passport offer such protections is not as great as PingID.

The example given by PingID is of Automated Teller Machine (ATM) agreements between banks. These machines would not allow non-bank customers to withdraw cash without some form of legal agreement and standards that all the banks can rely on and fall back on in the event of some failure or challenge. This agreement defines the processes, bounds, and limits for transactions, as well as the agreed upon processes for remediation.

Visa International operates their member network in a similar way. A member organization that wants to allow visa card-holders to make purchases or payments at their establishment agrees to the terms and conditions of the network, and gains the benefits associated with that network from access and validation to the similar remediation policies. The danger is that many of these types of affiliations arise, creating too many standards.

Workflow

There are many workflow solutions available, some of which can help you in your Identity Management implementation. The question is, do workflow standards actually help you? When looking at internal development or third-party solutions, consider that workflow is required to ensure the right processes are followed; however, it is very rare for systems to interoperate at the workflow level. As such, the need for a solution to support a workflow standard is less important than being able to expose the workflows in a way in which you can easily manage and monitor them.


If you want to understand the level of interoperability available, you could consider reviewing the Workflow Management Coalition (WfMC—<http://www.wfmc.org/>) who “promote and develop the use of workflow through the establishment of standards for software terminology, interoperability, and connectivity between workflow products.” Alternatively, in line with the relentless drive toward XML, you might be looking for BPML or Business Process Execution Language (BPEL). For more information about BPML, see <http://www.bpml.org/bpml.esp>.

BPEL

Published in August 2002, BPEL is an update and replacement for IBM’s Web Services Flow Language (WSFL) and Microsoft’s XLANG specification. BPEL is a specification for a programming language that enables a task to be accomplished using a combination of Web services, possibly involving more than one company. As noted at <http://xml.coverpages.org/bpel4ws.html> “BPEL allows companies to describe business processes that include multiple Web services and standardize message exchange internally and between partners.”

For example, a BPEL program could be used to describe a business protocol between travel agents and tour operators such that each can automate the process by which they will exchange order and confirmation information, and more importantly, how to deal with exceptions. Perhaps most important is the definition of the order in which steps are processed and if they are parallel or serial. How those things are processed at each step of the transaction is left to the Web service definitions.

BPEL is seeing uptake especially by its original developers, Microsoft, IBM, and BEA Systems. However, BPEL has not achieved widespread use.

 For more information about BPEL, see <http://www-106.ibm.com/developerworks/webservices/library/ws-bpel/>.

Provisioning

Standards in the provisioning space are minimal. There have been several efforts to provide standards-based provisioning solutions. The workflow standards provide methods to ensure that provisioning takes place in the correct order, and importantly allow for the specification of what to do if something fails. The only provisioning-specific standard worth discussing at this time is SPML.

SPML

SPML is a proposed specification through OASIS, which has been working on the development of the specification since late 2001. The development has some way to go before it reaches the level of sophistication of SAML, but the first version of SPML is due for release in mid 2003.

SPML requests are intended to facilitate the creation, modification, activation, suspension, enablement, and deletion of data on managed Provisioning Service Targets (PSTs). OASIS has been working on SPML since late 2001, and it has some way to go to reach the level of SAML; however, this version is due for 1.0 release in mid 2003.

To understand SPML, we must review the Web services model that we discussed earlier in this chapter. In that model, there is a networking layer, on top of which is an XML-based messaging layer. This layer, which is based on SOAP, makes communications possible between Web services and their clients. SPML will specify the provisioning or subscribing function of the Web services. SPML will determine the provisioning (for example, to add, create, delete, modify, or query) of provisioning service points (PSPs) and provisioning service targets (PSTs). SPML will make this determination based on a formal submittal from the Requesting Authority (RA). In certain situations, the PST might be an RA that is requesting access to a service on another PSP.

As we discussed earlier, security is one a key factor in Web services solutions. Such being the case, we can see a relationship between the protocol/API and security solutions, one of which is SPML:

- HTTP—HTTP over SSL
- SOAP—Signed requests and/or reliance on HTTPS for secure channel
- SPML—WSS

Thus, you can see that SPML is being developed to address the severe demands of today's e-businesses, which include security management and quality of service management.

Biometric Standards


Biometrics provides automated mechanisms for identifying a person based on physiological or behavioral characteristics. We discussed this idea in Chapter 1 as “something you are.”

Examples of biological aspects that could be used in biometrics are:

- Deoxyribonucleic Acid (DNA)
- Fingerprints
- Facial recognition
- Handwriting analysis
- Retinal and iris scanning
- Voice recognition

The biometrics arena is growing quickly. However, this market has many considerations that need to be addressed, including the definition of biometric information and more esoteric and moral factors. Many in this market are working to address such unresolved issues.

The media often shows clever individuals that can easily fool biometric solutions (for example, by wearing a latex glove and powder or stick-on fingerprints to dupe a palm scanner or by using a recording to trick a voice-recognition solution). Thus, one of the key challenges of using biometrics is that if the definition of the biometric challenge is held in a central place and the scanner used to gain the biometric scan and feed it through the verification process remains in a fixed position, there is the possibility for impersonation due to the assumption that the actual input mechanism is foolproof. This factor will always be an issue; however, vendors of biometric solutions now have the technology to deploy the scanner (the input mechanism) with the actual biometric signature, which can minimize the ability of interception of the biometric data. For example, SafeNet offers iKey that has a fingerprint scanner built-in to the actual device. This configuration ensures that the biometric signature stays within the device and can never be intercepted.

 For more information about biometrics and the evolution of this market, check out <http://www.biometrics.org/>. This Web site provides a definition of biometrics as well as the current issues being addressed in this market.

BioAPI

The most prevalent biometric standard outside governments is the BioAPI, which defines an open API for developers to integrate with biometric mechanisms in a standard way. Originally approved by ANSI in February 2002, NIST and the NSA and the U.S. Biometric Consortium sponsored a unification meeting in March of 1999 in which the ANSI Human Authentication API (HA-API) working group (originally sponsored by the U. S. Department of Defense, which published the high-level biometric API in 1997) agreed to merge their activities with the BioAPI Consortium. The HA-API is a high-level API that was published in November 1997.

The BioAPI still has a ways to go to make the standard broadly interoperable, specifically in terms of support for definition of matching agreements, wherein the standard needs to define the levels of accuracy to be agreed or required between technologies using the BioAPI. The BioAPI organization plans to release a new version in 2004.

 Current BioAPI-compliant products are listed on the BioAPI organization's home page at http://www.bioapi.org/BioAPI_products/products.htm.

