GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Identity and Access Management Solution

GIAC Security Essentials
Certification (GSEC)
Practical Assignment
Version 1.4c

Option 1 - Research on Topics
in Information Security

Submitted by: Martine LINARES on February 14, 2005
Location: SANS Conference – Amsterdam – September 2004

To securely manage the end-to-end identity life cycle while protecting corporate resources, organizations must adopt a complete, integrated, modular approach to manage users and control resource access.
This paper is an overview of Identity and Access Management solution. It shows how the challenges of today's word and the strength of government regulations have moved up organizations to a comprehensive approach to managing account identities and controlling access to their resources. This overview is illustrated by one of many vendor solutions: "Microsoft Identity and Access Management Series".

© SANS Institute 2000 - 2005 Author retains full rights.

Table of Contents

1 Introduction 3
2 Business challenges 3
2.1 Extend access to information systems 3
2.2 Create relationships with different identities 4
2.3 Manage multiple passwords 4
2.4 Manage users' life-cycle 4
2.5 Implement auditing requirements 5
3 Federal regulations 5
3.1 Health Insurance Portability and Accountability Act (HIPAA) 5
3.2 Food and Drug Administration (FDA) 21 Code of Federal Regulations (CFR) Part 11 6
3.3 Gramm-Leach-Bliley Act (GLB) 6
3.4 Sarbanes-Oxley Act (SOA) 7
4 Identity and Access Management concept 8
4.1 Directory Services 9
4.2 Identity Life Cycle Management Services 10
4.2.1 Provisioning services 11
4.3 Access Management Services 11
4.3.1 Authentication 12
4.3.2 Authorization 12
4.3.3 Federation and Trust 14
4.4 Security Auditing 14
5 Microsoft Identity and Access Management Series overview 14
5.1 Directory Services 16
5.2 Identity Life-Cycle Management 16
5.3 Access Management 16
5.3.1 Authentication 16
5.3.2 Authorization 18
5.3.3 Trust 18
5.4 Security Auditing 19
6 I&AM deployment challenges 19
6.1 Scope, Schedule and Cost 20
6.2 Assessing the current environment and I&AM 20
6.3 Interoperability 20
6.4 And also Scalability, Manageability… 21
7 Conclusion 21
8 References 22

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

List of Figures

Figure 1: I&AM general description 9
Figure 2: Metadirectory concept 10
Figure 3: Processes and services in the Microsoft Identity and Access Management Framework 15
Figure 4: The authentication API and protocol hierarchy in the Windows operating system 17
Figure 5: Windows 2003 forest trust relationships 19

© SANS Institute 2000 - 2005, Author retains full rights.

1 Introduction

To meet the challenges of today's world, competitive companies need to increase their business agility in a secure environment and need to enforce the performance of their IT infrastructure. With the development of e-business, enterprises now require new methods to manage secure access to information and applications across multiple systems, delivering on-line services to employee, customer and suppliers without compromising security. Companies must be able to trust the identities of users requiring access and easily administer user identities in a cost-effective way.
During these last two years, an emerging concept: the Identity and Access Management (I&AM) solution has been developed, based on the users and access rights management through an integrated, efficient and centralized infrastructure. This concept combines business processes, policies and technologies that enable companies to:

- provide secure access to any resource,
- efficiently control this access,
- respond faster to changing relationships,
- protect confidential information from unauthorized users.

This paper illustrates the business challenges of today's world, what constraints impose the main US regulations, explains the principles of Identity and Access Management solution, gives an example of such solution through a major vendor product: "Microsoft Identity and Access Management Series" and lists the main challenges in deploying this solution.

2 Business challenges

During the last few years, organizations have developed their business through the Internet, which increases access to their network. This creates a challenge of maintaining two opposite constraints: being more flexible and keeping a secure environment. This section lists the main challenges, in term of identity and access management, of today's organizations, coming from an outdated security model.

2.1 Extend access to information systems

For doing business, enterprises have to "open" their network, first to customers, but also to partners. More and more users and applications bring a critical concern to these enterprises which is to ensure and maintain the security of assets and privacy protection [1], while identifying authorized parties. To realize these operations, enterprises need efficient management tools and security policies. The absence of a centralized method for managing accounts and

[1] Identity Management in a Virtual World
ftp://ftp.ealaddin.com/pub/Marketing/eToken/White_Papers/WP_IDC/IDC%20Whitepaper_ID%20Mgmt%20in%20Virtual%20World_June%202003.pdf

© SANS Institute 2000 - 2005 Author retains full rights.

accesses is a source of operational risks.

2.2 Create relationships with different identities

Organizations may have to manage on-growing relationships with different types of communities: employees, customers and business partners [2]. All these kinds of populations have different needs. For employees, focus is done on productivity, which means quick access to the right resources. For customers, one critical point is the web access security including ease of use and private data and transaction confidentiality [2]. At last, for business partners, the priority is the definition of trust models and bilateral agreements [2] to allow access to confidential information between each organization.
Without an integrated identity and access management approach involving both IT systems and Web services, enterprises will not be able to correctly manage security for these different populations.

2.3 Manage multiple passwords

As the number of business applications has proliferated, users and system administrators are faced with a wide number of passwords to do their job. As well as being time consuming for a user to sign in to different operating systems, directory services or applications, the high number of passwords and user names increase Helpdesk costs when processing password-related requests. Another problem with password proliferation is to put in place a strong password policy to avoid easy-to-guess passwords or prevent users to write on paper “Hard-to-Guess passwords” [3]. In this situation, organizations need to place the emphasis on an efficient logon methodology.

2.4 Manage users’ life-cycle

The fast growth of the user population makes the task of managing users more complicated. Within wider environments, enterprises have to efficiently manage each individual user’s life-cycle, as well as keeping control of security, despite frequent job turn over. Creation of new accounts with appropriate privileges to adequate resources, and modifying privileges associated to a user when his job role changes or disable outdated accounts for employees/contractors/partners/customers when these accounts are no longer needed, have to be performed efficiently and in a secure way [4]. If not, this can result in an unmanageable number of permissions, loss of productivity and might lead to major security issues.

