Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

An Introduction to Identity Management

Identity management refers to the process of employing emerging technologies to manage information about the identity of users and control access to company resources. The goal of identity management is to improve productivity and security while lowering costs associated with managing users and their identities, attributes, and credentials. The purpose of this document is to offer a broad overview of current identity management technologies and provide a framework for determining when an identity management system woul...

Copyright SANS Institute
Author Retains Full Rights

AD

An Introduction to Identity Management

Spencer C. Lee

March 11, 2003

SANS Security Essentials Certification
Practical Assignment version 1.4b option 1

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Contents

Abstract....3
The Problem....3
Account setup....4
Account maintenance....4
Account teardown....5
The Business Risks....5
Lower productivity....5
Duplicate and conflicting information....6
Lack of information security....6
Inability to comply with audits and regulations....6
The Challenges of an Identity Management Solution....7
The Functions of an Identity Management System....7
Stores information....7
Authentication and authorization....8
External user registration and enrollment....8
Internal user enrollment....8
Password management....8
Auditing....8
User self-service....9
Central administration....9
Delegated administration....9
The Identity Management Infrastructure....9
Authoritative sources....9
Directory component....9
Directory integration component....10
Provisioning component....10
Access control component....10
Administration component....11
Generalized application interfaces component....11
The Identity Management Solution....11
Directory component....11
Administration component....12
Directory integration component....12
Provisioning component....13
Access control component....13
Is an Identity Management Solution Right For Your Company?....13
Conclusion....14
References....15

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Abstract

Identity management refers to the process of employing emerging technologies to manage information about the identity of users and control access to company resources. The goal of identity management is to improve productivity and security while lowering costs associated with managing users and their identities, attributes, and credentials.

The purpose of this document is to offer a broad overview of current identity management technologies and provide a framework for determining when an identity management system would benefit your company. This document first defines the underlying business problems and resulting business risks inherent in managing user identity information across a heterogeneous technology infrastructure. Next, this document highlights the unique challenges of implementing an identity management solution. This document introduces the functionality of an identity management solution and describes this functionality within the context of the identity management infrastructure. Next, this document highlights products from leading vendors. Finally, a basic framework is provided to help determine if an identity management solution would benefit your company.

The Problem

The underlying problem is the absence of federated directories. Microsoft defines federation as "the technology and business arrangements necessary for the interconnecting of users, applications, and systems. This includes authentication, distributed processing and storage, data sharing, and more."[1] Federated directories interact and trust each other, thus allowing secure information sharing between applications. Companies are currently running isolated, independent directories that neither interact with nor trust each other. This is a result of applications having their own proprietary identity stores. Each proprietary directory requires its own method of user administration, user provisioning, and user access control. This scenario, sometimes referred to as identity chaos, sparks growing problems in a company's technology infrastructure. The problem with proprietary identity stores is that users require a logon for every application, which in turn burdens users with having to remember numerous username and password combinations. The problem with proprietary administration is that every application will have its own set of tools, procedures, and policies to manage users. Therefore, each new application adds a significant burden on the IT staff and unnecessarily complicates a company's identity management infrastructure. The problem with proprietary user provisioning is demonstrated in the amount of time necessary for a user to be given access to the resources needed to conduct business. The problem with proprietary user access control is that it leads to various methods of authentication within the company. Therefore, users are burdened with having to

[1] Microsoft Corporation. "Microsoft's Federated Security and Identity Roadmap" p. 1

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

logon and authenticate multiple times and with various credentials. Due to the functional inability of these current processes, companies are finding it more difficult to manage user identities throughout the identity lifecycle.

The identity lifecycle consists of account setup, maintenance, and teardown.[2] Account setup consists of giving users the appropriate level access to resources necessary to do their job. Account maintenance consists of keeping user identity information up-to-date and to appropriately adjust levels of access to resources needed to conduct business. Account teardown consists of deactivating the user account when the user is no longer affiliated with the company. As companies rely more heavily on computerized systems to run the business, companies are experiencing increased difficulty in efficiently managing user identities at each of these three stages of the identity lifecycle.