X9.84—Biometric Information Management and Security for the Financial Services Industry

The X9.84 Biometric Information Management and Security for the Financial Services Industry standard defines the security and management of biometric data, including secure transmission and storage, and security of the surrounding hardware. Essentially, X9.84 helps secure the authenticity and integrity of biometric data using digital signatures. To do so (and unlike the BioAPI at the time of this writing), X9.84 defines recommendations around false match rates for verification and identification. As the title suggests, this standard is driven by the financial services industry and is being shepherded by ANSI.

XML Common Biometric Format

Developed to consolidate and enhance interoperability through the use of Web services-based solutions, the XML Common Biometric Format (XCBF) is an initiative under the OASIS banner.


This consolidation exercise is taking the BioAPI and X9.84 specifications and providing a common XML format using a common schema. Eventually XCBF would also become a format supported by CBEFF.

The main dilemma with the BioAPI and X9.84 specifications are that they are binary constructs. This type of representation allows for minimal memory waste and is critical when dealing with resource-constrained devices such as smart cards and tokens. However, while it appears that the drive towards XML-based standards seems to be trying to replace every existing standard, using XML representations makes them easier to read and use in Web services models and sometimes easier to transport.

CBEFF


As previously noted, CBEFF was the result of consolidated work by NIST and the BioAPI consortium (see Table 5.1). The goal of the exercise was to provide a “technology-blind biometric file format that would include all modalities of biometrics and would not bias, encourage, or discourage any particular vendor or biometric technology from another. It would not attempt to translate among different biometric technologies, but would identify them and facilitate their co-existence.” NIST published the “Common Biometric Exchange File Format (CBEFF)” on January 3, 2001 as NISTIR 6529.

Incorporating a method to encapsulate payloads of biometric data in a standard format, CBEFF currently “recognizes” two standards, the BioAPI and X9.84. As a result, CBEFF smoothes the interoperability issues between the two.

 For more information about CBEFF, check out <http://www.itl.nist.gov/div895/isis/bc/cbeff/>.

Smart Card Standards

Although the standards we've discussed so far cover the main Identity Management components, you can check out the Smart Card Industry Association's Web site for more information. This site contains information on related Identity Management standards, industry events, and newsletters related to smart card technology.

 For more information about smart cards and the related standards, check out <http://www.smartcardalliance.org/>.

Summary

Many Identity Management-related standards have existed for some time, but this area is still rapidly evolving and as such, expectations must be set around the level of real interoperability these standards will supply. Efforts by the involved forums and groups that were mentioned in this chapter as well as those of vendors will help these efforts maintain a progressively smoother level of integration.

The standards keep rolling forward, ranging from loose to tight affiliations with the requirements of Identity Management. The key is to look for those that solve your challenges and are well supported.

In Chapter 6, we will look at the organizations that can help you plan and implement your Identity Management initiative, and finally take a look at where this market is going. The rapid developments alluded to make Identity Management an interesting and dynamic space with massive potential to improve productivity and value in your organization.

Chapter 6: Identity Management Technologies and Trends

Welcome to the final chapter of *The Definitive Guide to Identity Management*. Before we dive into this chapter, let's review what we've covered so far:

- In Chapter 1, we defined the who, what, where, and when of Identity Management and briefly explored Identity Management standards.
- Chapter 2 began to delve deeper into the components required and available to support an Identity Management initiative, focusing on how Identity Management can help meet most organization's key security requirements.
- By Chapter 3, we had established a common vocabulary and baseline understanding of Identity Management components and concepts, so we moved on to explore Identity Management applications.
- This discussion led smoothly into Chapter 4, which covered Identity Management implementation. As a result of the new and rapidly evolving Identity Management market, there is much flexibility in the terms that vendors use to market their solutions. In this chapter, I discussed how this scope affects the requirements of Identity Management implementations, which will be unique to each organization.
- And in Chapter 5, we built on the foundation of Identity Management standards information that we laid in Chapter 1, focusing on which standards will solve the challenges of your organizations' environment.

This final chapter is intended to provide an overview of some of the current Identity Management vendors and the technologies they have to offer and are developing. In addition, this chapter provides a concise list of organizations that specialize in the Identity Management space—in particular those organizations that are independent and can help you define and realize the right Identity Management solutions and implementation timelines for your organization.

In this chapter, I'll also explore the trends of the Identity Management market, including likely trajectories and intersections with other technologies. Hopefully, this information will give you insights into the future of the Identity Management market that will help in planning your Identity Management solution. We'll start by exploring the benefits of Identity Management consultants.

Consultants

Although organizations are working to develop standards within the Identity Management space, as we explored in Chapter 5, there is much legacy and proprietary technology still in use and being deployed. This technology makes it a challenge to attempt to integrate the potential Identity Management capabilities available and ensures that such a task is tricky to accomplish without some degree of difficulty. One way to work around this challenge is through consultancy services that are not new to the Identity Management market. Through their expertise and understanding of Identity Management, consultants can assist your organization in rapidly deploying your Identity Management solutions.

Consulting around Identity Management has boomed over the past couple of years and will continue to do so as the industry strengthens and matures. Most IT consulting companies have either established an Identity Management practice or have consultants with specific skills in this area.

Determining which consulting organization to work with during an Identity Management planning and/or deployment exercise is an important task, and, as I stated in Chapter 3, is usually necessary unless you have experienced people on staff. Some companies are very good at assisting you in setting strategy, documenting requirements, and developing business cases to help in the early phases of a project. Others are very good at managing an Identity Management project and/or carrying out the deployment work. Many can carry out both the strategic and deployment functions.

Be aware that many of the specialist companies have strategic partnerships with certain vendors that might influence their product choices. However, this very fact can work to your benefit if you have already chosen a vendor product and want highly skilled expertise focused on that product.

Professional Services

As I've mentioned in previous chapters, careful planning is vital to an Identity Management solution deployment. Developing a comprehensive strategy to evolve your company's Identity Management infrastructure, procedures, and policies will help to ensure that each part of an implementation exists within an overall plan. Some of the well-known companies that offer specialist Identity Management practices include ePresence, Burton Group, PricewaterhouseCoopers, and Deloitte Touche Tohmatsu.

ePresence is an interesting company that originally started out as Banyan Systems. Banyan produced one of the first commercial directory-based OSs. Banyan's gradual disappearance from the OS marketplace had very little to do with the quality of its product (it was a good product) and had a lot to do with market penetration and competition from Novell, Microsoft, and Microsoft licensees'. Banyan's senior management team decided to turn its company into specialists in the directory consultancy market and have morphed into the Identity Management market. The company's original staff of highly skilled directory experts has been expanded to include project managers, architects, and people with hands-on skills across a broad range of Identity Management products.