2.5 Implement auditing requirements

To meet new regulatory requirements (see Federal regulations section for more

---

[2] eTrust Identity and Access Management Suite- Page 3
http://www3.ca.com/Files/WhitePapers/etrust_identity_access_mgmt_suite_wp.pdf

[3] Track 1 - SANS Security Essentials. Defense-In-Depth - Page 186

[4] Track 1 - SANS Security Essentials. Secure Communications - Page 284

© SANS Institute 2000 - 2005 Author retains full rights.

details), organizations have to provide the evidence (auditable proof) that user access is based on justified business needs (privileges principle). They must ensure they control and audit the process transactions of conducting business inside and outside their organization. A major focus for enterprises is to be able to prove that authorized users access the right Web services, files or databases. Moreover gathering audit logs from different security systems of multiple applications and data repositories is a huge task for IT managers and it quickly becomes unmanageable without a centralized solution.

3 Federal regulations

Adding to previous business challenges, many new governmental or federal regulations have been introduced in recent years, growing focus on privacy, protection and auditing [5]. Being compliant with these regulations becomes a priority for enterprises, to gain new market opportunities and prevent significant financial and legal liability.
These laws address different topics of IT security, such as protecting confidentiality of private information, or requiring the documentation of financial decisions and transactions. However all these regulations have one point in common: they place emphasis on the security of the IT infrastructure.
This section lists the main US regulations promulgated recently in financial, health care or pharmaceutical domains which have an impact in term of identity and access management.

3.1 Health Insurance Portability and Accountability Act (HIPAA)

HIPAA is a US law which came into effect in 1996. It provides a standard for electronic health care transactions over the Internet. As the integrity and confidentiality of patient information is critical, this requires being able to uniquely identify and authenticate an individual. HIPAA has strict guidelines on how healthcare organizations can manage private health information. This includes [6]:

- Authentication: An unique identification for individuals using the health care system
- Access control: Manage accounts and restrict access to health information
- Password management: Centrally define and enforce a global password policy
- Auditing: Centralize activity logs related to the access of health information

[5] Track 1 - SANS Security Essentials. Secure Communications - Page 282

[6] HIPAA Compliance and Identity & Access Management, http://www.evidian.com/newsonline/art040901.php

© SANS Institute 2000 - 2005 Author retains full rights.

- Secure communication: Implement standards and procedures for the electronic transmission and authentication of signatures

There is no unique solution to address all the privacy requirements of HIPAA [7], but the bottom line is that a centralized solution, such as I&AM, can greatly help enterprises to be compliant to this law in a cost effective and coherent manner.

3.2 Food and Drug Administration (FDA) 21 Code of Federal Regulations (CFR) Part 11

For medical/pharmaceutical organizations, FDA regulations became effective in 1997 and enforced in 2000. CFR part 11 established the US Food and Drug Administration requirements for electronic records and signatures. It includes the following requirements [8]:

- Secure audit trails must be maintained on the system
- Only authorized persons can use the system and perform specific operations
- Records must be stored in a protected database
- Identity of each user must be verified before providing them any credential.

Part 11 is very high level and does not provide strict recommendations, however this regulation provides the basic principle for the use of computers in the pharmaceutical industry. To be compliant, an organization must define, implement and enforce procedures and controls to ensure the authenticity, integrity and the confidentiality of electronic records.

3.3 Gramm-Leach-Bliley Act (GLB)

In November 1999, the Gramm-Leach-Bliley Act was issued to regulate the privacy and protection of customer records maintained by financial organizations. GLB compliance for financial institutions became mandatory by July 2001, including the implementation of the following security requirements [9]:

- Access controls on customer information systems
- Encryption of electronic customer information
- Monitoring systems to perform attacks and intrusion detection into customer information systems
- Specify actions that have to be taken when unauthorized access has

---

[7] HIPAA:The critical role of strong authentication, http://www.rainbow.com/library/8/hipaa.pdf

[8] 21 CFR Part 11, http://wwwGULATORY/C.netegrity.com/PDFS/RE FR%20Part%2011%20Sheet.PDF

[9] Gramm-Leach-Bliley Security Requirements, http://www.itsecurity.com/papers/recourse1.htm

© SANS Institute 2000 - 2005 Author retains full rights.

occurred

To comply with GLB, institutions have to focus on administrative and technological safeguards to ensure the confidentiality and integrity of customer records, through the implementation of security solutions and secure systems management.

3.4 Sarbanes-Oxley Act (SOA)

The Sarbanes-Oxley Act issued in 2002 generates consistent changes in corporate governance, financial statement disclosure, accuracy of financial reporting, management compensation and auditor independence.
Section 404 of the SOA requires companies to put in place internal controls over business operations to ensure the integrity of financial audit records within the company with a real emphasis on computer and network security. This involves [10]:

- Internal Operational controls: control interactions between people and applications and audit rights and responsibilities.
- Employees and business partners controls: put in place authentication and control access to know who can access which systems and data and what can they do with those resources.
- Applications controls: apply operational controls directly to systems that will be connected to access each other data.
- Auditing and reporting : show compliance of all implementation of internal controls

Enforcing controls and making them operational are organizations main objectives to comply with SOA. Another focus point of this law is the improvement of security policies and procedures to address risks to the achievement of specific control objectives, which includes to [11]:

- Define security standards of protection
- Create security education programs for employees
- Identify and document security exposures and policy exceptions
- Evaluate periodically security compliance with metrics and put in place action plans to ensure compliance of policies.

Ensuring security and integrity of systems is a key focus of complying to SOA and organizations have to implement new security measures to improve

---

10 Achieving Sarbanes-Oxley Compliance with Oblix Management Solutions
http://www.oblix.com/resources/whitepapers/sol/wp_oblix_sarbox_compliance.pdf

11 Controlling your controls: Security Solutions for Sarbanes-Oxley
http://download.netiq.com/Library/White_Papers/NetIQ_SarbanesWP.pdf

© SANS Institute 2000 - 2005 Author retains full rights.

employee security skills, controls, technologies and security policies.

To conclude, each of these laws regulates the proper use of computers and data in specific industries, such as health, food and finance. They require organizations to provide control and visibility into the activities of employees, customers, partners, across multiple systems and domains, which could be done through the implementation of an Identity And Access Management solution.

4 Identity and Access Management concept

Identity and Access Management (I&AM) has emerged to help enterprises meet today's business challenges and being compliant with federal regulations, as described previously. I&AM merges business processes, security policies and technologies to help organizations manage digital identities (user attributes which describe who users are, how they prove their identity and the resources they can access) and control resource access [12]. I&AM covers the following services:

- Directory Services
- Identity Life Cycle Management Services :
  - Provisioning
  - Identity Management
  - Administration
- Access Management Services

Following diagram from Lewis presentation [13], illustrates the relationship between these components that will be described hereafter:

© SANS Institute 2000 - 2005, Author retains full rights.