Account setup

Companies are experiencing rising costs associated with account setup due to the growing complexity of company resources and the growing variety of users. Company resources are growing in complexity because companies continue to add applications to their information technology infrastructure. Due to the previous lack of identity standards, each individual application or system has its own user identity store to control access to that particular resource. In addition, each proprietary identity store contains a varying degree of identity information (e.g. name, title, employee ID). As a result, each application has its own method for managing user accounts (e.g. scripts, applications, Web-based tools). For example, personal identity information is entered in various resources such as network operating systems, human relations databases, payroll databases, and email directories. User access rights are assigned in a range of resources that include network operating systems, intranets, electronic commerce applications, enterprise resource planning applications, and customer relationship management applications. It is now clear that users have a potentially long list of resources with which they need to be integrated with. To complicate matters further, companies are now interacting with a growing variety of internal and external users that need access to company resources. Internal users include employees, temporary employees, and contractors. External users include customers, vendors, and business partners. Each type of employee requires its own account setup process. Thus, the account setup process takes longer, the IT staff devotes more time to this process, and the users lose productivity while they wait to receive access to the resources needed for them to begin work.

Account maintenance

Companies are experiencing rising costs associated with account maintenance due to forgotten passwords and access rights errors caused by incorrectly setup accounts. For companies with more than $500 million in annual revenue, META

[2] M-Tech, page 5.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

group research shows that 45% of total calls to the average help desk are for password reset assistance.[3] When users forget passwords they contact the IT help desk to have their passwords manually reset. Password resets consume a large part of the IT help desk's time. For companies with more than $500 million in annual revenue, META group research shows that 11% of employees will experience an access rights issue per month.[4] Users who experience access rights errors also contact the IT help desk to resolve configuration errors made during the account setup process. In these situations the IT help desk usually must first collaborate with other departments to find out how the user access rights should be configured, trace the configuration error, and then fix the problem. Because this process involves communication with other departments, there is an increased burden to the IT help desk and the company as a whole.

Account teardown

Companies are experiencing rising costs associated with account teardown because of the lack of account documentation and increased urgency involving adverse terminations. Often times there is no documentation as to what privileges and access rights a user has been given. Even if normal processes produce documentation, situations with time constraints lead to rights and privileges being assigned ad hoc without going through the normal documentation processes. Consequently, it is almost impossible to find complete documentation listing every resource that any given user has access to. To reduce the security risk involved with a terminated account, normally all access must be revoked within a few of days. However, certain adverse terminations require that user access be immediately revoked. For example, an adverse termination of a company executive, manager, or IT staff member may require that user access be revoked by the time the person is escorted out of the building.

The Business Risks

The business risks associated with the current user management techniques are lower productivity, duplicate and conflicting user information, lack of information security, and difficulty in evaluating regulatory compliance. All of the aforementioned business risks result in increased costs.

Lower productivity

The loss of productivity is caused by the amount of time it takes to execute routine account management tasks such as password resets, changing identity information, and provisioning access to resources. For example, for companies with more than $500 million in annual revenue, META group research shows that

[3] Meta Group Inc., p.9
[4] Meta Group Inc., p.6

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

the average time to complete a user provisioning request is 6 to 29 hours.[5] The lower productivity of the IT help desk also affects the user, who has to wait to gain access to resources.

Duplicate and conflicting information

Due to the number of identity stores, duplicate and conflicting user information threatens the quality of customer service and reduces productivity due to erroneous data. For companies with more than $500 million in annual revenue, META group research shows that, on average, internal user information is stored in 22 different identity data stores and external user information is stored in 6 different identity data stores.[6]

Lack of information security

Lapses in information security are a result of inefficiencies in current identity management processes. Due to the difficulty in managing user identities, the IT staff usually does not have enough time to correctly manage identities. For example, users can be granted too much access because it is the easy thing to do. Because the IT staff does not have time to interpret how security policies affect each user, users can be granted access rights in violation of company security policies. Because the priority of the IT staff normally lies with new and existing, terminated users can easily be ignored. Consequently, departing employees find that they can still access company resources through their old accounts, other orphaned accounts, or undocumented access points.