Infrastructure Help

Novell seems to be moving in a similar direction to ePresence. Novell has a very good directory product in eDirectory, and through the fairly recent merge with Cambridge Associates, Novell employs a valuable army of consultants. Novell has accepted that directories are commodity products—plumbing for value-added products and services, so it often offers eDirectory as a giveaway. The company is now focusing on meta directory, security, provisioning, and other Identity Management-related products to provide a revenue stream. This effort coupled with the professional services the company can now offer should ensure Novell's survival in the Identity Management arena for some time.

Microsoft seems to have taken an infrastructure-only approach. Having delivered AD as a core service in Win2K Server, Microsoft then obtained meta directory technology through the acquisition of Zomet, which Microsoft now sells as Microsoft Metadirectory Server (MMS). As I discussed in the Identity Management components section of Chapter 1, Microsoft has so far taken a similar strategy with Critical Path, focusing on core infrastructure components upon which organizations can build their own applications and user interfaces (UIs). In addition, Microsoft offers many extra tools and infrastructure components from which to build solutions, such as Visual Studio, Internet Information Server (IIS), and so forth. Microsoft has recognized that Identity Management, especially at the infrastructure stage, requires expertise, and as a result Microsoft Consulting Services are almost mandated when an organization wants to deploy MMS.

The Risk Management Factor

Many consultancies such as PricewaterhouseCoopers and Deloitte Touche and Tohmatsu have arrived at the Identity Management market as part of their risk management or security practices. This evolution is an important intersection which resonates well with Identity Management. In fact, many other organizations have internal risk management—in particular, but not exclusively, financial, medical, health, and manufacturing organizations.

Risk management embraces many strategic, operational, and process components of an organization. Risk management is about trying to eliminate or mitigate potential risks in and to the organization through planning and the deployment of systems and processes. Many of the organizations that come from the risk management background have extensive experience in the risk vs. reward-type scenarios that you will face when looking at the Identity Management market. Remember that although it might seem that your environment grows more secure the more security processes and technology you put in place, there is the risk that you will develop a solution that is too complex to use or too complex to identify possible methods of failure or intrusion.

☞ If your organization has an existing risk management team, it would help a great deal if they were identified as a stakeholder in any Identity Management initiative. The experience of risk management teams is not only in identifying risks and in clarifying which are the most important risks to be dealt with, but also in which risks are not very important at all.

The key point to take away from this section is that, for many organizations, an Identity Management solution is part of the resolution of many issues—risk management being another part. The challenges faced by many organizations might be larger than an Identity Management initiative can immediately solve, although Identity Management might form part of the solution.

Solution Vendors

There is a category of consultants called solution vendors. These are vendors of Identity Management–related products that provide professional services that can help you plan and deploy their products into your organization. Some solution vendors might go beyond this scope and help provide general Identity Management strategy guidance as well. Some of the larger solution vendors include IBM, Computer Associates, Sun Microsystems, and Novell, though most of the vendors mentioned in Chapter 3 have some form of professional services and/or consultants available. Consultants who work for solution vendors or trained partners and resellers often have very detailed knowledge of the vendor’s products. Although many Identity Management solutions are becoming more integrated and easier to install, the expertise of solution vendors’ consultants is still close to a requirement for installing these products. These consultants can help you avoid problems that arise as a result of the complex integration issues across other back-end systems.

To increase exposure and market penetration, many of the vendors have set up strategic relationships with some of the larger consulting firms. Access360, Business Layers, Netegrity, Critical Path, OpenNetwork, and several others have a partnership with ePresence. Vendors such as Oblix, Novell, Sun Microsystems, Waveset Technologies, and BMC Software have a partnership with PricewaterhouseCoopers. These types of relationships help to increase the number of consultants and support personnel that have skills in the Identity Management arena and with specific Identity Management products. In addition, these relationships allow companies that are deploying Identity Management solutions to use consultants with expert knowledge in the Identity Management field and make a choice from multiple products to meet their needs.

Emerging Identity Management–Related Issues

Aside from the consolidation of specific Identity Management functionality that we explored in Chapter 1, the following areas will become more prevalent in the Identity Management market over the next few years. These areas will increasingly become more significant to Identity Management as time progresses:

- Federated identity
- Contexts-sensitive Identity Management
- Identity theft
- Intrusion detection
- Intellectual property management
- Content and digital rights management
- Regulatory and compliance issues
- Identity Management appliances
- Advanced biometric applications

This list highlights the areas of focus that Identity Management solutions will continue to move toward and envelop as well as help drive the development of.

Federated Identity

We have discussed federated identity several times throughout this book, and its importance has led me to include it again in this section. Although federated identity is a definite trend, there has been minimal interaction with the existing infrastructure and solutions already established to support X.509 certificates. The model used for X.509 is based on the X.500 directory model, wherein there is a top-down, mandated structure for information authorities. It appears to many that solutions based on SAML or Microsoft's .NET Passport will avoid much of the complexity of solutions such as X.509. However, both SAML and .NET Passport, as well as similar efforts, will need to be evolved to meet more general requirements as more commercial implementations are made.

This situation is akin to that of LDAP and X.500. X.500 was planned as an all-encompassing, world-wide, solve-everything directory standard; whereas, LDAP was planned as a simple solution that would meet the needs of a small environment (such that it could be quickly implemented and easily used). Although X.500 found favor with large organizations and many national and educational institutions, it did not have widespread commercial adoption. LDAP, however, being quick and easy to implement and, more importantly, designed to work on the Internet-standard TCP/IP protocols, had rapid commercial adoption. As LDAP became more widely used, implementers found many deficiencies, such as limitations with data distribution or replication, large-scale data management, and so forth. Interestingly, all these issues were dealt with in the X.500 standard. This situation parallels that of federated identity—although one solution is less complex, that simplicity comes at the cost of functionality. Sometimes the best and most complete solution isn't necessarily the most popular. As federated identity solutions evolve and replace existing solutions, they might not address every issue but instead will offer enough functionality to allow organizations to move forward with their implementations.


Challenges to Federated Identity

On the privacy front, federation faces many challenges. A major consideration is the complex relationship between federated identity and legality. The sharing of information between organizations may be governed by local or national laws or international agreements. The issue is compounded when laws contradict each other about what information can be shared. Since its launch in 1999, .NET Passport has been under much scrutiny from public and private organizations. For example, from .NET Passport's launch through 2001, the Electronic Privacy Information Center (EPIC) along with numerous other consumer advocacy groups raised privacy issues with the United States Federal Trade Commission (FTC) concerning .NET Passport, which in turn led to the FTC to investigate .NET Passport. The European Commission has asked similar questions about .NET Passport. Most issues focus on the following concerns:

- Unclear privacy policies that make it difficult to determine what will happen to personal data once it is provided
- The process of securing the collection and storage of personal information
- Particular concern about protection of data relating to children
- Potential transfer of personal data beyond organizations with which a relationship was established
- Potential transfer of personal data across state or national borders, potentially breaking established laws either locally or internationally
- The lack of ability to delete an account

Much work has been done to deal with the policy issues, making them clearer and more restrictive about how personal data is handled.