[12] Microsoft Identity and Access Management Series – Fundamental concepts http://www.microsoft.com/technet/security/topics/identity/idmanage/P1Fund.mspx

[13] Lewis, Jamie. "The Emerging Infrastructure for Identity and Access Management" – Page 21 http://www.opengroup.org/security/lewis.pdf

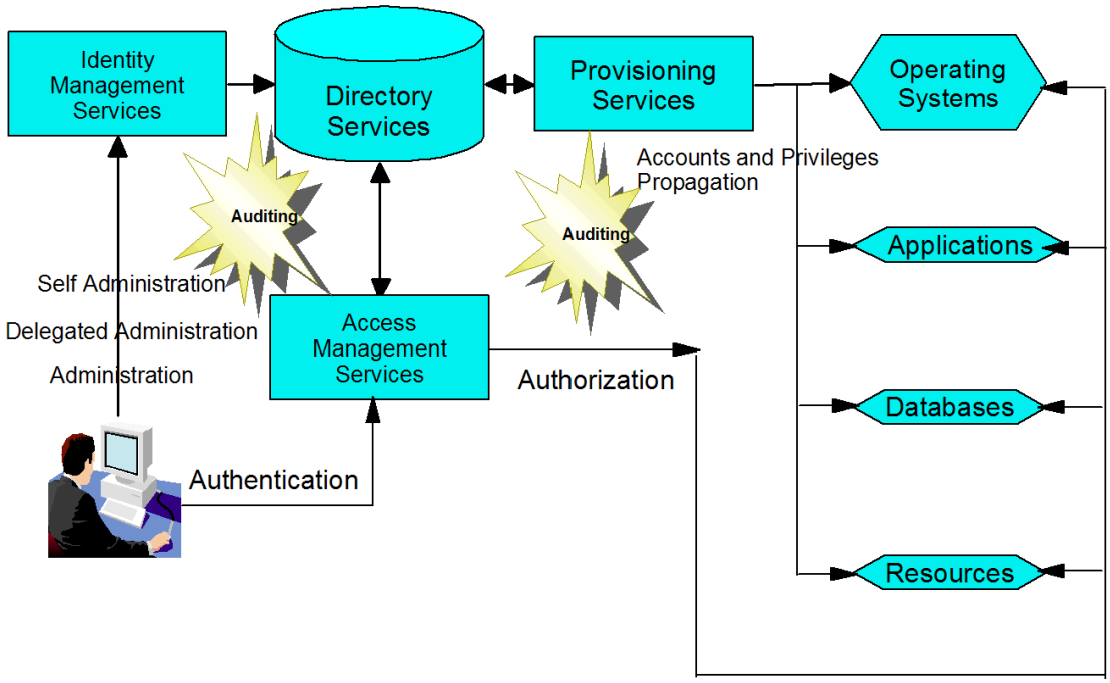


Figure 1: I&AM general description

4.1 Directory Services

Directory services are the core components of any I&AM solution, as they provide a central identity and resource repository that contains user profile information, as well as passwords, through different data supports: flat files, databases, directories. Most of the reliable directories are compliant with the Lightweight Directory Access Protocol (LDAP) which provides a standard extendable centralized storage and an efficient management of identity details. When in a heterogeneous and complex environment, where more than one directory is needed, an important point is to have only one entry for all existing directories to facilitate and centralize the management. This is the concept of Metadirectories which has been introduced to[14]

- create a global view of isolated identity information stored in multiple locations,
- synchronize the data values that each authoritative source provides throughout the organization,
- provide a focal access point to LDAP and non-LDAP directories.

[14] Microsoft Identity and Access Management - Solution Overview – Page 4
http://download.microsoft.com/download/f/2/5/f257d36e-ba68-416f-8ce9-66dafee69cf0/IdMwhitepaper.doc

© SANS Institute 2000 - 2005 Author retains full rights.

Metadirectories using LDAP standard interface, offer organizations the possibility to keep heterogeneous infrastructures, with a unified view of all identity and resource information. This is illustrated by the following figure:

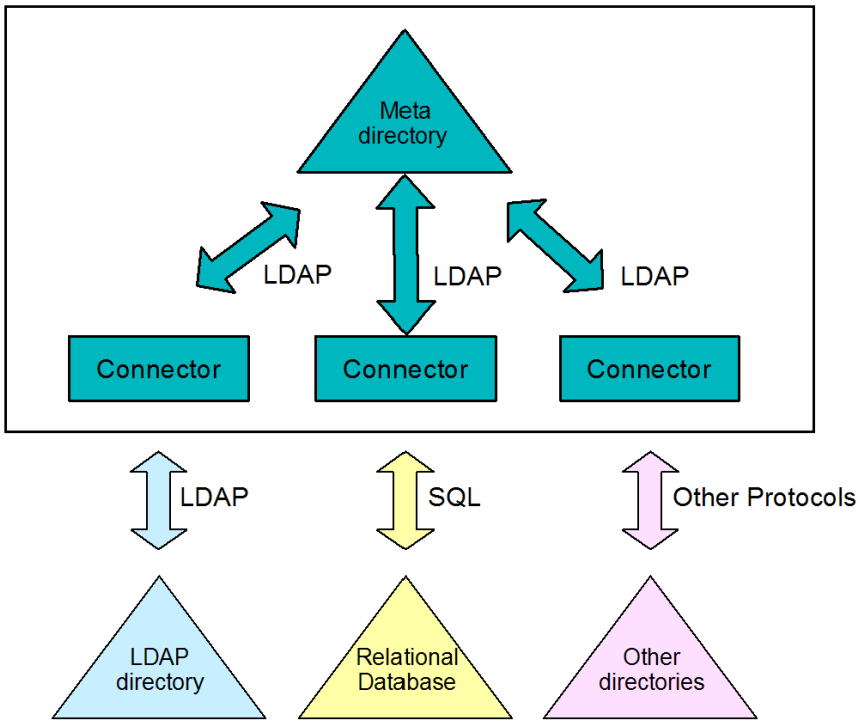


Figure 2: Metadirectory concept

In terms of directories services, the challenge of the I&AM solution is to unify security standards. The starting point is to discover all the managed identity stores, overall parts of the organization, to create a global view of identity information which will allow deciding on and implementing the best directory technology for the organization.