Inability to comply with audits and regulations

Companies can experience difficulty in meeting audit requirements or complying with government regulations due to lack of properly identified users, their roles, and their associated resources.[7] A failure to meet audit requirements may negatively affect the company's reputation and prevent business expansion. Before establishing relationships with other business often times each party will require an independent review of the controls and safeguards the other party has in place to protect the confidentiality, integrity, and availability of data. This type of audit, known as the Statement on Auditing Standards Number 70 (SAS 70), can be a necessary component in negotiating projects that require information sharing between companies. A failure to comply with government regulations may threaten the viability of a company. Significant government regulations include the Health Insurance Portability and Accountability Act of 1996 (HIPPA) in the healthcare industry and the Gramm-Leach-Bliley Act of 1999 in the financial services industry.

---

[5] Meta Group Inc., p.5
[6] Meta Group Inc., p.3
[7] Amendt, p.5

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

The Challenges of an Identity Management Solution

Significant challenges exist for an identity management solution because in order for it to achieve a positive return on investment it must be reliable, flexible, secure, and user-friendly. The solution must be reliable because if it were to fail business would cease. As a result, the solution must be designed in a way to provide redundancy and automatic failover during any number of unpredictable events. The solution must be flexible because every company will have specific business, technical, and operational requirements. In addition, there are different kinds of identity data such as personal information, legal information, logon credentials, etc. Furthermore, the identity lifecycle: setup, maintenance, teardown, is different for every user. The identity management solution must be adaptable to numerous applications (e.g. ERP, CRM, HR, email) and devices (e.g. pagers, PDAs) that need to be integrated within the system. The solution itself must be secure because it hosts confidential data and it ensures the security of corporate resources. The identity management system acts as the backbone for access control and security, and if it were to be compromised then the security of the entire company would also be compromised. Therefore, it must encrypt stored confidential information such as social security numbers and passwords. It must also encrypt confidential information during transmission between components of the identity management infrastructure, which includes the network transmissions during synchronization, replication, and authentication. In addition, the identity management software must reside on security-hardened servers and be a part of a secure networking environment. The solution must be user-friendly because it will extend to external users such as customers and business partners that will expect a friendly, intuitive interface.

The Functions of an Identity Management System

The identity management system stores information on all aspects of the identity management infrastructure. Using this information, it provides authorization, authentication, user registration and enrollment, password management, auditing, user self-service, central administration, and delegated administration.

Stores information

The identity management system stores information about the following resources: applications (e.g. business applications, Web applications, desktop applications), databases (e.g. Oracle, DB2, MS SQL Server), devices (e.g. mobile phones, pagers, card keys), facilities (e.g. warehouses, office buildings, conference rooms), groups (e.g. departments, workgroups), operating systems (e.g. Windows, Unix, MVS), people (e.g. employees, contractors, customers), policy (e.g. security policy, access control policy), and roles (e.g. titles, responsibilities, job functions).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Authentication and authorization

The identity management system authenticates and authorizes both internal and external users. When a user initiates a request for access to a resource, the identity management first authenticates the user by asking for credentials, which may be in the form of a username and password, digital certificate, smart card, or biometric data. After the user successfully authenticates, the identity management system authorizes the appropriate amount of access based on the user's identity and attributes. The access control component will manage subsequent authentication and authorization requests for the user, which will reduce the number of passwords the user will have to remember and reduce the number of times a user will have to perform a logon function. This is referred to as "single sign-on" or "reduced sign-on." A realistic goal for an identity management system is to enable single sign-on for all Web applications, but it is currently unrealistic to provide single sign-on functionality for all applications across the enterprise.

External user registration and enrollment

The identity management system allows external users to register accounts with the identity management system and also to enroll for access privileges to a particular resource. If the user cannot authenticate with the identity management system the user will be provided the opportunity to register an account. Once an account is created and the user successfully authenticates, the user must enroll for access privileges to requested resources. The enrollment process may be automated based on set policies or the owner of the resource may manually approve the enrollment. Only after the user has successfully registered with the identity management system and enrolled for access will access to that resource be granted.

Internal user enrollment

The identity management system allows internal users to enroll for access privileges. Unlike external users, internal users will not be given the option to register because internal users already have an identity within the identity management system. The enrollment process for internal users is identical to that of external users.

Password management

The identity management system allows for password management. Users are able to reset their own passwords and synchronize passwords across multiple systems. The IT help desk is also able to reset passwords on behalf of users.