This factor is an important consideration if you plan to do business with international partners or customers, whether they are other organizations or individuals. It is in situations like these in which an organization that has already worked through these issues becomes valuable. The effort that Microsoft is putting into .NET Passport is one example of an organization that is attempting to find a balance between the benefits of federated identity and legality. Visa, Master Card, and American Express also provide a model wherein these issues have been dealt with, such that the correct and legal exchange of identity information can occur. These companies have established a trusted network in which to exchange information and a formal membership model for the distribution and usage of credit cards as the identifier for undertaking transactions. The trend with federated identity will be based on these models. A company known as PingID provides a new version of these models specifically for the use of identity in federated environments.

 As defined on its Web site. "Ping Identity Corporation was established to meet the growing demand for solutions that manage the emergence of Identity Federation—the linking and movement of identity information between two or more organizations." For more information about the PingID network and corporation, check out <http://www.pingid.com>.

Context-Sensitive Identity Management

Another area of Identity Management that will become increasingly important is context. For example, most current OSs employ a form of the concept of allowing logon at specific times of the day or to specific resources, such as remote access. The consideration for many organizations is that unless all your resources are protected by the same access control mechanism, such as an SSO solution, you cannot apply the same policies across many different types of resources.

Time-based restrictions are an example of basic context-based controls. The following list offers other context-based information that could be used to control access to systems as well as determine the identity of the access requester (generally consider an individual, but could also be an application or service that needs access to other resources):

- Location of the access requester—Is the access requester accessing the resource from a controlled environment (an intranet, extranet, or VPN), or is the access requester trying to gain access from a remote location (unencrypted dial-up, DSL)? Can the location be determined and validated by an outside source?
- Location of the resource—Is the resource within a physically secure environment?
- Authentication method—Is the authentication method an account and password, token, or biometric?
- Access method—Is the access requester trying to access resources via fixed connection, wireless connection, or other? What type of connection is being used—wireless and WiFi, Bluetooth, infra red?
- Access device—What device is the access requester currently using—laptop, desktop, handheld device, or other?

These as well as additional pieces of information help define the context of the situation and can allow a system to change the level of access a user may have. This functionality can help ensure that secure data is only accessed over a secure (for example, encrypted) connection. In addition, there are more extensive sets of context information closely related to biometric challenges such as whether the access requester is under stress—is the access requester's blood pressure, body temperature, or pulse rate outside of scoped limits. Certainly, these types of methods might seem far-fetched or beyond the needs of many organizations. However, there is a growing niche for such context-sensitive information, and these types of solutions are already available in high-end security solutions that will become more prevalent as well as cheaper over time.

In addition, context expands the ability of an Identity Management solution to provide dynamic profile information to applications—profiles are extended through context information. A profile is a set of characteristics that relate to an identity, including data about that identity ranging through the following:

- Name
- Addresses/locations
- Age
- Identifying references
 - Passport Number
 - Student number
 - USA Social Security Number
- Application preferences
 - Color schemes

Although Identity Management is generally thought of as dealing with the identity of individuals, another context of Identity Management solutions is that of systems and applications that need access to each other. In some cases, this might be an application that needs access to another to enact changes on behalf of a user. Thus, context provides the dynamic aspects of the profile, allowing for very complex scenarios (applications acting on behalf of users, for example) to be automated.

Identity Theft

Identity theft is when somebody gains information about, or the identifiers of, someone else, and uses that information to masquerade as the person whose identity has been stolen. Because identity is based on key pieces of information about a person (for example, date of birth, address, and so on, many identity solutions base their validation on those pieces of information; in some cases, making the assumption that an individual in possession of that information must be the same individual to whom they belong. In these situations, a thief can establish a bank or credit card account with some basic address information. It is difficult to protect against such criminally fraudulent behavior, but by placing controls around how information is exchanged we can mitigate the risk.

There are many ways identity theft can occur in the real world, such as:


- **Pickpockets and purse snatchers**—The classic theft that traditionally nets cash is now used more and more to obtain credit card, driver’s license, and other personal data that can be used to obtain additional credit at a later date.
- **Swiping**—Thieves use swipers (small electronic card readers) to capture credit card details that can be uploaded to a computer at a later time. These thieves often “employ” staff in heavy tourism areas and upscale restaurants in which credit cards are often used. Cards might not even be used for some time after the theft, meaning that tracking where the incident took place can be extremely problematic.
- **Mail theft**—Much identity theft today is through simple theft of physical mail from a mailbox. This type of theft focuses on credit card approvals (that is, pre-approved credit card offers), payments (utilities, car registrations), and so forth. The goal is to gain as much personal information about individuals, or alternatively, to gain a person’s actual credit card, license, or otherwise such that the thief can easily pretend to be that person. This theft affects domestic as well as business mail.
- **Trash or dumpster diving**—Similar to mail theft, thieves can obtain information about an individual or organization by searching through trash either at home or near a business. Thus, the need is very high to shred any paperwork that contains personal information.
- **Insider access**—Unfortunately, insider access to data is a growing concern wherein employees of organizations that deal with personal data (for example, a Human Resources staff person or customer service representatives) exploit their position.
- **Private data on second-hand computers or similar electronic devices**—Thieves may obtain old computing resources from individuals or organizations and attempt to recover information from the devices. Corporations should ensure that all data on old computing devices is thoroughly wiped before selling or giving them away. Ideally, the hard drive should be removed and destroyed prior to the machine being moved on.
- **Redirection**—Thieves might use a change of address or similar method to redirect mail to an address that they control.
- **Internet**—There are many potential risks in exchanging information over the Internet. Although there are common methods for encrypting data between clients and providers, primarily SSL, there is still a danger in how the data is stored and that the data might be compromised in any number of ways.

Identity theft over the Internet is an area of focus for the Identity Management arena. It is an organization’s responsibility to not only protect identity information, but also to ensure that the organization is able to help in the event that the information is compromised in some way—for example, by ensuring that organizational perimeters are secure and monitored along with being able to provide forensic evidence (log files, audit trails, and so on) should the need arise.