4.2 Identity Life Cycle Management Services

Life Cycle management is the process of modifying user attributes, entitlements (access rights and privileges) and their credentials, based on business policies, for all types of enterprise populations. This process is supported by management directories tools and includes [15]:

- Provisioning: digital identities administration and propagation of identities

[15] Microsoft Identity and Access Management Series - Fundamental Concepts – Chapter 3: Microsoft Identity and Access Management Technologies
http://www.microsoft.com/technet/security/topics/identity/idmanage/P1Fund_2.mspx

© SANS Institute 2000 - 2005 Author retains full rights.

modification towards each back-end application [16].

- Delegated administration: delegation of some selected account management functions to another trusted group (most of the time, for partner accounts).
- Self-service administration: administration of some users' attributes by the user himself
- Credential and password management: "keys" of authentication and authorization, which need to be carefully administrated with appropriate technologies and procedures [15].

4.2.1 Provisioning services

Provisioning allows centralizing and automating the process of managing user accounts and entitlements across multiple applications and directories. This is one of the most visible features of I&AM. The provisioning process must be related to organization's operational procedures, as account creation/modification need approval to be executed. The main steps of the provisioning process are the registration which includes the verification of identity, the fulfillment of which means getting the approval of resources owners through a workflow and the termination or account deletion [17].
Advantages of provisioning services are [18]:

- Opportunity to manage identities across disparate systems and applications based on directory infrastructure
- Possibility to get a single management access point for account maintenance and synchronization across multiple systems
- Automation of approval workflow (necessary to create/modify user accounts…) with a complete audit trail
- Password management

4.3 Access Management Services

Access management services consist in controlling, monitoring and auditing access to resources across internal or external networks. This process is based on security policies, using authentication, authorization and trust mechanisms.

4.3.1 Authentication

Authentication is the process used to verify the identity of a person or entity. There are many techniques to control user identities depending on the sensitivity

---

16 Enterprise Identity And Access Management technical White Paper – Page 2
http://radio.weblogs.com/0100367/stories/2002/05/11/enterpriseIdentityAndAccessManagement.html

17 What is User Life-Cycle Management ?, http://mtechit.com/customer/metagroup.pdf

18 Enterprise Identity And Access Management technical White Paper – Page 3
http://radio.weblogs.com/0100367/stories/2002/05/11/enterpriseIdentityAndAccessManagement.html

© SANS Institute 2000 - 2005 Author retains full rights.

of accessed resources. The technology chosen depends on the security policy requirements and it must integrate the following parameters: ease of use, ease of integration, ability to support multiple applications, manageability and cost considerations.

The following list shows example of different software and hardware authentication methods [19]:

- User name and password
- Personal identification numbers (PINs)
- X.509 digital certificates
- One-time passwords
- Biometrics (fingerprint, iris scans ….)
- Smart cards
- Electronic passport
- Hardware tokens

Note that all these techniques are not equally robust. The most robust (needed for hardened security) use cryptographic mechanisms to protect user credentials themselves and the authentication sessions when credentials are transferring across the network.

Single Sign On (SSO)

Particular attention must be given to Single Sign On which is promoted by the I&AM process. It enables when possible, authorized users to access multiple protected resources across domains, while authenticating only once [20]. SSO is based on the fact that the user only has to remember one password value. Once authenticated, SSO application provides the password credentials automatically and, generally, it is transparent to the user. Even if integration of SSO capability into the organization reduces helpdesk cost, it should be done step by step and has to meet all business requirements, for example working "outside" enterprise boundaries or being flexible enough to support enterprises evolution.

4.3.2 Authorization

Authorization is the process used to check a user has the proper permission to access various resources or can perform a specified action, based on user's identity. Authorization is performed after the user has been authenticated and is based on access control policies (rules to specify who may access, what resources), models (formalisms to describe policies) and mechanisms (translation of a user's access request into a table to grant or deny access) [21].

---

19 Microsoft Identity and Access Management Series - Fundamental Concepts – Chapter 3: Microsoft Identity and Access Management Technologies
http://www.microsoft.com/technet/security/topics/identity/idmanage/P1Fund_2.mspx

20 Track 1 - SANS Security Essentials. Defense-In-Depth - Page 162

© SANS Institute 2000 - 2005 Author retains full rights.

They are many access control models and mechanisms, of which the most well known are:

- Discretionary Access Control (DAC)
- Mandatory Access Control (MAC)
- Role Based Access Control (RBAC)

Note that the following can also find Rule Set Based Access Control, List Based Access Control or Token Based Access Control, listed in SANS documentation [22].

Discretionary Access Control (DAC)

DAC is based on the identity of users and/or membership in groups. The DAC concept is that every object has an owner who may grant rights to access an object to other users [23]. Drawbacks of this method are: that the administration of resource permissions can not be centralized as they are dependant on users, the DAC mechanisms are vulnerable to "Trojan horse" attacks. An example of implementation of the DAC model is Access Control Lists (ACL).

Mandatory Access Control (MAC)

MAC assigns a security level (classification) to all resources, a security clearance to each user and ensures that users can only see information below their clearance. MAC prevents "Trojan horse" attacks, but is very heavy to implement and often used for extremely secure systems, such as military environments.

Role Based Access Control (RBAC)

RBAC are based on individual's roles and responsibilities within the organization. In this case, permissions are associated with roles (usually closed to the security policy of the organization), users are members of specified roles and when a user starts a session, he can activate his roles. Access decision is granted depending on the activated roles. The advantage of RBAC is that there is a central control and maintenance of access rights ensuring flexibility (separation of duties…). One of the constraints is that RBAC is based on the assignment of users to roles and associated privileges. This point is an administrative challenge for implementation in large organizations, as it requires the identification of job functions, the specification of the set of privileges required to perform each function, and the restriction of the user to a domain with those privileges and nothing more

---

[21] Ferraiolo David F., Kuhn D. Richard, and Chandramouli Ramaswamy Role-Based Access Control - Page 28

[22] Track 1 - SANS Security Essentials. Defense-In-Depth - Page 144

[23] Ferraiolo David F., Kuhn D. Richard, and Chandramouli Ramaswamy Role-Based Access Control - Page 35

© SANS Institute 2000 - 2005 Author retains full rights.

[24].

4.3.3 Federation and Trust

The concept of trust is an important feature of access management, as it allows sharing resources in a structured way between different organizations (as business partners, for example). Trust is a complex mechanism, as it enables secure authentication and authorization of identities between independent systems [25], but it is often essential for gaining business opportunities.

