realtimepublishers.com™

The Definitive Guide™ 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.

Copyright Statement

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.

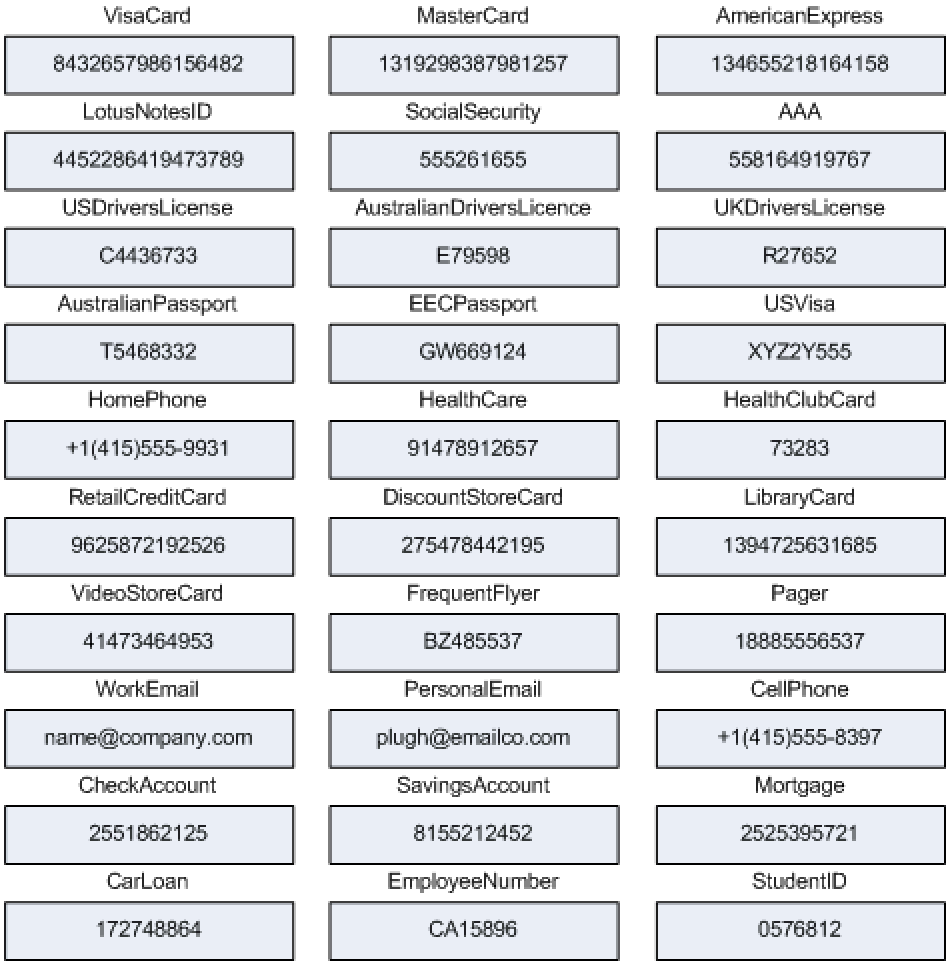
Identity Management Challenges

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 by 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 a 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 facilities 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.