Recent research by students at the Massachusetts Institute of Technology (MIT) found that in a surprising number of cases important and confidential data is not correctly or sufficiently erased from storage before it is released into the public domain. Although non-conclusive so far, the anecdotal evidence is alarming. To undertake their study, the researchers purchased 158 disk drives for less than \$1000. Of the 129 functional drives, there had been little or no attempt to erase information on 28 of these. Many contained a great deal of personal data, including confidential emails. Alarmingly, one of the drives had come from an ATM machine, one contained a year's worth of financial transactions, one contained more than 5000 credit card numbers, and yet another contained confidential medical records.

The Keys of Identity

One way to sidestep potential identity theft is to not use standard information as key identifiers or account names. Many organizations, particularly in the United States, tend to use common social information as identifiers. Almost ubiquitous is the Social Security Number (SSN), assigned to every resident. Arguably, the SSN is in such widespread use that to use it as a sole identifier is at least questionable. Worse still, many online organizations use the SSN as a logon identifier. Interestingly, this situation makes a variation of brute-force hacking quite easy, such that hackers can determine the validity of an SSN.

 Brute force methods of hacking attempt to overwhelm a system by trying many different types of entry. For example, the most common brute force attack is to obtain an account name on a system and use a dictionary of possible passwords to try and “guess” the correct one. This hack works when the system is made unsecured by not setting password lockouts as well as the fact that most people still use common words for their passwords. Consider an ATM card. In this case, the equivalent to a password is a Personal Identification Number (PIN). In most cases, the PIN is only four digits, equaling a *potential* 10,000 possible combinations. If it were achievable, you could try all 10,000 possible combinations; however, ATM machines protect against this scenario by “eating” or “swallowing” the card after a set number of unsuccessful attempts (usually three). The ATM model uses two-part authentication. Essentially, the ATM solution combines “something you have” (the ATM card) and “something you know” (the PIN). Either factor is weak by itself as cards can be stolen and PINs can be guessed (or worse still, written down by the card holder). When combined correctly, however, the solution is less prone to attack.

The introduction of smart cards and further advances in the capabilities of readers (ATMs and similar) will help to eliminate such brute force attacks. Fingerprint and other biometric information will form part of the process as well.

In the case of an organization using SSN or similar for their account identifiers, hackers can attempt to work out “which number works,” as in the following case. On March 6, 2003, it was announced that the University of Austin was compromised by hackers who made off with approximately 59,000 names and SSNs of current and former staff and students.

What this means is that increasingly, organizations that use such identifiers will become increasingly targeted. The question many of these organizations face is whether to spend the money changing their identification, authentication, and authorization processes now or bear the brunt of being compromised. Of course, the answer should be that an organization spends the money now, but many organizations play the risk game to their and their customers' detriment. Of course, the impact on the integrity and perception of the institution will take a significant beating as the result of such a scenario, as the message posted on the University of Texas Web site attests (the message follows and can be read at <http://www.utexas.edu/datatheft/>). It is important to understand the implications of the entire message, as it serves as a severe warning to the importance of secure management of identity data:

The University of Texas at Austin regrets that one of its administrative databases was breached by a deliberate attack through the Internet. Since the security breach was discovered Sunday evening, March 2, the University has devoted all available resources to identifying the origin of the attack and recapturing the data before they could be misused or transmitted. Through this Web site and other means, the University seeks to inform the University community and the public about the University's response as well as the status of personal data exposed in this incident.

The University is grateful for the prompt and expert response of the Travis County District Attorney's Office, the U.S. Department of Justice, and the U.S. Secret Service. In particular the University wishes to call attention to the March 6 statement of United States Attorney Johnny Sutton, "... it does not appear at this time that the information that was obtained from the University database has been disseminated, nor has it been used to the detriment of the persons to whom it rightfully belongs." This statement followed execution of a search warrant on the two residences identified as the source of the attack.

Although the U.S. Attorney's statement is reassuring, the University does not seek to minimize the concern raised by this incident. Accordingly, through this Web site the University makes available several communications mechanisms for concerned individuals, as well as a set of resources for monitoring credit records and protecting your identity.

If you are unfamiliar with the basics of this incident and the University's response, see "Initial Report."

The "Am I Affected" page lists the three ranges of Social Security numbers that were used to attack the University System. A total of 2,670,797 SSNs fall in this range, whereas only 55,200 SSNs were exposed from the University database. If you have had no affiliation with the University, it is highly unlikely that you are affected, even if your SSN falls within range.

If you believe you are affected, or might be affected, we encourage you to complete the online form at "How To Contact Us" so that we are assured of an up to date postal mail and e-mail address for you. The University intends to contact every individual whose Social Security number was exposed by this unfortunate incident.

This Web site will be updated whenever the University is made aware of new information about the progress of the investigation by law enforcement authorities as well as when the University can clarify when and how it will communicate with affected individuals.

Intrusion Detection

As we have just discussed under the identity theft heading, one of the Identity Management–related issues faced by many organizations is determining whether your system is under attack. Commonly today, an intrusion detection system monitors network communications and, using profiles or thresholds, attempts to determine whether a hacker/cracker is attempting to break into a system or cause a Denial of Service (DoS) attack. If the determination is made that intrusion is being attempted, the system might send out alerts (email, SMS, SNMP, page, and so on), log the attack (syslog, NT event logs, custom log file), and/or try to modify the operating parameters (configuration, port numbers, communication speed, and so forth) of the system being monitored in order to prevent or alleviate the attack.

It is important to remember that attacks can come from inside or outside your network. Although many studies say that a majority of attacks or security breaches come from within the organization by insiders, the increasing reliance on the Internet ensures that more connectivity is in place and more doors are being opened to the world outside your network. The question your organization must ask is whether the doors are being secured correctly? The importance of Identity Management to intrusion detection is to help minimize the scope of potential damage in any unauthorized use of a system.

Intellectual Property Theft

Protecting intellectual property is a goal of most Identity Management solutions, even if it is not advertised as such. Intellectual property is defined by the World Intellectual Property Organization (WIPO) in the following way: “Intellectual property refers to creations of the mind: inventions, literary and artistic works, and symbols, names, images, and designs used in commerce.” Intellectual property is essentially intangible assets or resources. Business processes, staff and customer lists, sales data, and research and development activity are all examples of intellectual property. The trend is that Identity Management provides additional security and process around the protection of intellectual property in addition to assets and resources.

Throughout this book, the Identity Management framework has been presented as largely managing resources that are under your direct control. One trend today is that organizations are increasingly concerned with management of resources or assets that go outside of their control, often referred to as proprietary technology or intellectual property.

Granting access to an organization to utilize services or data is a common reason for initiating an Identity Management solution. However, there is the consideration of what happens if the consumer of that data is able to take it outside of the controlled environment. There exists today many mechanisms and standards for the protection of intellectual property, including copyright, trademark, and patent registrations as well as Digital Rights Management (DRM) technologies. The basis of these protections are a cultural acceptance of what these registrations mean in legal terms, and what the results are should the law be broken.