4.4 Security Auditing

Auditing is part of every service of the I&AM solution, as this is a requirement of today's business word [26] (referred to SOA regulation). Auditing provides the necessary trail to explain who, what, when, where and how resources are accessed across the network. At least, the following events have to be registered for audit purposes:

- Authentication events
- Authorization events
- Directory objects modification

An efficient way to implement a security auditing policy is to centralize logs, to ensure the integrity of accurate audit logs and to allow the filtering of auditing reports. All these features are part of the I&AM solution.

5 Microsoft Identity and Access Management Series overview

After the overview of the I&AM concept, it is interesting to see how vendors have integrated this concept into products available on the market. In the last two years, many vendors, such as Microsoft with its product: "Identity and Access Management Series", Bull Evidian based on "AccessMaster" product, Computer Associates with "eTrust Identity and Access Management Suite", Netegrity with "SiteMinder" and IBM with "Tivoli" have developed integrated and standard-based solutions for access management, user administration and resource provisioning. Often, they are directly mapped on vendor products, even if, as previously explained, I&AM is not a system but a framework, merging policies, technologies and processes. To illustrate, this section will provide more details of the Microsoft solution: Microsoft Identity and Access Management Series. During the course of 2004, Microsoft has made a consequent effort to structure

---

[24] Ferraiolo David F., Kuhn D. Richard, and Chandramouli Ramaswamy Role-Based Access Control - Page 50

[25] Microsoft Identity and Access Management Series - Fundamental Concepts - Chapter 3: Microsoft Identity and Access Management Technologies
http://www.microsoft.com/technet/security/topics/identity/idmanage/P1Fund_2.mspx

[26] Track 1 - SANS Security Essentials. Secure Communications - Page 315 to 320

© SANS Institute 2000 - 2005 Author retains full rights.

and document its solution [27], focusing on security policies and processes required on top of the technology. The rest of this chapter will focus around the technology aspects of the Microsoft solution. Three main parts can be identified:

- The Foundation for Identity and Access Management
- Identity Life-Cycle Management
- Access Management and Single Sign On

Moreover, this is not a stand-alone solution, as Microsoft also presents complementary solutions of partners, such as Oblix "NetPoint", OpenNetwork "Universal IdP" and Netegrity "SiteMinder".
The following figure of Microsoft documentation [28] shows a global view of the main components making up the Microsoft solution:

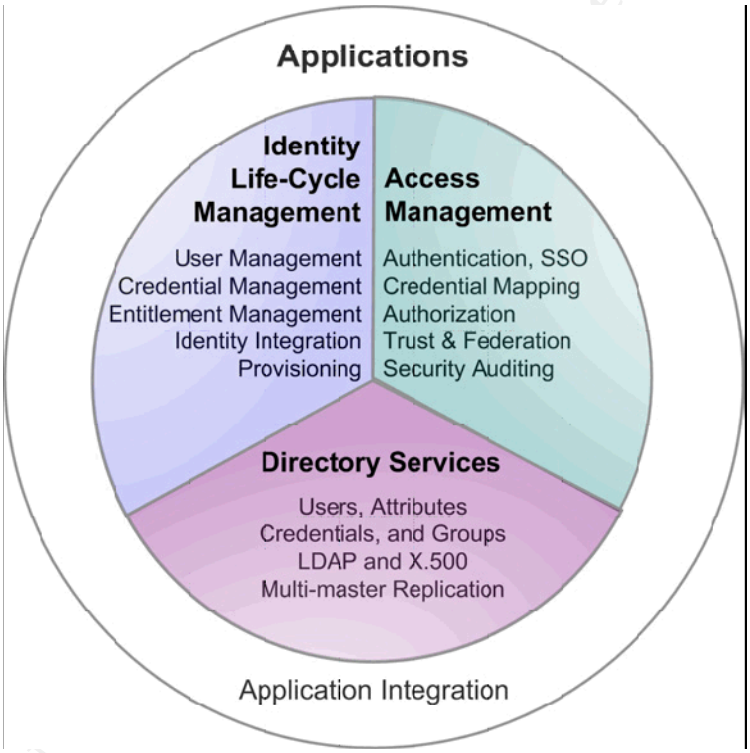


Figure 3: Processes and services in the Microsoft Identity and Access Management Framework

5.1 Directory Services

[27] Microsoft Identity and Access Management Series
http://go.microsoft.com/fwlink/?LinkId=14841

[28] Microsoft Identity and Access Management Series - Fundamental Concepts – Chapter 3: Microsoft Identity and Access Management Technologies – Figure 3.2
http://www.microsoft.com/technet/security/topics/identity/idmanage/P1Fund_2.mspx

© SANS Institute 2000 - 2005 Author retains full rights.

Microsoft's current directory services are based on the "Microsoft Active Directory" (integrated with Windows 2000 Server and Windows Server 2003). Active Directory is Microsoft recommended technology for storing identity information, complying with LDAP 3.0.
A new stand-alone directory product: Active Directory Application Mode (ADAM) provides facilities to applications:

- when strong authentication features are needed,
- when data to be stored requires frequent changes (which is not suitable with Active Directory, as it decreases performances),
- to migrate applications which support X.500 style naming (not supported by Active Directory) [29].

5.2 Identity Life-Cycle Management

To get a global view of users and implement identity provisioning and de-provisioning across different identity stores, Microsoft products are based on [30]:

- Microsoft Identity Integration Server 2003 (MIIS 2003), which adds services to Active directory, especially interoperability capabilities and synchronization of identity changes (automatically detected) across multiple systems. It also provides password management functions through the password propagation between all connected directories.
- Identity Integration Feature Pack for Microsoft Windows Server Active Directory, to integrate identity information between Active Directory, ADAM and Exchange 2000/2003 address lists.
- For non-Microsoft operating systems (UNIX, NetWare…), a set of products are provided to enable the integration with Windows environment.