Auditing

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

The identity management system facilitates auditing of user and privilege information. The identity management system can be queried to verify the level of user privilege. The identity management system provides data from authoritative sources, providing auditors with accurate information about users and their privileges.

User self-service

The identity management system allows users to maintain their own personnel information and perform certain routine account tasks. For example, users can update their personal contact information, change their passwords, or synchronize passwords across all systems. If necessary, the changes can be validated before the appropriate authoritative sources are updated.

Central administration

The identity management system allows administrators to centrally manage multiple identities. Administrators can centrally manage both the content within the identity management system and the structural architecture of the identity management system.

Delegated administration

The identity management system allows delegated administration, so that administrators can manage identities for which they are responsible. Delegated administrators are not able to make any structural changes to the identity management system. Delegated administrators are only able to manage the information stored in the identity management system.

The Identity Management Infrastructure

The identity management infrastructure consists of many authoritative sources, a directory component, an administration component, a directory integration component, a provisioning component, an access control component, and a generalized application interfaces component.

Authoritative sources

The authoritative sources are the point where identity data originates. For example, an authoritative source for user's contact information may be an existing human resources database. An authoritative source for a user's email address would be the company email application.

Directory component

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

The main component of the identity management solution is the directory. The directory component stores identity and resource information, policies, and user credentials. It provides a logical architecture to define schemas and namespaces. It protects the confidentiality, integrity, and consistency of identity data as well as provides for monitoring and auditing of its data. LDAP, which is based on the ISO X.500 specification, is the emerging directory standard. Using the LDAP protocol, any application running on any platform can query and access data stored in the LDAP directory via TCP/IP. LDAP can be implemented over HTTP to leverage Internet communications. If sensitive communication needs to be secured, LDAP can be implemented over SSL or TLS. The administration component, directory integration component, provisioning component, and access control component interact directly with the directory.

Directory integration component

The directory integration component has two main functions. First, it facilitates the bi-directional flow of information due to synchronization of changes between the directory and other identity stores. This is done using meta-directory services, custom scripts, or import/export utilities. Although user accounts may be stored in various sources scattered across a heterogeneous environment, the directory integration component can create a unified view of user account information. Second, it processes the unidirectional flow of data coming from authoritative sources and transfers the data into the identity management system.

Provisioning component

The provisioning component provides the tools to manage user and application access to resources. The three main functions of this component are to efficiently provision users, de-provision users, and manage provisioning policies. Users are provisioned with the appropriate amount of access based on company-defined application definitions. Application definitions define the appropriate amount of access required to perform a specific business process. Application definitions may specify access to multiple resources. Users may be assigned to any number and combination of application definitions. Users are de-provisioned rapidly because the component knows what the user has been provisioned. Users are effectively de-provisioned if their account is disabled or if their application definitions are removed. Provisioning policies can be centrally administered to ensure that policies are applied universally and uniformly.

Access control component

The access control component provides management of authentication and authorization methods. The access control component relies on policies and allows for Role Based Access Control. Role Based Access Control manages

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

user access based on a grouping of functions, rules, or privileges. This component tracks user sessions to maintain state and conserve bandwidth.

Administration component

The administration component provides the tools to manage directory entries. The administration component provides a framework to delegate administration to certain departments, business partners, or users themselves. This component allows users to reset their own passwords. Customized application interfaces can be tailored to each user, which helps to ensure that users are only given the least amount of privilege necessary.

Generalized application interfaces component

The generalized application interfaces component allows developers to interact with the identity management system without having to interface directly with vendor-specific application interfaces. There is a directory integration interface, provisioning interface, access control interface, and an administration interface. The directory integration interface facilitates the one-way data flow and data conversion from the authoritative sources to the directory component of the identity management system. The provisioning interface transfers data from the directory component to the systems to which it provisions. This data transfer may be based on developing standards such as SPML (Service Provisioning Markup Language). The access control interface passes user credentials to the access control component. The administration interface passes information between any components of the identity management system. There may not be an administration interface to allow communication between any two components.

<u>The Identity Management Solution</u>

The identity management solution consists of various software packages, often times coming from different vendors. Companies tend to select "best-of-breed" products that address five of the seven components of the identity management infrastructure: directory, administration, directory integration, provisioning, and access control. The generalized application interfaces component is not included in the solution because it is custom developed after the software packages are selected. The generalized application interfaces component is not provided by any vendor, but is instead created by each company to address the specific identity management solution that is implemented. Authoritative sources are not included in the identity management solution because they already exist in your company as the directories, databases, and applications that act as “systems of record” for the information they contain.