Interestingly, these protections are primarily what would be referred to as out-of-band solutions. That means that the protection is not a part of the actual product or resource that is being used, but rather relies on an almost separate agreement, conducted outside of the transaction that actually takes place. This is the role of contracts such as an End User License Agreements (EULAs) associated with most software sales. The issue with this type of solution is that there is no guaranteed control over the intellectual property unless unauthorized use is detected. Instead, the solution's use is based on trust and belief that the user of the resource will do so in a valid way because of a perceived level of honor, or more likely the potential threat through other means (legal ramifications that can have significant financial and social consequences).

The rise of technology, and specifically the Internet, has created new opportunities for rapid exploitation as well as rapid enforcement or protection of intellectual property. The issues surrounding this are that intellectual property in electronic format (such as documents, music, video, and so forth) are now easily transferable via electronic mechanisms in an unchecked manner—there are many more people who are now able to abuse the out-of-band agreements. Truthfully, it is not so much these agreements that protected intellectual property, but rather the cost of acquiring the intellectual property in a useable format.

The rise of peer-to-peer (P2P) networking solutions has been popularized by both Instant Messaging and file sharing networks. The growth of file sharing has created several identity challenges. Napster provides a perfect example. Although Napster was shut down as a result of legal proceedings, similar solutions have sprouted in its place (Gnutella, OpenNap, FastTrack, and more). Users identify themselves to these networks and connect to other users to download files (primarily copyrighted music and video formats), but there is no real control over the process. Users can define their own name, alias, and so forth, making the tracking of who is using the system more difficult. Ultimately, of course, these users must reside on the Internet somewhere, have an IP address, and have a physical presence that can be tracked. ISPs have recently been subpoenaed to provide logs in order to allow the Recording Industry Association of America (RIAA) to correlate an IP address with a real-world user.

How is this important in the Identity Management market? For many years, organizations have had the goal of protecting assets in isolation. Solutions have evolved through software encryption or license enforcement requiring license keys to unlock and physical security devices such as dongles shipping with a product. To protect documents from unauthorized use or copying, a number of companies have introduced software and hardware solutions to do so, such that the rights of the creator are tied to the asset and can be enforced by tools that want to access or make use of that asset. Essentially, this is known as persistence and is embodied in DRM.

For example, Adobe has introduced protection into its Acrobat solution. Acrobat is a software solution for creating and reading documents. Adobe includes incorporates in this solution basic document protection within the framework for protecting content from copying, printing, and so forth.

In addition, vendors of portal products, document management solutions, and similar are incorporating DRM and SMS principles into their core products in response to enterprise customers asking for “good enough” security at more manageable costs. This natural consolidation of security technology into content servers and document repositories is a significant trend that will brighten IT budgets and dim the fortunes of secure content management systems suppliers. The key is that DRM solutions are also being driven by regulatory compliance (HIPAA and GLBA) and ultra-high-value intellectual property such as product design plans with limited user communities. Each layer of the stratification builds upon previous layers.

Authenticated self-service download of a PDF document over an SSL session provides an audit log of restricted access to content that cannot be easily modified after delivery. Recipients are trusted not to share passwords or abuse the trust relationship.

Secure messaging provides a cryptographically protected push capability to designated recipients with tighter audit capability and tighter desktop security. Implementations consist of software to transparently encrypt and decrypt messages, manage license keys, and allow organizations access when passwords are forgotten.

DRM enforces policy and restricts an end user’s ability to save local copies, print hard copy, electronically forward content, and copy and paste to lift information into another body of work. The implementations involve maintaining a user registry, setting policies for stored content, managing distinct license servers, and providing technical support to business partners. This trend has had a sobering impact on the bottom line for vendors of DRM and secure email products. Consumer-oriented content providers jumped off the DRM bandwagon, while enterprises pulled up short on assuming the extra overhead burdens of complex security systems to limit what business partners can do with online content.

Content and DRM

As well as attempting to control software piracy, electronic copyright protection extends to many other forms of electronic media, such as music, video, and electronic books. Protecting content can take two main forms. The first and most simplistic is to encrypt the source to ensure that it can’t be copied from one place to another, or if it is copied, ensure that it cannot be decrypted elsewhere.

For example, a music CD could be encrypted to prevent it from being copied onto a PC and copied elsewhere or downloaded to MPEG players. The second method of controlling access to copyrighted material is to embed some form of access control into the media itself. This option is designed to allow the material to be copied freely but only accessed if a particular individual has the appropriate access. Access control implies knowledge of the identity of an end user of some form.



“Digital Rights Management (DRM) systems restrict the use of digital files in order to protect the interests of copyright holders. DRM technologies can control file access (number of views, length of views), altering, sharing, copying, printing, and saving. These technologies may be contained within the operating system, program software, or in the actual hardware of a device.”

—DRM & Privacy, Electronic Privacy Information Centre, January 2003

There have been several attempts over the past few years to set standards around DRM systems. The Trusted Computing Platform Alliance (TCPA) was formed by some of the larger vendors who had been working independently on copyright controls. The vendors are Microsoft, Intel, IBM, Compaq, and Hewlett-Packard (the latter two having now merged).

The most concrete and controversial DRM system to be outlined as a part of the trusted computing push is the Microsoft Palladium initiative—now known as Next-Generation Secure Computing Base (NSCB). This initiative is a combination of controls deployed in hardware and in the OS itself. Although this initiative is still in the early stages of development, there are plans to include features such as virus and spam controls as well as an Identity Management store of some form and DRM controls.

Some of the main players in the DRM space have been the music industry, movie producers and distributors, and online book distributors. These players have a desire to protect the intellectual property of the material they offer. They want to capitalize on the broad reach of the Internet without having their products freely copied between third parties. They have formed partnerships with vendors such as Microsoft and worked through the political system to have bills approved to protect their intellectual property.

Regulatory and Compliance Issues

The increasing set of regulatory and compliance challenges have already been discussed throughout the book. Expect these pressures to increase.

Paradoxically, expect privacy issues to both support as well as resist the rollout of Identity Management solutions, primarily in the case of extending Identity Management beyond the organizational perimeter. This is why organizations such as PingID, which, as I mentioned earlier, provides a non-proprietary network through which identity information can be exchanged within a legal framework, will be increasingly important to mediate these issues and support your own rollouts.

Identity Management Appliances

The goal of appliance-based solutions is to offer a secure and focused solution implemented on a system based on a single-purpose appliance architecture. This prevents the possibility that holes in the underlying general purpose OS could compromise the entire system.