5.3 Access Management

5.3.1 Authentication

Several authentication methods and security protocols are imbedded in Windows server 2003 and Windows XP. The goal is to build applications using these authentication mechanisms. Those mechanisms based on Microsoft .NET Passport and public key authentication do not have the same robustness and could be mixed depending on application requirements [31].
The following figure extracted from Microsoft documentation [31] shows the different layers of authentication protocols:

---

[29] Microsoft Identity and Access Management Series - Fundamental Concepts – Chapter 4: Directory Services
http://www.microsoft.com/technet/security/topics/identity/idmanage/P1Fund_3.mspx
[30] Microsoft Identity and Access Management Series - Fundamental Concepts – Chapter 5: Identity Life-Cycle Management
http://www.microsoft.com/technet/security/topics/identity/idmanage/P1Fund_4.mspx
[31] Microsoft Identity and Access Management Series - Fundamental Concepts – Chapter 6: Access Management
http://www.microsoft.com/technet/security/topics/identity/idmanage/P1Fund_5.mspx

© SANS Institute 2000 - 2005 Author retains full rights.

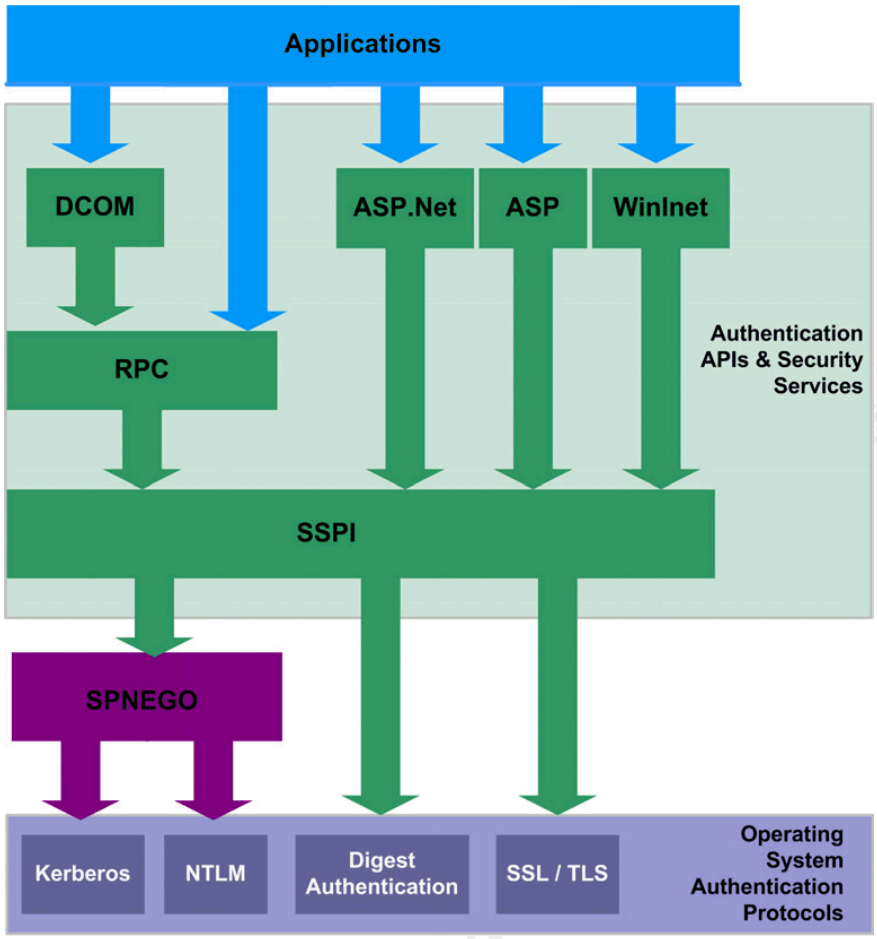


Figure 4: The authentication API and protocol hierarchy in the Windows operating system

High-level APIs and services provide inter-process communication (IPC) secure mechanisms for transmitted application data. They are based on [32]:

- Distributed Component Object Model (DCOM) which allows using Kerberos version 5 protocol (the basis of authentication to Active Directory),
- NT LAN Manager (NTLM) challenge/response, remote procedure calls (RPC) which enables data exchange,
- Microsoft ASP.NET, ASP,
- WinInet (an application protocol interface which supports Secure Sockets Layer (SSL))…

The lowest level application interface for authentication is the Security Support Provider Interface (SSPI). This is a generic interface to all authentication protocols imbedded into Windows operating systems, which can be used by

[32] Microsoft Identity and Access Management Series - Fundamental Concepts – Chapter 6: Access Management http://www.microsoft.com/technet/security/topics/identity/idmanage/P1Fund_5.mspx

© SANS Institute 2000 - 2005 Author retains full rights.

applications for authentication purpose and to secure their data [32].
Secure Protocol Negotiation (SPNEGO) is a security package which can be used to interface with Kerberos or NTLM avoiding using these protocols directly.
Digest authentication is another standards-based authentication protocol which provides interoperability between Windows and non-Windows platforms for Internet authentication [32].

Microsoft Single Sign On feature:
Another feature of authentication is the Microsoft Passport, a Web service which allows extranet users authentication and enables WEB Single Sign On (SSO) capabilities on many WEB sites [32]. Microsoft Passport allows large user accounts to be managed outside the organization through a secure WEB site with its own life-cycle management and with self administration capability.
In addition to WEB SSO (through the support of Passport), Microsoft proposes the Desktop integrated SSO (on Windows platforms, which offers the possibility to use a single user identity maintained in Active Directory, across an organization's intranet or Windows domains) and the Enterprise SSO (different techniques that uses a form of credential mapping through a specific database to simulate a SSO function) [32].

5.3.2 Authorization

Windows Server 2003 supports several authorization mechanisms [32]:

- Windows Access Control List (ACL) - DAC model - defines what access level the users or groups have to an object
- The roles-based Authorization Manager - RBAC model – the authorization Manager Interface assigns the roles defined in the Authorization Policy Store to users within the application, for a given task.
- ASP.NET Authorization - RBAC model – applicable to standalone applications, uses Active Directory groups as well as application roles.

5.3.3 Trust

A "trust relationship" is the link established between two identity stores or directories (in case of partner relationship for example) that enables users who can authenticate to one identity store to authenticate to a second one without having a digital identity in the second identity store [33]. In Active Directory environments, trusts can be established between domains. In Windows server 2003 you can find the "forest trusts" notion. A forest is a set of domains hierarchically organized. A forest trust is a single trust link between the root domains of two forests. It enables a transitive trust between all of the domains contained in the two forests. This is illustrated by the following figure extracted from Microsoft documentation [33]:

---

[33] Microsoft Identity and Access Management Series - Fundamental Concepts – Chapter 6: Access Management
http://www.microsoft.com/technet/security/topics/identity/idmanage/P1Fund_5.mspx

© SANS Institute 2000 - 2005 Author retains full rights.