Directory component

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

For the directory component, the leading vendor offerings are Microsoft Active Directory, Novell eDirectory, Sun ONE Directory Server, and IBM LDAP Directory Server. As of version 1.0, Microsoft Active Directory provides strong integration with Windows 2000 and benefits from its easy-to-use graphical administrative utilities. Active Directory is gaining popularity in the enterprise, and many vendors are building support for Active Directory in their products. As of version 8.6.2, Novell eDirectory boasts a feature-rich, mature directory technology. In addition, it runs on various operating systems and is very scalable. eDirectory supports online maintenance of such tasks as replication topology modification and backups. As of version 5.1, Sun ONE Directory distinguishes itself as a market leader in e-business directories, and is often considered the de facto standard for e-business Web applications. It is a flexible, general-purpose directory. There is a large developer support for the Sun ONE Directory. As of version 4.1, IBM LDAP Directory boasts strong support for Java, J2EE, LDAP v3, and HTTP/SSL. It leverages IBM's DB2 database as the identity repository.

Administration component

For the administration component, the leading vendor offerings are Netegrity Delegated Management Services (DMS), Oblix COREid, RSA ClearTrust, and Tivoli Web Portal Manager. As of version 2.0, Netegrity DMS boasts the capability for numerous levels of delegated administration. As of version 5.2, Oblix COREid is considered the industry leader in delegated administration due to its functionality and usability. COREid provides delegated administration for the directory component, provisioning component, and access control component using one tool. COREid allows for the temporary assignment of responsibilities while employees are on vacation. COREid provides a customizable workflow process that can implement, approve, and execute many tasks. As of version 4.7, RSA ClearTrust benefits from a parametric rules engine that uses a decision tree for calculating complex authentication and authorization decisions. ClearTrust also benefits from RSA's encryption technologies, which are embedded to offer strong support for encryption and PKI. As of version 3.9, Tivoli Web Portal Manager provides Web-based tools for basic functionality out of the box. Development tools are provided for customization of user interfaces and functionality.

Directory integration component

For the directory integration component, the leading vendor offerings are Microsoft Meta-directory services, Critical Path Metadirectory, Novel DirXML, and Tivoli/MetaMerge Integrator. As of version 2.2, Microsoft Meta-directory Service offers strong integration Active Directory. As of version 3.3, Critical Path Meta-Directory is considered the market leader in meta-directories. It boasts strong integration with relational database management systems such as Oracle and DB2. As of version 1.1, Novell DirXML offers flexibility and support for

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

heterogeneous environments. Tivoli MetaMerge Integrator offers rapid deployment and lightweight design that utilizes any LDAP v3 directory.

Provisioning component

For the provisioning component, the leading vendor offerings are BMC CONTROL-SA, WaveSet Lighthouse, and Tivoli Identity Manager. As of version 3.7, BMC CONTROL-SA boasts the largest install base, strong support for legacy platforms, and bi-directional synchronization with agent software modules. As of version 1.6, WaveSet Lighthouse architecture facilitates rapid deployment and scalability. In addition, Lighthouse benefits from Waveset's industry leadership in developing the SPML provisioning standard. As of version 1.1, Tivoli Identity Manager provides Web self-service tools, a single point monitoring and control of access rights, and embedded workflow and policy-based provisioning.

Access control component

For the access control component, the leading vendors are Netegrity SiteMinder, Oblix NetPoint, RSA ClearTrust, and Tivoli Access Manager. As of version 5.0, Netegrity SiteMinder supports a wide variety of authentication methods that can be combined to create various levels of security. Netegrity is considered to be the market leader and has a large install base. As of version 5.2, boasts fine-grained access management that can specify fields within an application. As of version 4.7.1, RSA ClearTrust is directory-enabled and benefits from RSA's encryption technologies. As of version 3.9, Tivoli Access Manager offers broad supports a variety of authentication methods, manages user sessions on a WebSeal Server instead of on client-side cookies, and supports wireless users.

Is an Identity Management Solution Right For Your Company?