Appliances have seen an increasing role in supporting businesses. For example, firewalls are a very prevalent example, wrapping multiple but specific functionality into a black box. This feature appeals to numerous organizations that do not want to spend time implementing specific functionality for their general environments.

Identity Management appliance-based solution vendors also provide authentication services, DNS, DHCP, mail and calendar, and directory stores through appliances. Examples of authentication services include:

- SafeNet's iGate—The iGate combines authentication and encryption capabilities. This functionality lets you manage users' access via a secured browser-based application through the use of a USB-based token, or iKey, and a PIN.
- SingleSignOn.Net Practical PKI and Least Privilege—These solutions offer role-based access control on a dedicated appliance running a hardened OS.

Expect the trend to continue with more Identity Management-specific appliances becoming available over the next few years that offer role-based access controls, provisioning, and so forth.

When looking at these types of devices, one of the common indications that the solution is secure is certification such as FIPS-140 (<http://csrc.nist.gov/publications/fips/>) or ANSI X.9F (<http://www.ansi.org/>). FIPS-140 is a United States government standard (also recognized by the Canadian government) that describes the security requirements for cryptographic hardware and software modules (the most recent and current version is FIPS140-2). ANSI, through the related financial services committee X.9F, is drafting several standards that embrace FIPS-140 to support financial solutions.

Software Licensing Enforcement

As the software industry has grown, there has been an increasing requirement to protect the intellectual property of the software developers. Most products have licensing schemes and enforcement of some form. For example, the open source community has the GNU General Public License (GPL). In order to enforce licenses, there is a need to identify who licenses the software, which is where Identity Management is and will become increasingly important.

Advanced Biometric Applications

An improving area of biometrics focuses on cases in which the user isn't aware of the scan. For example, an airport might have a facial-features scanner designed to trigger based on known terrorists. Equipment could be installed under the floor in order to discover people according to their gait, or even weight, as they walk over them (such systems can distinguish among multiple people walking simultaneously). Body odor and DNA can be extracted from a person's "thermal plume" as they walk under a sniffing system.

Biometrics introduces a huge privacy debate. For the first time, it provides the government with a means to track its citizens in a manner that the citizens cannot avoid. This functionality gives totalitarian governments the ability to tightly control their populations. At the same time, it provides businesses equal opportunity to invade their employees and customer's privacy.

Biometrics is considered to be based upon a single, unalterable identity. A private key, for example, can be destroyed in case it is compromised (through key revocation). However, the features detected by biometric technology are with you for life. Today's authentication is usually through pseudonyms that are only roughly related to who you really are.

The key to biometrics is that they cannot be forgotten; many companies are adopting biometrics as a cost-saving issue because lost passwords are becoming a leading problem in IT departments. Biometric features cannot be passed on from one person to another and are considered extremely difficult to forge. However, biometric verification hardware isn't currently difficult to fool. In fact, several fingerprint readers have been fooled with something as simple as a piece of gelatin.

 For more information about this fingerprint-reader experiment, check out <http://www.counterpane.com/crypto-gram-0205.html#5>.

Even worse, biometrics has a number of other problems. The first is that biometric measurements get worse over time, such that there are no guarantees that biometric measurements are permanent. For example, signatures can and do change over time. An injury can change fingerprints or ocular characteristics. Voice recognition systems fail when people have a cold, and biometric technology doesn't always account for those who don't have the requisite physical features. Over time, weight can change and medical changes can significantly alter measured biometrics. Thus, the future of biometric solutions must ensure that biometric solutions can adequately deal with these sorts of issues. The processes to manage the lifecycle issues of biometrics could therefore be considered as complex as those faced by PKI and certificate lifecycle management, where the issues reside around certificate lifecycle of issuance, renewal, updates, revocation, and removal.

Identity Management Resources

As you dive into planning and deploying an Identity Management solution for your organization, you will benefit from research. Table 6.1 provides areas of interest that relate to Identity Management and where you can find more information about these topics.

Area of Interest	Company/Organization	Web Site
Digital identity commentary	Digital Identity World	http://www.digitalidworld.com/
Electronic privacy	Electronic Privacy Information Center (EPIC)	http://www.epic.org/
	Platform for Privacy Preferences (P3P) Project	http://www.w3.org/P3P/
	Privacy Rights Clearinghouse	http://www.privacyrights.org/identity.htm
DRM	Internet Digital Rights Management (IDRM)	http://www.idrm.org/
	Microsoft Corporation Digital Rights Management site	http://www.microsoft.com/windows/window_smedia/drm.aspx
	Trusted Computing Platform Alliance (TCPA)	http://www.trustedcomputing.org
Software licensing/activation	Microsoft Corporation Software Piracy site	http://www.microsoft.com/piracy/basics/activation/
Identity theft	U.S. government's central Web site for information about identity theft—maintained by the Federal Trade Commission (FTC)	http://www.consumer.gov/idtheft/
	Fight Identity Theft	http://www.fightidentitytheft.com/
	Federal Citizen Information Center	http://www.pueblo.gsa.gov/cfocus/cfjuly2000/focus.htm
	Identity Theft Resource Center (ITRC)	http://www.idtheftcenter.org/
	Cross-border Econsumer.gov—e-commerce complaints	http://www.econsumer.gov/english/

Area of Interest	Company/Organization	Web Site
Information security	Computer Security Institute	http://www.gocsi.com
	The Encyclopedia of Computer Security	http://www.itsecurity.com
	The SANS Institute Online	http://www.sans.org
	The Software Institute's CERT Coordination Center (CERT/CC)	http://www.cert.org
	The World Wide Web Consortium (W3C) Security FAQ	http://www.w3.org/security/faq/www-security-faq.html
	Information Systems Security Association (ISSA) organization	http://www.issa.org
	Information Systems Audit and Control Association and Foundation	http://www.isaca.org
	Internet Security Alliance	http://www.isalliance.org
International privacy resources	Privacy Commissioner of Canada	http://www.privcom.gc.ca/
	The European Union Online	http://europa.eu.int/
	Internet Users Privacy Forum Web site	http://www.iupf.org.uk/
	New Zealand—Office of the Privacy Commissioner	http://www.privacy.org.nz/
	Ontario Information and Privacy Commissioner's Web site	http://www.ipc.on.ca/english/index.htm
	Isle of Man Government Office of Data Protection Registrar	http://www.gov.im/odpr/
	Italian Data Protection Commission	http://www.garanteprivacy.it/garante/navig/sp/index.jsp
	French Data Protection Authority Web site—Commission Nationale Informatique et Libertés	http://www.cnil.fr/uk/index.htm
	The Office of the Privacy Commissioner of Australia's Web site	http://www.privacy.gov.au/
	Swiss Federal Data Protection Commissioner (SDPC)	http://www.edsb.ch/
	Berlin Data Commissioner's Web site	http://www.datenschutz-berlin.de/

Area of Interest	Company/Organization	Web Site
	Hong Kong Special Administrative Region of the People's Republic of China Government Information Center Web site	http://www.info.gov.hk/eindex.htm
	Web site of the Office of the Privacy Commissioner for Personal Data, Hong Kong	http://www.pco.org.hk/
	Web site of the United Kingdom Information Commissioner	http://www.dataprotection.gov.uk/
	Web site of the Data Protection Commissioner of Ireland	http://www.dataprivacy.ie/

Table 6.1: Identity Management resources.