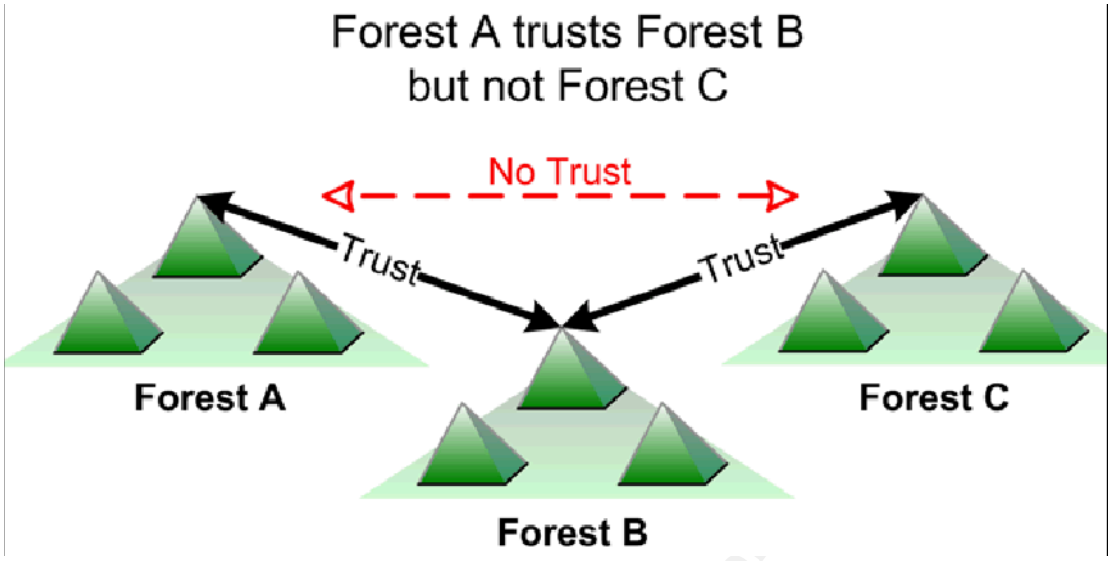


Figure 5: Windows 2003 forest trust relationships

5.4 Security Auditing

Microsoft security auditing and reporting are provided by the Windows Security Event Log which collects all generated authentication, authorization and trust auditing events [34]. Windows Management Interface (WMI) and Microsoft Operations Manager (MOM) are technologies and products that enable the manageability of the Windows server system infrastructure.

2 I&AM deployment challenges

Despite the I&AM solution being detailed by different vendors and associated with well-known products, I&AM implementation is a huge and complex project, specific to each organization. It requires clear goals, detailed planning, a good understanding of organization's requirements and efficient project management based on a phased approach. It is often difficult for organizations to integrate the whole Identity And Access Management components without changing the way they do business. Moreover, to avoid confusion, I&AM issues should not be solved at the same time. To illustrate this, below are listed some challenges that organizations may meet when deploying the I&AM solution:

2.1 Scope, Schedule and Cost

[34] Microsoft Identity and Access Management Series - Fundamental Concepts – Chapter 6: Access Management
http://www.microsoft.com/technet/security/topics/identity/idmanage/P1Fund_5.mspx

© SANS Institute 2000 - 2005 Author retains full rights.

Companies today are interested in increasing their technology while reducing risks and costs. In most cases I&AM is an expensive project raising the question whether benefits will exceed costs. To ensure that I&AM implementation will finally offer a payback and a significant return of investment, a strong focus must be placed on developing a positive business case. It will help to define the right balance between the scope, schedule and cost of the I&AM solution.

2.2 Assessing the current environment and I&AM

Assessing the current environment is the preliminary step to the I&AM solution implementation. It includes [35]: documenting the current infrastructure (software and hardware), establishing or gathering all security processes, determining the business relationships across organization boundaries and collecting all current security policies. This phase is essential to determine the real business needs of the organization and to better understand I&AM project goals and constraints. The next step is to establish the functional requirements of I&AM, as aggregating the existing identities information into a metadirectory, or if this is not possible, decreasing the number of identities stores by sharing identity information across different entities and at least including the applications in the whole architecture. These assessments are a huge effort and a challenge for large organizations involving many stakeholders, but they are mandatory to implement a successful I&AM solution.

2.3 Interoperability

A successful I&AM solution depends on interoperability among different systems and applications, including the sharing of authentication and authorization information, as well as maintaining the consistency of identity information.
Interoperability and portability are strengthened by standards. Standards related to authentication and authorization processes emerged in recent years. They are often dependant on a directory services infrastructure and combined together they provide methods to support the I&AM solution. The most well known standards are:

- eXtensible Markup Language (XML) – provide an implemented and standard way to describe any type of data and to share them.
- Security Assertions Markup Language (SAML) – allow exchange of identities (used for authentication and authorization processes).
- XML Key Management Services (XKMS) – allow Public Key Infrastructure (PKI) enabling applications.
- X.500 – a series of standards that describe the functionality and interoperability of autonomous centralized identities data stores.

[35] The National Electronic Commerce Coordinating Council, « Enterprise Identity and Access Management: The Rights and Wrongs of Process, Privacy and Technology"- Page 6
http://www.ec3.org/Downloads/2003/EnterpriseIdentity.pdf

© SANS Institute 2000 - 2005 Author retains full rights.

Being compliant with the standards is a condition for the I&AM solution to be integrated in current products and to be flexible enough to support organization evolution. They are complex to understand and deciding which will fit the need of the organization is very challenging.

2.4 And also Scalability, Manageability…

The I&AM solution has to securely support, more and more users (partners, employees, customers) and many types of sensitive applications in changing technical environments. Therefore scalability, manageability and flexibility are crucial points when implementing such a solution. These features are often integrated in vendor solutions, but have to be carefully studied before choosing the appropriate product(s).

3 Conclusion

The concept of Identity and Access Management enables private or public organizations to securely manage identities and access in and out of enterprise boundaries while meeting the requirements of today's business world. The implementation of a solution which can require multiple products from multiple vendors is a real investment: money, time, as well as resources. It also results in business process change for organizations which need to define the right phases of I&AM deployment and the key concerns that must be resolved through efficient project management. However, the return of investment is achieved through multiple factors: simplified centralized administration with a complete provisioning system, an access enforcement system including extranet management and single sign-on, faster application development and deployment, less Help Desk involvement and a strong auditing capability.

There is a lot of uncertainty about the future demand of I&AM and to what extent organizations will be willing to move into this IT area. Even with this degree of uncertainty, major IT worldwide protagonists such as Microsoft, IBM, Computer Associates (CA) are increasing their efforts to provide an integrated Identity and Access Management solution to fit within their platform offerings. This clearly dictates the need for strong commitment to address this emerging market, encouraging organizations to define a global security infrastructure including federated identity and improvement of access management. Findings of this paper clearly suggest the I&AM solution will be in the center of this strategy.

© SANS Institute 2000 - 2005, Author retains full rights.

4 References

Cheney Anne." eTrust Identity and Access Management Suite." Computer Associates. Feb. 2004. 20 Nov. 2004.
URL:http://www3.ca.com/Files/WhitePapers/etrust_identity_access_mgmt_suite_wp.pdf

Chong Frederick. Microsoft Corporation. "Identity and Access Management." Jul. 2004. 6 Dec. 2004.
URL: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnmaj/html/aj3identity.asp

Computer Associates. " eTrust Identity and Access Management Suite." 2003. 20 Dec. 2004.
URL: http://2004.rsaconference.com/downloads/CAbroch.PDF

Davis Jeff. Satestone."Secure Identity and Access Management." Safestone. 2004. 15 Dec. 2004.
URL:http://www.safestone.com/downloads/whitepapers/managing_user_access.pdf

Evidian."HIPAA Compliance and Identity & Access Management." Sept. 2004. 10 Nov. 2004.
URL: http://www.evidian.com/newsonline/art040901.php

Ferraiolo David F., Kuhn D. Richard, and Chandramouli Ramaswamy. Role-Based-Access Control. Norwood: Artech House. 2003.

Harvey Rick, Kelley Diana."eTrust Directories Foundations for Online Services." Computer Associates. Apr. 2004. 20 Nov. 2004.
URL:http://www3.ca.com/Files/WhitePapers/etrust_directory_foundation_white_paper.pdf

Kahn, Jam."HIPAA: The critical role of strong authentication." Safenet. Apr. 2002. 10 Nov. 2004.
URL: http://www.rainbow.com/library/8/hipaa.pdf

Kolodgy, Charles J. "Identity Management in a Virtual World." Jun. 2003. 22 Nov. 2004.
URL:ftp://ftp.ealaddin.com/pub/Marketing/eToken/White_Papers/WP_IDC/IDC%20Whitepaper_ID%20Mgmt%20in%20Virtual%20World_June%202003.pdf

© SANS Institute 2000 - 2005 Author retains full rights.

Langin, Daniel J. “Gramm-Leach-Bliley Security Requirements: Keeping Robbers and Regulators from the Door.” Jun. 2002. 12 Nov. 2004.
URL: http://www.itsecurity.com/papers/recourse1.htm

Lewis Jamie. “The Emerging Infrastructure for Identity and Access Management”. Open Group In3 Conference. Jan. 2002. 15 Oct. 2004.
URL: http://www.opengroup.org/security/lewis.pdf

Meta Group. “What is User Life-Cycle Management ?.”800-945-META [6382]. Jun. 2004. 6 Dec. 2004.
URL: http://mtechit.com/customer/metagroup.pdf

Microsoft Corporation.”Microsoft Identity and Access Management Series.” Jul. 2004. 18 Oct. 2004.
URL: http://go.microsoft.com/fwlink/?LinkId=14841

Microsoft Corporation.”Microsoft Identity and Access Management Series – Fundamental concepts.” Jul. 2004. 18 Oct. 2004.
URL:http://www.microsoft.com/technet/security/topics/identity/idmanage/P1Fund.mspx

Microsoft Corporation. “Identity and Access Management – Solution Overview.” Jul. 2003. 20 Oct. 2004.
URL: http://download.microsoft.com/download/f/2/5/f257d36e-ba68-416f-8ce9-66dafee69cf0/IdMwhitepaper.doc

Netegrity. “Identity and Access Management: The Promise and the Payoff – How An Identity and Access Management Solution Can Generate Triple-digit ROI.” Jun. 2003. 20 Nov. 2004.
URL: http://wp.bitpipe.com/resource/org_976643855_646/IAMROI.pdf

Netegrity.’”21 CFR Part 11 (FDA regulation on Electronic records & Signatures).” 2004. 10 Nov. 2004.
URL:http://www.netegrity.com/PDFS/REGULATORY/CFR%20Part%2011%20Sheet.PDF

Netegrity. “Gramm-Leach-Bliley”. . 15 Nov. 2004.
URL:http://www.netegrity.com/PDFS/REGULATORY/GLBA%20Handbook%20Sheet.PDF

Netegrity. “Sarbanes-Oxley”. . 15 Nov. 2004.
URL:http://www.netegrity.com/PDFS/REGULATORY/SOA%20Handbook%20Sheet.PDF

NetiQ. “Controlling your controls: Security Solutions for Sarbanes-Oxley.” Jun. 2004. 15 Nov. 2004.

© SANS Institute 2000 - 2005 Author retains full rights.

URL:http://download.netiq.com/Library/White_Papers/NetIQ_SarbanesWP.pdf

Oblix."Strong Authentication Methods and Identity Management".October 2004. 22 Nov. 2004.
URL:http://www.oblix.com/resources/whitepapers/sol/wp_oblix_strong_authn_idm.pdf

Oblix. "Achieving Sarbanes-Oxley Compliance with Oblix Management Solutions." Sept. 2004. 15 Nov. 2004.
URL:http://www.oblix.com/resources/whitepapers/sol/wp_oblix_sarbox_compliance.pdf

SANS Institute. Track 1 - SANS Security Essentials Version 2.2. Defense-In-Depth, Volume 1.2. SANS Press, Jan. 2004.

SANS Institute. Track 1 - SANS Security Essentials Version 2.2. Secure Communications, Volume 1.4. SANS Press, Jan. 2004.

United States. The National Electronic Commerce Coordinating Council. "Enterprise Identity and Access Management: The Rights and Wrongs of Process, Privacy and Technology." Nov. 2003. 5 Dec. 2004.
URL: http://www.ec3.org/Downloads/2003/EnterpriseIdentity.pdf

© SANS Institute 2000 - 2005 Author retains full rights.