The first step in determining whether an identity management solution is right for your company is to evaluate your company's current identity management infrastructure. To help simplify this evaluation, Sun offers a simple "Network Identity Capability Assessment Tool" in their white paper "Network Identity Capability Assessment" (URL: http://wwws.sun.com/software/sunone/wp-readiness.pdf) on appendix page iii-viii. This tool consists of a report card with questions regarding an organization's current capabilities and the identity benefits provided with each capability.

The following characteristics are good signs that your company should consider an identity management solution:

- Users have more than six username and password combinations
- It takes more than one day to setup and provision an account for new employees

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- It takes more than one day to revoke all access and disable the account for terminated employees
- Access to critical resources cannot be restricted
- Access to critical resources cannot be audited or monitored
- Your company generates at least a couple million dollars of annual revenue

A very common method of evaluating any investment is to calculate the return on investment. The first step in calculating your ROI is to estimate your cost savings. A survey by Meta Group Consulting of 420 companies with annual revenue of at least $500 million estimated a potential average saving of $4,395,081.60 per year.[8] The cost of an identity management solution will run in the millions of dollars. To help in your ROI calculation, Waveset Technologies, Inc., an identity management vendor, offers an ROI calculator on their Web site (URL: http://www.waveset.com/Solutions/Resources/roi_calculator/index.html).

The identity management solution is expensive, complicated, and will be unique for every organization. The identity management solution will require several years to plan and implement, and as a result requires a high level of management support and organizational commitment. If your company is considering an identity management solution, the best course of action will be to seek advice from a third-party identity management consulting firm like Deloitte & Touche or PricewaterhouseCoopers. Reputable consulting firms will help your company evaluate the need for an identity management solution, define the scope of the project, plan the architecture and design of the solution, select vendors, and implement and integrate the solution into your company's infrastructure. Deloitte & Touche offers their own i-MAAP™ methodology that consists of identity Management, Authentication, Authorization, and Protection[9]. PricewaterhouseCoopers breaks up its identity management methodology into several main categories: permission and policy management, enterprise directory services, user authentication, user provisioning, and workflow.[10]

Conclusion

The ultimate goal of an identity management solution is to create federated identity systems so users can be effectively identified and provisioned across company boundaries. Using federated identities, information can be securely shared between companies, enabling employees to access another company's data without manually re-authenticating. This is made possible by leveraging Web single sign-on technology included in each company's identity management solution. Aberdeen concludes that federated identity systems "are the next logical evolution in authentication and entitlement system."[11] However, only after

[8] Baseline, p.1
[9] Amendt, p. 9
[10] Schlarman, p. 8
[11] Aberdeen, p.10

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

your company has the technology, infrastructure, and processes in place to effectively manage internal resources can your company begin to share and manage identity information with other companies. Thus, the first step towards a federated identity system is to implement an identity management solution in your company.

The identity management solution offers tangible results by increasing productivity and security while at the same time lowering the costs associated with trying to manage the identity chaos that has resulted from the influx of standalone applications. As the Internet continues to open new doors of business opportunity, it concurrently exposes the insecurities of corporate networks. Large enterprises are concluding that an identity management solution, alongside an enterprise-wide security strategy, is necessary to ensure the confidentiality, integrity, and availability of critical resources.

References

Aberdeen Group, Inc. "Federated Identity Systems."
URL: http://wwws.sun.com/software/sunone/wp-federatedid.pdf (26 Jan 2003)

Amendt, Bruce. Deloitte & Touche LLP. "Identity Management and Portal Security." Sept. 2002.
URL: http://www.isacaaustin.org/presentations/sep02.pdf (26 Jan. 2003)

Arevolo, Waldir. Gartner Research. "Identity and Access Management: Foundation for Next Generation Businesses.
URL: http://www.novell.com/brasil/sim/gartner.pdf (28 Jan. 2003)

Baseline Magazine. "What Price, Identity Management?" Baseline Magazine. 1 August, 2002.
URL: http://www.baselinemag.com/article2/0,3959,656089,00.asp (9 Feb. 2003)

Byrnes, Christian. "Who Goes There?" Optimize. October 2002, Issue 12.
URL: http://www.optimizemag.com/issue/012/roi.htm (9 Feb 2003)