Summary

In conclusion, Identity Management should be part of any organization's current and future framework, even if it is not specifically identified yet. Identity Management intersects with security as well as other parts of the infrastructure and business processes, although it is its own discipline. The desire to quickly and securely deliver new information, capabilities, functionality, and services to customers, partners, suppliers, contractors, and employees is a significant goal and deserves recognition in the technology and budget tables.

The following section summarizes the functional aspects and key steps to be taken toward an Identity Management deployment. In addition, this content restates the value that can be gained from an Identity Management initiative for your organization. Figure 6.1 illustrates the Identity Management components that we've explored in this book as well as relates the business value and the complexity of the components.

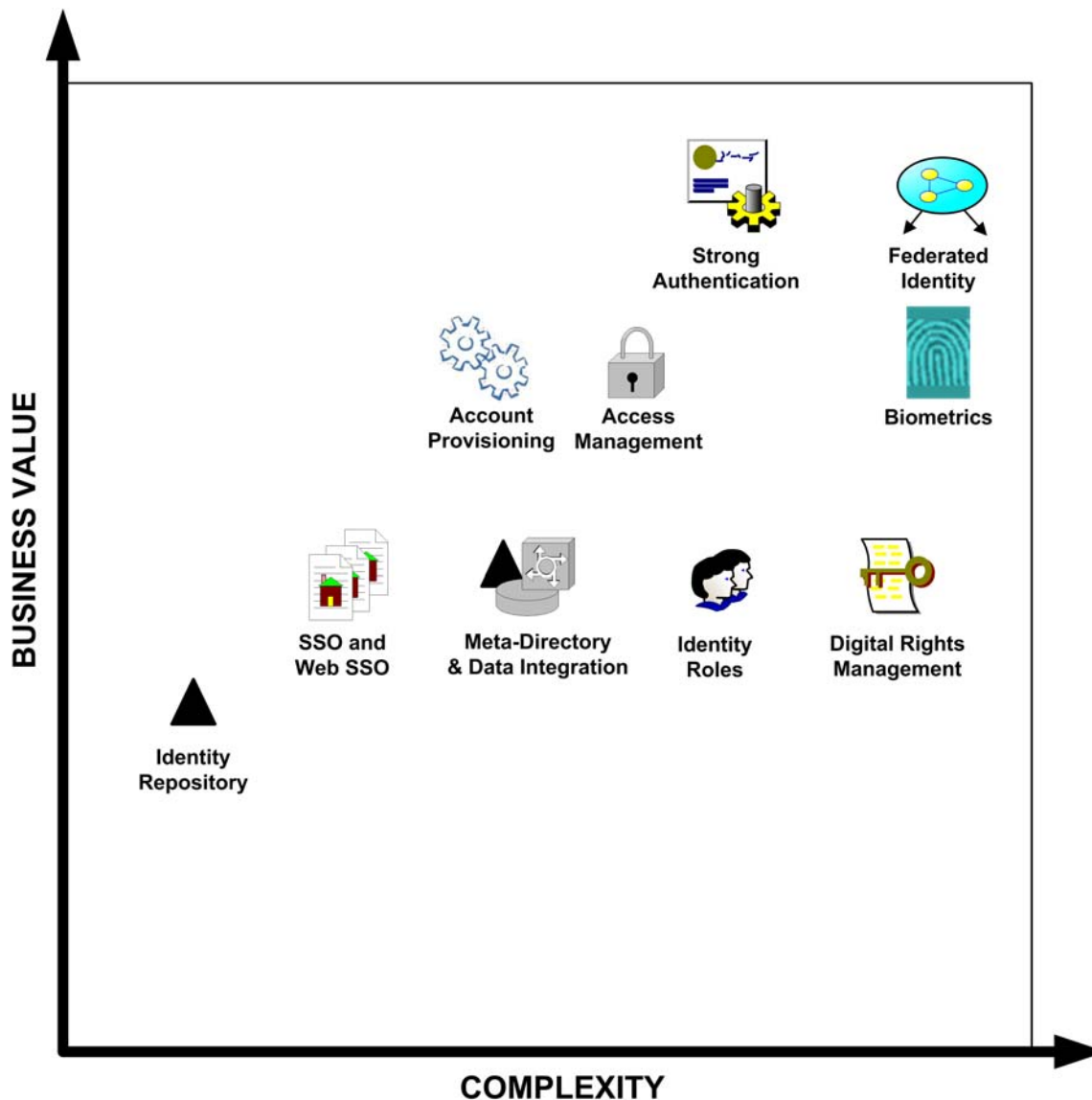


Figure 6.1: The incremental value components of an Identity Management initiative.

As you can see, much can be gained in business value through steps toward a complex but effective Identity Management solution. However, remember that you will benefit only if your infrastructure is useable enough that you can take advantage of the functionality of a complex Identity Management solution.

Although many of the currently available Identity Management solutions claim support for the existing Identity Management standards, and will likely support new standards as they arrive, the clear driver for most organizations is to support and embrace their legacy or heritage applications within an Identity Management framework. Doing so might make it difficult to realize the benefits of the improved standards and solutions as they become available.

As I've stated throughout this book, the following factors are key to the critical success of your organization's Identity Management initiative. During the planning phase and throughout the deployment, you will need to evaluate the process to ensure that your organization meets the following requirements for your Identity Management solution:

- Address core security solutions and key elements
- Ensure management processes are included in the solution
- Manage privacy issues ahead of implementation
- Identify key deliverables such as TCO and ROI
- Identify existing processes and flaws when dealing with management of personal data and related applications and services that require provisioning

We also explored the requirements of implementing your Identity Management solution. The process necessitates people, methods, and focus, as the following list of requisite components highlights:

- Dedicated teams—part time resources do not work
- Methods and tools—the team needs to know what to do
- Tools and enablers—enable efficient implementations

A successful implementation means more than a functioning technology, it requires:

- Organizational alignment
- Process and people integration
- Data integration
- Technical integration
- Roll out and maintenance approach

I hope that the information in this book helps start your organization on its way to a successful and useful Identity Management implementation. Good luck!