Desmond, Paul. "Identity Management Combines Security, ROI." July 8, 2002.
URL: http://www.esecurityplanet.com/views/article.php/10752_1381381 (26 Jan. 2003)

Durbidge, Phil. WRDC. "Metadirectories." 22 May 2002.
URL: http://www.wrdclogsys.com/docs/whitepapers/MetaDirectories%20White%20Paper.pdf (28 Jan. 2003)

Ehrsam, Time. Oracle Corporation. "Directories: The Centerpiece for Enterprise Management."
URL:http://www.oft.state.ny.us/security/electronic%20presentations/conference2000/Directory_pres.pdf (26 Jan 2003)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

ePresence Inc. "An Introduction to Secure Identity Management." White Paper version 2.0. July 2002.

ePresence Inc. "What is eProvisioning?" Directions. Summer 2001.
URL: http://www.nd.edu/~eds/docs/other/olddocs/White_Papers/ePresence_eProvisioning.pdf (26 Jan 2003)

Gartner Research. "2H02 Metadirectory Service Market Magic Quandrant." Research Note 19 August 2002.

Gartner Research. "ROI Drives Identity Management and Access Management Implementation." Research Note 3 Dec 2002.

Gartner Research. "User Provisioning – Automated Accounts and Access." Research Note 2 Oct 2002.

Lewis, Jamie. "Directory Services Morph Into Enabler For Other Apps." Internet Week. 26 Nov. 2001.
URL: http://www.internetweek.com/graymatter/lewis112601.htm (28 Jan. 2003)

Meta Group Inc. "The Value of Identity Management: securing identity management provides value to the enterprise." August 2002.
URL:
http://www.pwcglobal.com/Extweb/service.nsf/8b9d788097dff3c9852565e00073c0ba/88a387cdb58b4c0085256c6a006e0036/$FILE/ValueofIMWhitePaper.pdf (26 Jan. 2003)

Microsoft Corporation. "Identity Management."
URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/ittasks/architect/idman.asp (26 Jan. 2003)

Microsoft Corporation. "Microsoft's Federated Security and Identity Roadmap."
URL: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnwebsrv/html/wsfederate.asp (2 Mar. 2003)

M-Tech Information Technology, Inc. "Defining Enterprise Identity Management."
URL: http://www.psynch.com/docs/what_is_identity_management.html (26 Jan. 2003)

PriceWaterhouseCoopers LLP. "Identity Management: The Business Context of Security." January 2002.
URL:
http://www.pwcglobal.com/extweb/newcoatwork.nsf/docid/9FBA7A678F38F43885256B12007D5EA9 (26 Jan. 2003)

Schlarman, Steve, and Brian Jensen. PricewaterhouseCoopers.
"Security as a Business Process: A Framework for Information Security and Identity Management."
URL: http://csiannual.com/pdf/c1.pdf (23 Feb. 2003)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Shillito, Peter. "Identity Management - Delivering Security and Value." 12 June 2002.
URL: http://www.infosecnews.com/opinion/2002/06/12_04.htm (26 Jan. 2003)

Sun Microsystems, Inc. "How to Implement Network Identity."
URL: http://wwws.sun.com/software/sunone/wp-implement_ni.pdf (26 Jan 2003)

Sun Microsystems, Inc. "Network Identity Capability Assessment."
URL: http://wwws.sun.com/software/sunone/wp-readiness.pdf (26 Jan 2003)

Sun Microsystems, Inc. "Strategic Implications of Network Identity."
URL: http://wwws.sun.com/software/sunone/wp-identity.pdf (26 Jan 2003)

Sun Microsystems, Inc. "Sun ONE Identity Management."
URL: http://wwws.sun.com/software/sunone/wp-identity_mgnt.pdf (26 Jan 2003)

Waveset Technologies, Inc. "Return on Investment (ROI) Calculator."
URL: http://www.waveset.com/Solutions/Resources/roi_calculator/index.html (9 Feb 2003)

Yasin, Rutrell. "What is Identity Management?" Information Security Magazine. April 2002.
URL: http://www.infosecuritymag.com/2002/apr/cover_casestudy.shtml (26 Jan. 2003)

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: September 4th, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
Security Leadership Summit & Training	Dallas, TXUS	Dec 03, 2015 - Dec 10, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced