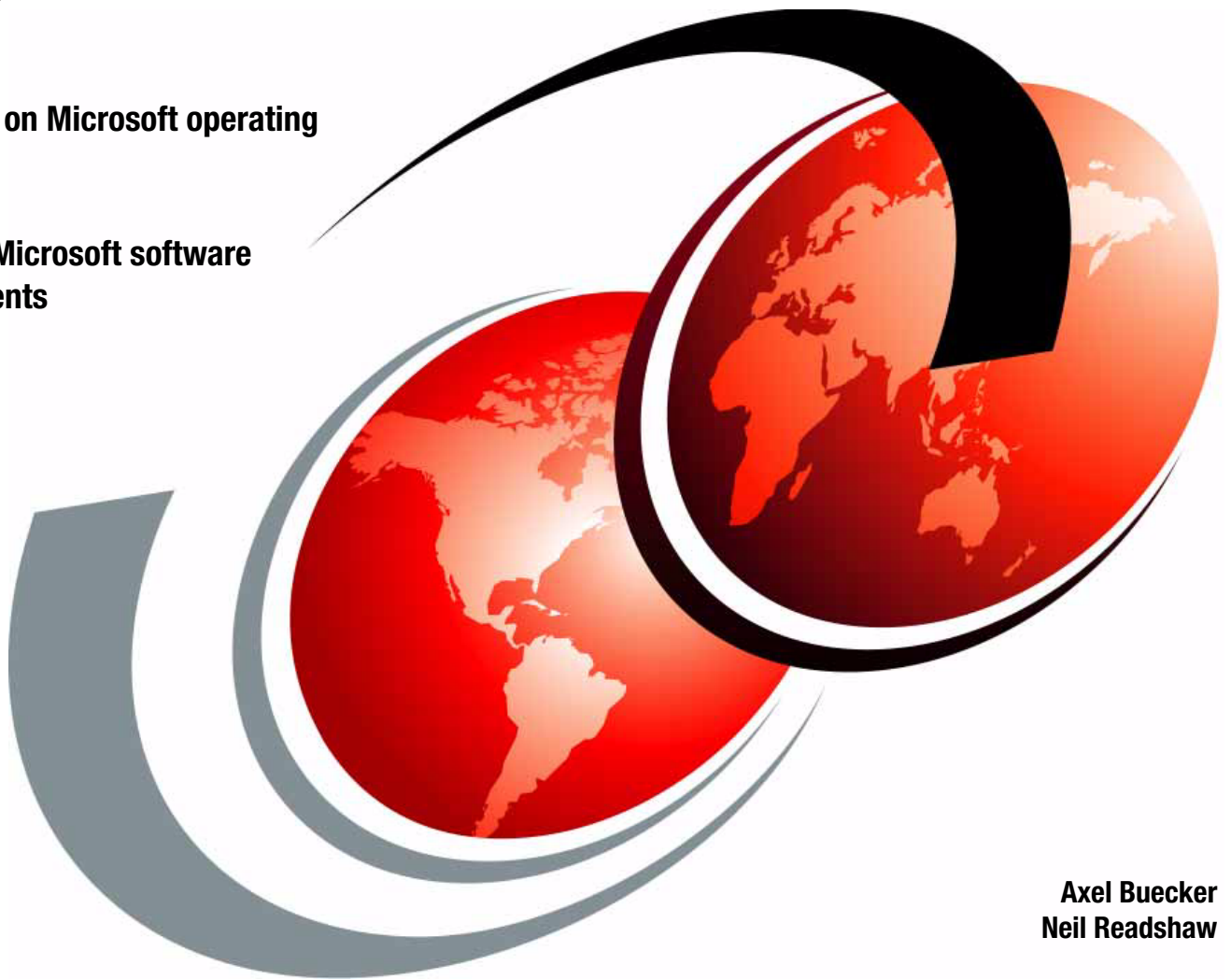


IBM Tivoli Security Solutions for Microsoft Software Environments

Explaining common architecture and standards

Deploying on Microsoft operating systems

Securing Microsoft software environments



Axel Buecker
Neil Readshaw



International Technical Support Organization

**IBM Tivoli Security Solutions for Microsoft Software
Environments**

September 2008

Note: Before using this information and the product it supports, read the information in “Notices” on page v.

First Edition (September 2008)

This document created or updated on September 18, 2008.

© Copyright International Business Machines Corporation 2008. All rights reserved.

Note to U.S. Government Users Restricted Rights -- Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Notices	v
Trademarks	vi
Preface	vii
The team that wrote this paper	vii
Become a published author	viii
Comments welcome	viii
Chapter 1. Architecture and standards	1
1.1 IBM Security Framework	2
1.2 IBM Service Management strategy	3
1.2.1 Visibility	3
1.2.2 Controls	3
1.2.3 Automation	3
1.3 Security standards	4
1.3.1 LDAP	4
1.3.2 Kerberos	4
1.3.3 SPNEGO	4
1.3.4 SSL and TLS	5
1.3.5 Service-oriented architecture and Web Services Security	5
1.4 Conclusion	9
Chapter 2. IBM Tivoli Security Solutions using Microsoft operating systems and middleware	11
2.1 Microsoft products that we discuss in this chapter	12
2.1.1 Operating systems	12
2.1.2 Middleware	12
2.2 Support summary by IBM Tivoli Security product	13
2.2.1 IBM Tivoli Directory Server	13
2.2.2 IBM Tivoli Directory Integrator	14
2.2.3 IBM Tivoli Access Manager Family	14
2.2.4 IBM Tivoli Identity Manager	15
2.2.5 IBM Tivoli Federated Identity Manager	15
2.2.6 IBM Tivoli Security Information and Event Manager	16
2.2.7 IBM Tivoli Security Compliance Manager	16
2.2.8 IBM Tivoli zSecure Suite	17
2.3 Conclusion	17
Chapter 3. Integration with Microsoft software environments	19
3.1 Security compliance	20
3.2 Identity and access	20
3.2.1 Identity data synchronization	20
3.2.2 Password synchronization	21
3.2.3 User life cycle management	22
3.2.4 Desktop single sign-on	24
3.2.5 Web single sign-on	24
3.2.6 Federated single sign-on	27
3.2.7 Identity propagation in service-oriented architecture	28
3.2.8 Role-based access control	29

3.3 Information security	30
3.4 Application security	30
3.5 Infrastructure security	30
3.6 Conclusion	32

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.


COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. These and other IBM trademarked terms are marked on their first occurrence in this information with the appropriate symbol (® or ™), indicating US registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at <http://www.ibm.com/legal/copytrade.shtml>

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

Alerts®	Everyplace®	Redbooks (logo)  ®
CICS®	IBM®	Tivoli®
DB2®	Rational®	WebSphere®
developerWorks®	Redbooks®	z/OS®

The following terms are trademarks of other companies:

SAP, and SAP logos are trademarks or registered trademarks of SAP AG in Germany and in several other countries.

Java, JDBC, and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Active Directory, Internet Explorer, Microsoft, SharePoint, SQL Server, Windows CardSpace, Windows Server, Windows Vista, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

Preface

You can use IBM® Tivoli® Security products to build open, flexible, and scalable solutions to address business requirements in the areas of:

- ▶ Identity and access management
- ▶ Security information and event management

One of the many strengths of the IBM Tivoli Security offerings is that they are designed and implemented as *cross-platform* solutions. This design enables broad adoption of the solutions across the range of disparate platforms typically found in an enterprise. IBM Tivoli Security solutions are, therefore, an excellent choice as organizations move further towards service-oriented architecture (SOA) and the security integration challenges present in SOA.

In many enterprises, software solutions from Microsoft® are important components of the IT strategy. In this IBM Redpaper publication, we consider the use of IBM Tivoli Security solutions in Microsoft environments from a number of perspectives. In this paper, we discuss:

- ▶ Architectures and standards that are common to IBM Tivoli Security and Microsoft software.
- ▶ IBM Tivoli Security solutions running on Microsoft operating systems utilizing Microsoft middleware.
- ▶ How to secure a Microsoft software environment with IBM Tivoli Security solutions.
- ▶ IBM Tivoli Security solutions providing improved security and security management for Microsoft operating systems, middleware, and applications through integration.

Who should read this paper

IT architects responsible for enterprise security architecture can learn about the architecture and standards that the IBM Tivoli Security and Microsoft software portfolios share. We discuss the scope of capability that IBM Tivoli Security solutions provide for heterogeneous and especially Microsoft software environments.

IT specialists who design and implement IBM Tivoli Security solutions can gain an introductory understanding of how to deploy the solutions on Microsoft operating systems and of the solution's capabilities when securing Microsoft software environments.

The team that wrote this paper

This paper was produced by a team of specialists from around the world working at the International Technical Support Organization (ITSO), Austin Center.



Axel Buecker is a Certified Consulting Software IT Specialist at the ITSO, Austin Center. He writes extensively and teaches IBM classes worldwide on areas of Software Security Architecture and Network Computing Technologies. He holds a degree in computer science from the University of Bremen, Germany. He has 22 years of experience in a variety of areas related to Workstation and Systems Management, Network Computing, and e-business Solutions. Before joining the ITSO in March 2000, Axel worked for IBM in Germany as a Senior IT Specialist in Software Security Architecture.



Neil Readshaw is a Senior Certified Consulting IT Specialist in the IBM Australia Development Laboratory. He has 17 years IT experience, including 11 years of experience in the information security field. He holds degrees in computer engineering and computer science from the University of Queensland. His areas of expertise include SOA security and user-centric identity management. He was a co-author on both editions of the *Understanding SOA Security Design and Implementation*, SG24-7310, and the *Federated Identity and Trust Management*, REDP-3678, and *Propagating Identity in SOA with Tivoli Federated Identity Manager*, REDP-4354. He has also written extensively for IBM developerWorks®.

Thanks also to the following people for their contributions to this project:

Alexander Amies, Mike Campbell, Christopher Choi, Scott Exton, Joseph Hamblin, Eddie Hartman, Scott Henley, Philip Nye, Charlie Saylor, Jason Todoroff, Patrick Wardrop
IBM

Become a published author

Join us for a two- to six-week residency program! Help write a book dealing with specific products or solutions, while getting hands-on experience with leading-edge technologies. You will have the opportunity to team with IBM technical professionals, Business Partners, and Clients.

Your efforts will help increase product acceptance and customer satisfaction. As a bonus, you will develop a network of contacts in IBM development labs, and increase your productivity and marketability.

Find out more about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

We want our papers to be as helpful as possible. Send us your comments about this paper or other IBM Redbooks® in one of the following ways:

- ▶ Use the online **Contact us** review Redbooks form found at:

ibm.com/redbooks

- ▶ Send your comments in an e-mail to:

redbooks@us.ibm.com

- ▶ Mail your comments to:

IBM Corporation, International Technical Support Organization
Dept. HYTD Mail Station P099
2455 South Road
Poughkeepsie, NY 12601-5400



Architecture and standards

The strategy and architecture of IBM Tivoli Security solutions is linked closely to two broader IBM initiatives:

- ▶ IBM Security Framework
- ▶ IBM Service Management strategy

Another important aspect of the IBM Tivoli Security strategy is to base its solutions on open industry standards. This strategy maximizes interoperability in the heterogeneous IT environments that is found in most organizations. Many of the standard efforts led by IBM and implemented in IBM Tivoli Security solutions are also implemented in Microsoft products. We describe these shared standards in this chapter.

1.1 IBM Security Framework

The great value of enterprise security management is realized when a *business focused, risk management* approach is taken. Security solutions that are built using a *collection of technology centric point products* cannot deliver the enterprise security benefits needed in the modern enterprise.

IBM has a broad set of security offerings that can enable an organization to secure its business processes and IT assets. Security offerings from IBM include:

- ▶ Software
- ▶ Hardware
- ▶ Consulting services
- ▶ Managed services

IBM has developed a security model—the IBM Security Framework—that takes advantage of the breadth of the IBM portfolio to mitigate security risks throughout all IT domains that can impact business processes. The IBM Security Framework is defined for the business executive first and foremost and is a model around which business and IT can converge upon a shared understanding of how to address business and IT security.

As shown in Figure 1-1, the enterprise security challenge is decomposed into five security domains within the IBM Security Framework. These security domains are aligned closely with other security models, such as the Control Objectives for Information and related Technology (COBIT) that is defined by the Information Systems Audit and Control Association (ISACA).¹

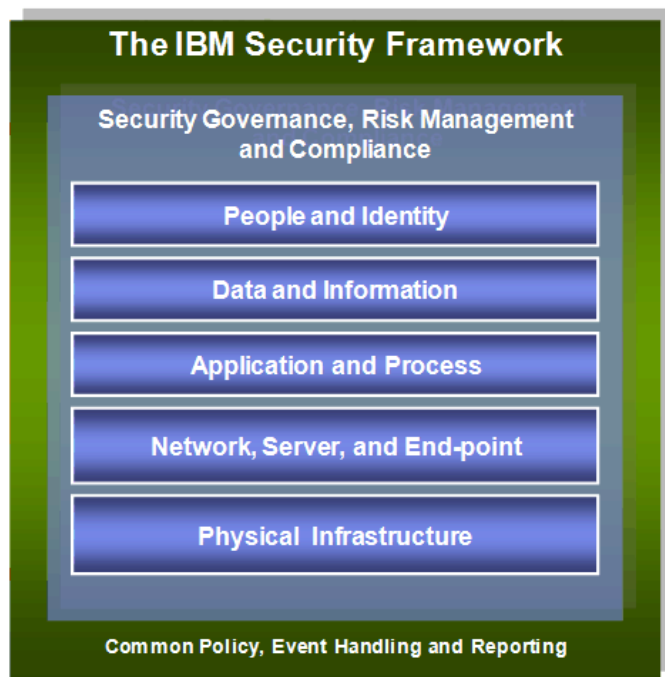


Figure 1-1 The IBM Security Framework

These domains define the holistic approach from IBM to enterprise security. Most security vendors focus only on one domain and can, therefore, manage only a portion of the total risk.

¹ You can find more information about COBIT and the ISACA at:
<http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981>

IBM brings strong focus and significant investment to provide the right technologies and expertise to provide leading edge security, from IT security asset life cycle management to operational control over security transactions, across every domain. With this, IBM can provide unparalleled capability to secure complete business processes.

1.2 IBM Service Management strategy

IT departments are challenged to deliver growth and business value to the organization. The cost of compliance and operations management of the existing IT infrastructure often constrains the ability to deliver sufficient growth.

The IBM Service Management strategy (Figure 1-2) provides three fundamental aspects of service management that can shift IT spending towards growth initiatives. The IBM Service Management strategy aligns the relevant IBM products and services.

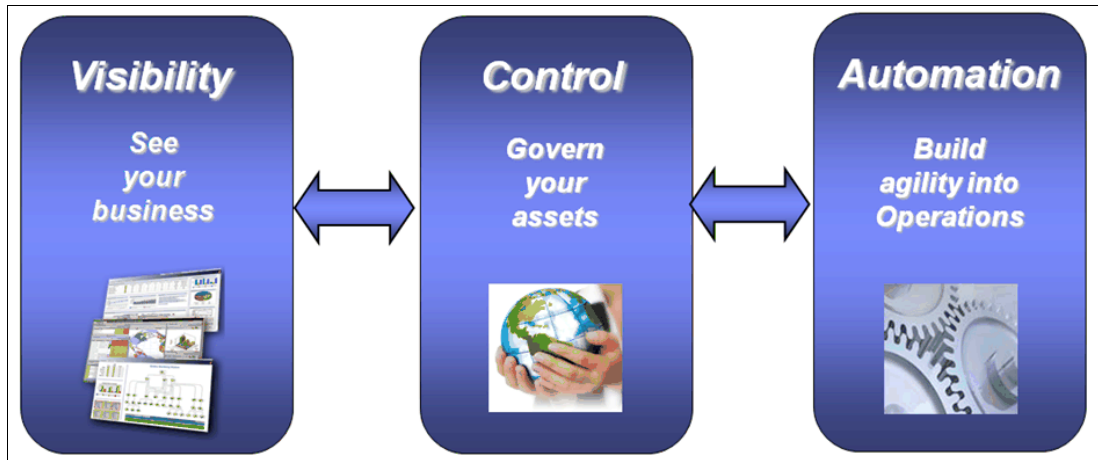


Figure 1-2 IBM Service Management strategy

1.2.1 Visibility

Service management starts with gaining *visibility* of the IT environment and how the services it provides are performing against business and operational objectives. This visibility enables prioritized response to events in the IT environment based on their business impact. For example, reports demonstrating compliance with regulatory requirements provide a business level perspective of the state of the IT environment.

1.2.2 Controls

When visibility of the IT environment is available, it is possible to determine which *controls* are required (and where) to support the goals of the business. These controls include governance over the changes in an IT environment. For example, authentication and access control in a Web-based environment ensures that users are identified and granted access only to the resources for which they are entitled.

1.2.3 Automation

When an organization gains visibility and control of their IT infrastructure, adding *automation* is a logical extension for improving operational efficiency. For example, automated

provisioning of user identities and their entitlements can reduce the time for a new employee to be productive from many days to considerably less than a day.

1.3 Security standards

In this section, we introduce selected industry standards in the security field. These standards are supported by the IBM Tivoli Security solutions as well as Microsoft software products.

1.3.1 LDAP

The *Lightweight Directory Access Protocol* (LDAP) is a set of simple protocols for accessing and modifying information in directories. LDAP is a pervasive protocol that operates on top of TCP/IP.

Note: LDAP is not a directory standard, but a directory access standard that you can use to access a variety of directories. Access control within the directory is not comprehensively covered by the LDAP standard.

Tivoli Directory Server, Microsoft Active Directory®, and Microsoft Active Directory Application Mode (ADAM) all support access using the LDAP protocol.

Note: The LDAP protocol specifications are available at:

<http://tools.ietf.org/html/rfc4510>

You can also obtain more information about LDAP by reading *Understanding LDAP - Design and Implementation*, SG24-4986.

1.3.2 Kerberos

Kerberos is a network authentication service based on symmetric key cryptography. It is suitable for authentication of clients and services in environments where the network itself can be untrusted. The Kerberos protocol relies on a trusted third-party component that contains Key Distribution Center and Authentication Service components.

Kerberos is used as the authentication protocol for Microsoft Active Directory. You can also use Kerberos security tokens in Microsoft and IBM implementations of Web services security.

Note: Version 5 of the Kerberos protocol is described in RFC 1510, which is available at:

<http://tools.ietf.org/html/rfc1510>

1.3.3 SPNEGO

The *Simple and Protected GSS-API Negotiation* mechanism (SPNEGO) is an authentication protocol that is used to authenticate a client to a server when the set of compatible authentication protocols is unknown. SPNEGO is based on the *Generic Security Services Application Programming Interface* (GSS-API).

SPNEGO is one of the authentication mechanisms that is supported by the Microsoft Internet Explorer® Web browser and Microsoft Internet Information Services (IIS) Web server. This

authentication mechanism is often referred to as *Integrated Windows® Authentication (IWA)*. Kerberos is one of the authentication mechanisms that can be used within SPNEGO. IBM Tivoli Access Manager for e-business supports SPNEGO authentication in its Web security components so that single sign-on can be achieved from a user's Windows desktop to Web applications that are protected by either the Tivoli Access Manager for e-business WebSEAL or the Plug-in for Web Servers component.

Note: For more information about Integrated Windows Authentication and the standards from which it is derived, see:

- ▶ <http://www.ietf.org/rfc/rfc2743.txt> (GSS-API)
- ▶ <http://tools.ietf.org/html/rfc4178> (SPNEGO)
- ▶ <http://tools.ietf.org/html/rfc4559> (SPNEGO over HTTP)

1.3.4 SSL and TLS

Secure Sockets Layer (SSL) is a ubiquitous protocol for transmitting data with confidentiality and integrity over a network. SSL makes use of encryption to protect data. *Transport Layer Security (TLS)* evolved from SSL and is intended to replace it.

Among many other examples, SSL and TLS are optional transports for communications for HTTP components such as Microsoft Internet Information Services and Tivoli Access Manager WebSEAL and for directory components such as Microsoft Active Directory and Tivoli Directory Server. They are also used internally in Tivoli Access Manager for communication between different Tivoli Access Manager services.

Note: You can find the TLS 1.1 specification at:

<http://tools.ietf.org/html/rfc4346>

1.3.5 Service-oriented architecture and Web Services Security

This section discusses the common standards in the service-oriented architecture (SOA) and Web Services (WS) Security realms.

WS-I Basic Security Profile

The *Basic Security Profile* is a specification that was developed by the Web Services Interoperability Organization (WS-I). The profile provides guidance for use of WS-Security specifications (see “WS-Security” on page 5) to maximize interoperability. IBM and Microsoft are both founding members of the WS-I and have used WS-I to lead standardization efforts for interoperable Web services.

Note: You can find the WS-I Basic Security Profile online at:

<http://www.ws-i.org/Profiles/BasicSecurityProfile-1.0.html>

WS-Security

The *Web Service Security (WS-Security)* specification provides *message-level* security. An advantage of using WS-Security instead of SSL is that it can provide end-to-end message level security. Thus, the messages are protected even if the message traverses multiple systems or intermediaries. Additionally, WS-Security is independent of the transport layer protocol, so you can use it for any SOAP binding, not just for SOAP over HTTP.

Figure 1-3 shows the WS-Security elements that can be added to the SOAP header.

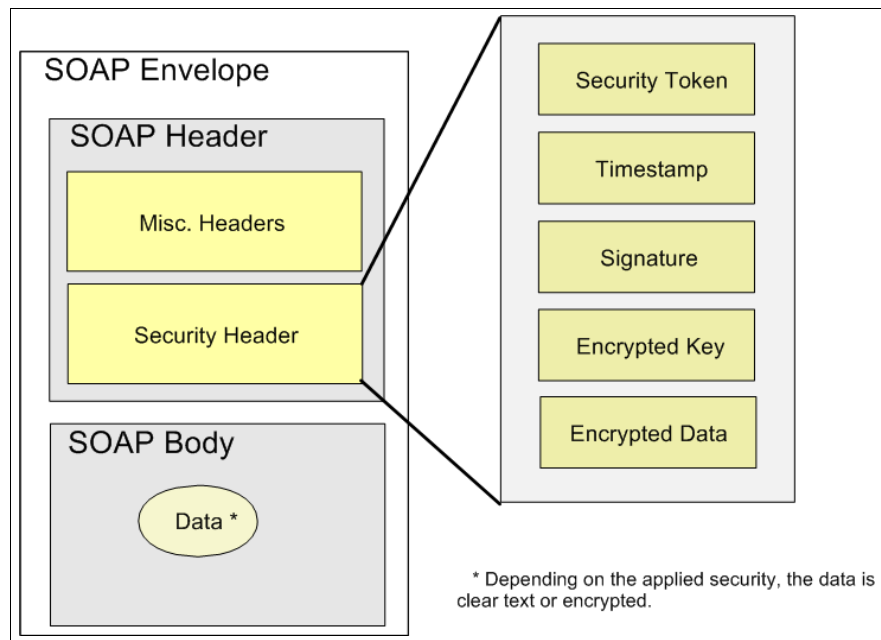


Figure 1-3 WS-Security extensions to the SOAP header

The WS-Security specification Version 1.1 was ratified by the OASIS WSS Technical Committee in February 2006. This specification proposes a standard set of SOAP extensions. It is flexible and is designed to be used as the basis for securing Web services within a wide variety of security models including PKI, Kerberos, and SAML. It supports multiple security token formats, multiple trust domains, multiple signature formats, and multiple encryption technologies to provide integrity or confidentiality.

The WS-Security specification defines the usage of XML Signature and XML Encryption. The specification includes security token propagation, message integrity, and message confidentiality. However, these mechanisms by themselves do not address all the aspects of a complete security solution. Therefore, WS-Security represents only one of the layers in a secure Web services solution design.

Web services frameworks from Microsoft, such as Web Services Enhancements (WSE) and Windows Communication Foundation (WCF), support WS-Security for runtime security. Web services software from IBM, including application development tools from Rational® and application servers from IBM WebSphere® also support WS-Security. IBM Tivoli Federated Identity Manager can process and generate WS-Security security token types.

Note: You can find more information about the OASIS WS-Security specification at:

http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss

WS-Policy

The *Web Services Policy Language* (WS-Policy) provides a flexible and extensible grammar for expressing the capabilities, requirements, and general characteristics of entities in an XML Web services-based system. WS-Policy defines a framework and a model for the expression of these properties as policies. Policy expressions allow for both simple declarative assertions as well as more sophisticated conditional assertions.

WS-Policy defines a *policy* as a collection of one or more policy assertions. Some assertions specify traditional requirements and capabilities that ultimately manifest on the wire (for example, authentication scheme and transport protocol selection). Some assertions specify requirements and capabilities that have no wire manifestation yet that are critical to proper service selection and usage (for example, privacy policy and quality of service characteristics). WS-Policy provides a single policy grammar to allow different kinds of assertions to be expressed in a consistent manner. Subordinate standards such as WS-SecurityPolicy provide more concrete profiles for interoperability in a particular class of policy.

Note: You can find the WS-Policy specification at:

<http://www.w3.org/Submission/WS-Policy/>

WS-SecurityPolicy

The WS-Policy specification defines a set of policy assertions that apply to Web services. The *Web Services-SecurityPolicy* (WS-SecurityPolicy) specification defines one profile of WS-Policy that relates to security and that provides policy assertions for WS-Security, WS-Trust, and WS-SecureConversation. WS-SecurityPolicy defines a base set of assertions that describe how messages are to be secured. Flexibility with respect to token types, cryptographic algorithms, and mechanisms used, including using transport-level security, is part of the design and allows for evolution over time. The intent is to provide enough information for compatibility and interoperability to be determined by Web services participants, along with all information necessary to actually enable a participant to engage in a secure exchange of messages.

Note: You can download the WS-SecurityPolicy specification from:

<http://docs.oasis-open.org/ws-sx/ws-securitypolicy/v1.2/ws-securitypolicy.pdf>

WS-Trust

The *Web services Trust Language* (WS-Trust) uses the secure messaging mechanisms of WS-Security to define additional primitives and extensions for the issuance, exchange, and validation of security tokens. WS-Trust also enables the issuance and dissemination of credentials within different trust domains.

To secure a communication between two parties, the two parties must exchange security credentials (either directly or indirectly). However, each party needs to determine if they can trust the asserted credentials of the other party. This specification defines extensions to WS-Security for issuing and exchanging security tokens and methods to establish and access the presence of trust relationships.

IBM Tivoli Federated Identity Manager implements the *Security Token Service* (STS) as defined in WS-Trust. You can use the STS to create, validate, and exchange security tokens for WS-Security and WS-Federation. The STS also provides for authorization of Web service requests.

Note: The WS-Trust specification is available from OASIS at:

<http://docs.oasis-open.org/ws-sx/ws-trust/200512/ws-trust-1.3-os.pdf>

WS-Federation

WS-Federation was created by a group of vendors led by IBM and Microsoft to provide extensions to the use of WS-Trust to address the identity requirements of both Web

applications and Web services. The intent is to provide a common method to support both browser based applications and Web services based applications. This commonality between browser and Web services is a differentiator for this specification over other federated single sign-on specifications. WS-Federation is closely aligned with the entire WS-Security family of standards.

WS-Federation defines extensions to the WS-Trust Security Token Service to enable identity brokering, attribute request and retrieval, authentication and authorization claims between federation partners and to protect the privacy of these claims.

Note: The WS-Federation specifications are available from OASIS at:

http://www.oasis-open.org/committees/documents.php?wg_abbrev=wsfed

Security Assertion Markup Language

Security Assertion Markup Language (SAML) is designed to provide cross-vendor single sign-on interoperability. SAML was developed by a consortium of vendors that included IBM through the OASIS Security Services Technical Council (SSTC). Figure 1-4 illustrates the components of the SAML specifications. It defines SAML assertions that describe security tokens representing users and SAML bindings and profiles for a single sign-on protocol.

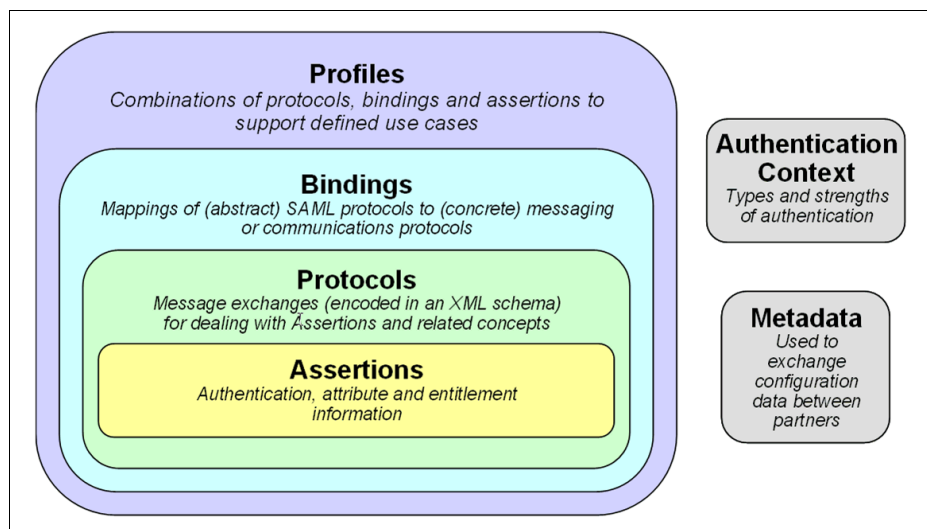


Figure 1-4 Categories of SAML specifications

An *SAML assertion* is an XML-formatted token that is used to transfer user identity (and attribute) information from a user's identity provider to trusted service providers as part of the completion of a browser single sign-on request or Web services request. A SAML assertion thus provides a vendor-neutral means of transferring information between a federation of partners. As such, SAML assertions have a lot of traction in the overall federation space.

As a protocol, SAML has three versions:

- ▶ SAML 1.0
- ▶ SAML 1.1
- ▶ SAML 2.0

SAML 1.0 and SAML 1.1 (collectively, SAML 1.x) focus on single sign-on functionality. Using Liberty Identity Federation Framework (ID-FF) 1.2 as input, SAML 2.0 represents a major functional increase over SAML 1.x. SAML 2.0 takes into account broad identity life cycle

functionality and addresses some of the privacy concerns that are associated with a federated environment.

Microsoft supports SAML 1.x assertions to represent identity in its InfoCard protocol (which is used by Windows CardSpace™), but it does not natively support SAML security tokens in Web services scenarios. Microsoft also does not support SAML protocols, bindings, or profiles. IBM Tivoli Federated Identity Manager contains all aspects of the SAML specification set.

Note: You can find more information about the SAML specification at:

http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

1.4 Conclusion

In this chapter, we discussed the IBM Security Framework and IBM Service Management initiatives and important security standards that are prevalent in both IBM and Microsoft IT solutions.

In the next chapter, we discuss the Microsoft operating systems that support IBM Tivoli Security solutions and the Microsoft middleware that IBM Tivoli Security solutions use.



IBM Tivoli Security Solutions using Microsoft operating systems and middleware

In this chapter, we provide information about:

- ▶ The Microsoft operating systems that support IBM Tivoli Security solutions
- ▶ Microsoft middleware that IBM Tivoli Security solutions use

Note: The information that we provide in this chapter assumes the state of the IBM Tivoli Security products with fixpacks as of September 2008. Later announcements and the availability of new products or fixpacks can impact the supported software products. Thus, you need to review the information that we provide here in this context. Always make sure to consult the latest product documentation. In 2.2, “Support summary by IBM Tivoli Security product” on page 13, we describe where you can obtain this information.

2.1 Microsoft products that we discuss in this chapter

In this chapter, we focus on the Microsoft software upon which Tivoli Security solutions depend. We also consider operating systems and middleware, such as directories and databases from Microsoft.

This chapter does not attempt to discuss the value that an IBM Tivoli Security solution provides to an environment of Microsoft software. We discuss that view of the integration of the Tivoli Security and Microsoft software portfolios in Chapter 3, “Integration with Microsoft software environments” on page 19.

2.1.1 Operating systems

Microsoft server operating system product families, such as Microsoft Windows Server® 2003 and 2008, are the primary platforms that we discuss. We also discuss Microsoft client operating system products such as Microsoft Windows XP and Microsoft Windows Vista®. Microsoft provides 32- and 64-bit versions of its more recent operating systems. In this paper, we discuss only operating systems that are still supported.

2.1.2 Middleware

Middleware is an industry term to describe common reusable software systems that simplify and standardize the construction of software applications. In the context of Microsoft middleware and IBM Tivoli Security solutions, we consider the following product families:

- ▶ Active Directory
- ▶ SQL Server
- ▶ Internet Information Services (IIS)
- ▶ Certificate Services

Active Directory

Active Directory is a key component of the Microsoft server operating systems. Active Directory is a directory that contains information about users, groups, and other objects that exist in a Windows network environment. It includes a Kerberos authentication service, and its data is available through LDAP or Microsoft Active Directory Service Interfaces (ADSI).

Microsoft also offers *Active Directory Application Mode (ADAM)*. ADAM is an LDAP directory that runs as a user service on Microsoft Windows platforms. This component offers different deployment choices compared to the Active Directory system service.

SQL Server

Microsoft *SQL Server*® is a relational database management server system (RDBMS). It uses Structured Query Language (SQL) and can be accessed using Open Database Connectivity (ODBC) and Java™ Database Connectivity (JDBC™).

Internet Information Services (IIS)

Microsoft *Internet Information Services (IIS)* is a Web server. IIS is also the HTTP front-end for the Microsoft ASP.NET application server.

Certificate Services

Microsoft *Certificate Services* is a component of the Windows server operating systems that provides an important operational service for a public key infrastructure (PKI). Certificate Services allow certificates to be issued and managed throughout their life cycle.

Microsoft Certificate Services is standards based. The certificates issued by Certificate Services can be used with all of the Tivoli Security products where use of certificates is either required or optional. Thus, no explicit references are made to Microsoft Certificate Services in the next section.

2.2 Support summary by IBM Tivoli Security product

The IBM Tivoli Security development organization, along with the remainder of the IBM Software Group, identifies the Microsoft operating environment as a strategic platform for its products. We discuss examples of the operating system and middleware support in the following sections, decomposed by IBM Tivoli Security product. The range of platform support for Tivoli Security solutions is dynamic and further platform support (major or fixpack releases) are delivered periodically through the IBM support process.

Tivoli provides a single location on the IBM Support site to find the current platform support information for all of its products:

<http://www.ibm.com/support/search.wss?q=Tivoli+Platform+Support+Matrix>

Note: The information in the remaining sections of this chapter was correct as of September 2008. We discuss support that is present only in the latest versions of IBM Tivoli Security solutions. You can find details for earlier versions of IBM Tivoli Security solutions and any considerations about the required fixpack levels at the IBM Support site available at the Web address listed above.

Note: This chapter does not provide detailed information about the IBM Tivoli Security products themselves. If you want additional information about these products, start at the portfolio home page on the IBM Web site:

<http://www.ibm.com/software/tivoli/solutions/security/products.html>

2.2.1 IBM Tivoli Directory Server

Tivoli Directory Server is the LDAP-compliant enterprise directory from IBM. Tivoli Directory Server uses IBM DB2® as the database that stores its directory information.

For Tivoli Directory Server Version 6.1:

- ▶ The Tivoli Directory Server server is supported on Windows Server 2003 (Standard, Enterprise and Data Center Editions). On 64-bit Windows platforms, the server runs as a native 64-bit application.
- ▶ The Tivoli Directory Server client runs on all 32-bit Windows XP, Windows Vista, and Windows Server 2003 platforms. On 64-bit Windows platforms, the Tivoli Directory Server client is available in 32- or 64-bit modes. On Windows Server 2008 platforms, the Tivoli Directory Server client is currently supported in 32-bit mode only.

2.2.2 IBM Tivoli Directory Integrator

Tivoli Directory Integrator is a flexible multiprotocol application that can be used for data synchronization.

For Tivoli Directory Integrator Version 6.1.1:

- ▶ The Tivoli Directory Integrator server runs on Windows Server 2003 (Standard and Enterprise Editions). On 64-bit Windows platforms, Tivoli Directory Integrator server runs in 32-bit mode.
- ▶ The Tivoli Directory Integrator Configuration Editor can also run on Windows XP and Windows Vista.

2.2.3 IBM Tivoli Access Manager Family

The Tivoli Access Manager product family provides authentication, authorization, and single sign-on solutions.

IBM Tivoli Access Manager for e-business

Tivoli Access Manager for e-business provides a Web access management solution with authentication, single sign on, and authorization capabilities.

For Tivoli Access Manager for e-business Version 6.1:

- ▶ Tivoli Access Manager for e-business components running on Windows 2003 Standard or Enterprise Editions run in 32-bit mode on both 32-bit and 64-bit versions of the operating system.
- ▶ Tivoli Access Manager for e-business components running on Windows 2008 Standard or Enterprise Editions run in 32-bit mode on both 32-bit and 64-bit versions of the operating system.
- ▶ The Web Security Plug-in for Microsoft IIS supports IIS versions 6.0 and 7.0.
- ▶ The Web Security Plug-ins for Microsoft IIS and IBM HTTP Server are only supported on 32-bit versions of Windows Server 2003 and Windows Server 2008.
- ▶ Developer components, such as the Application Developer's Kit, Runtime, and Runtime for Java, are also supported on Windows XP and Windows Vista operating systems.
- ▶ For complete information about Tivoli Access Manager for e-business components and the Microsoft Windows operating systems on which they are supported, refer to:

http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.itame.doc/am61_relnotes16.htm

Tivoli Access Manager for e-business Version 6.1 also supports the following Microsoft directory solutions:

- ▶ Microsoft Active Directory is one of the supported user registries for Tivoli Access Manager for e-business. If the Active Directory option is chosen the Tivoli Access Manager Policy Server must run on Windows 2003 server in this case.
- ▶ Tivoli Access Manager also supports Microsoft Active Directory Application Mode (ADAM). If this option is chosen there are no constraints on what supported operating system the Tivoli Access Manager Policy Server should run.

IBM Tivoli Access Manager for Enterprise Single Sign-on

Tivoli Access Manager for Enterprise Single Sign-on is a single sign-on solution for Web, Java, and desktop applications.

For Tivoli Access Manager for Enterprise Single Sign-on Version 8.0:

- ▶ The Integrated Management System Server component is supported on Windows Server 2003 operating systems (all editions).
- ▶ The AccessAgent component is the component that orchestrates single sign-on on a user's desktop (or virtual desktop). It is supported on Windows XP, Windows XP Tablet, Windows Vista, Windows CE, and Windows Server 2003 Terminal Services.
- ▶ Microsoft SQL Server 2000 and 2005 are supported for the Tivoli Access Manager for Enterprise Single Sign-on database, which holds credentials, policies, audit logs, and backups.
- ▶ Microsoft Active Directory is supported as an enterprise directory. When a user is added to Tivoli Access Manager for Enterprise Single Sign-on, Active Directory can be checked to verify the user. If desired, you can configure password synchronization between Active Directory and Tivoli Access Manager for Enterprise Single Sign-on.

2.2.4 IBM Tivoli Identity Manager

Tivoli Identity Manager manages the complete life cycle of identities. Tivoli Identity Manager includes capabilities such as provisioning, recertification, and workflow.

For Tivoli Identity Manager Version 5.0:

- ▶ The Tivoli Identity Manager server (a WebSphere application) is supported on Windows Server 2003 and Windows Server 2008 (Standard and Enterprise Editions). The Tivoli Identity Manager server is supported on 32-bit and 64-bit versions of the operating systems.
- ▶ The Tivoli Identity Manager server relies on a relational database to store information about scheduled tasks, mirror identity data for reporting and store Tivoli Identity Manager audit data. Tivoli Identity Manager includes Microsoft SQL Server 2005 Enterprise Edition as one of its supported database options.
- ▶ The Tivoli Identity Manager architecture includes adapters for integrating with different systems that it manages. We discuss Tivoli Identity Manager adapters for managing Microsoft products in Chapter 3, "Integration with Microsoft software environments" on page 19. In addition, adapters for many other systems, such as SAP® can be hosted on a Microsoft operating system. The complete list of Tivoli Identity Manager 5.0 adapters, and the operating systems on which they run, are available on the IBM Support site:

<http://www.ibm.com/support/docview.wss?uid=swg21292014>

2.2.5 IBM Tivoli Federated Identity Manager

Tivoli Federated Identity Manager provides federated Web single sign-on and identity propagation services for service-oriented architecture (SOA). Tivoli Federated Identity Manager is a WebSphere application.

Tivoli Federated Identity Manager Version 6.2 is supported on Windows Server 2003 (Standard, Enterprise, and Datacenter Editions). The federated SSO and runtime components of Tivoli Federated Identity Manager are also supported on Windows Server 2008. The plug-in for IIS is not supported on Windows Server 2008.

2.2.6 IBM Tivoli Security Information and Event Manager

Tivoli Security Information and Event Manager is a suite of software products that provide a complete solution for policy based management of security information.

IBM Tivoli Security Operations Manager

Tivoli Security Operations Manager improves administrator efficiency for handling security information and event information by aggregating and correlating security information to identify incidents that might require further investigation.

For Tivoli Security Operations Manager Version 4.1.1, the Central Management System (CMS) and Event Aggregation Module (EAM) components are supported on the Microsoft Windows 2003 Server SP2 (64-bit) platform.

The Universal Collection Module (UCM) is supported on Windows systems. The Universal Collection Module is used to collect events from sensors that cannot be configured to send events directly to the EAM using one of its standard data collection mechanisms.

The Tivoli Security Operations Manager user interface (a Java client application) is supported on Windows XP.

Tivoli Compliance Insight Manager

Tivoli Compliance Insight Manager provides automated user activity monitoring across heterogeneous systems. Tivoli Compliance Insight Manager provides dashboard and reporting to help measure an organization's security posture and respond to auditors' requests.

For Tivoli Compliance Insight Manager Version 8.5, the Tivoli Compliance Insight Manager server is supported on 32- and 64-bit versions of Microsoft Windows Server 2003 (Standard and Enterprise Editions). Microsoft IIS is used to serve the Tivoli Compliance Insight Manager Web applications.

Tivoli Compliance Insight Manager actuators (which collect audit data) are supported on Windows XP and Windows Server 2003 operating systems.

2.2.7 IBM Tivoli Security Compliance Manager

Tivoli Security Compliance Manager provides compliance management for desktop and server systems by collecting configuration data from those systems, comparing it to defined configuration policies, reporting on exceptions and performing remediation.

For Tivoli Security Compliance Manager Version 5.1.1.1:

- ▶ The Tivoli Security Compliance Manager server is supported on Windows Server 2003 (Standard and Enterprise Editions).
- ▶ The Tivoli Security Compliance Manager client and collectors are supported on Windows XP and Windows Server 2003 (Standard and Enterprise Editions).
- ▶ The Tivoli Security Compliance Manager console is supported on Windows XP and Windows Server 2003 (Standard and Enterprise Editions).

2.2.8 IBM Tivoli zSecure Suite

The Tivoli zSecure Suite provides a rich set of security and compliance capabilities for mainframe environments. Although the majority of zSecure products run on z/OS® itself, one component, zSecure Visual, provides administration of z/OS security from the Windows platform. The zSecure Visual Client 1.9 is supported on Windows XP and 32-bit Windows Vista operating systems.

2.3 Conclusion

In this chapter, we provided information about the supported Microsoft software platforms for IBM Tivoli Security products. In the next chapter, we describe the integration between IBM Tivoli Security solutions and Microsoft software. Specifically, we focus on the integration scenarios where IBM Tivoli solutions augment the security and compliance of a Microsoft software environment.



Integration with Microsoft software environments

In this chapter, we describe the integration between IBM Tivoli Security solutions and Microsoft software. Specifically, we focus on the integration scenarios where IBM Tivoli solutions augment the security and compliance of a Microsoft software environment.

We have structured this chapter according to the major solution areas that we introduced in 1.1, “IBM Security Framework” on page 2.

- ▶ Security compliance
- ▶ Identity and access
- ▶ Information security
- ▶ Application security
- ▶ Infrastructure security

3.1 Security compliance

IBM Tivoli Compliance Insight Manager provides a centralized solution for security compliance management. It collects audit data from *event sources* through *actuators*. *User information* sources provide Tivoli Compliance Insight Manager with a common view of user and group information. Tivoli Compliance Insight Manager can use Microsoft Active Directory as a user information source.

Tivoli Compliance Insight Manager provides the following actuators for integrating with Microsoft application environments:

- ▶ Windows Event Viewer, for collecting security, system and application log information from Windows XP, Windows 2000 and Windows Server 2003 systems. The actuator uses an API, which allows the actuator to connect to remote Windows systems.
- ▶ Active Directory, supporting a wide variety of possible event types from the Directory Service event log.
- ▶ Internet Information Services, which consumes Web request information in Microsoft IIS log file format and W3C extended log file format.
- ▶ SQL Server, which uses the SQL Trace facility and provides more detailed information than SQL Server entries in the application event log.
- ▶ W7, for consuming audit information that has been pre-processed into this normalized Tivoli Compliance Insight Manager format. This can be used to integrate custom application audit data into a Tivoli Compliance Insight Manager solution.

Tivoli Compliance Insight Manager also provides a variety of application specific actuators where the event source is provided on a Windows system. Examples include Tivoli Access Manager, Tivoli Identity Manager, and SAP.

3.2 Identity and access

The IBM Tivoli Security product portfolio possesses a rich set of identity and access management capabilities for a Microsoft environment. In this section, we discuss these capabilities in the context of:

- ▶ Identity data synchronization
- ▶ Password synchronization
- ▶ User life cycle management
- ▶ Desktop single sign-on
- ▶ Web single sign-on
- ▶ Identity propagation in service-oriented architecture
- ▶ Federated single sign-on
- ▶ Role-based access control

3.2.1 Identity data synchronization

Tivoli Directory Integrator provides a changelog connector for Microsoft Active Directory. The changelog connector detects changes in Active Directory data. The changes can be used in Tivoli Directory Integrator solutions to propagate to a variety of systems based on Tivoli Directory Integrator's rich set of connectors. The changelog connector can be used to detect new, modified, and deleted entries in Active Directory.

For more information about the Active Directory Changelog connector, consult the Tivoli Directory Integrator Reference Guide, which is available at:

http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.IBMDI.doc_6.1.1/referenceguide12.htm#adconnectv2

Tivoli Directory Server provides a tool for data synchronization with Active Directory based on the Tivoli Directory Integrator changelog connector. The tool synchronizes user and group data from Active Directory to Tivoli Directory Server. Passwords are not synchronized by this solution. This tool can be used for simple data synchronization between Tivoli Directory Server and Active Directory. Because the tool is built using Tivoli Directory Integrator, you can readily customize it to meet the requirements of a specific environment.

The Tivoli Directory Server Administration Guide provides more information about the Tivoli Directory Server tool for Active Directory synchronization. It is available at:

http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.IBMDI.doc/admin_gd37.htm

3.2.2 Password synchronization

Password synchronization involves intercepting password changes on one system and propagating those changes to other systems. A common use case is using password policy on the frequently used network login to trigger password changes. Tivoli Directory Integrator provides password synchronization plug-ins for a number of directories, including Microsoft Active Directory domain controllers and standalone Microsoft Windows systems. The plug-in exploits a documented Microsoft Windows interface for implementing password filters described on the Microsoft Developer Network:

<http://msdn.microsoft.com/en-us/library/ms721766.aspx>

The Tivoli Directory Integrator plug-in can propagate password changes to one of two intermediate stores:

- ▶ An LDAP server
- ▶ A WebSphere MQ Everyplace® queue

Password changes in the intermediate store can be stored using symmetric encryption to reduce their exposure to unauthorized entities. A Tivoli Directory Integrator configuration can then read from the password store to propagate the password to other systems as required. Tivoli Directory Integrator's AssemblyLine architecture and library of connectors provides a comprehensive set of components with which to build the password propagation solution.

In a Microsoft Active Directory environment containing multiple domain controllers, the Tivoli Directory Integrator password plug-in must be installed and configured in each domain controller instance, which is a requirement based on the interface that Microsoft Windows provides.

The Tivoli Directory Integrator Password Synchronization Plug-ins Guide describes the Tivoli Directory Integrator Windows Password Synchronization Plug-in in detail:

http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.IBMDI.doc_6.1.1/pluginsguide23.htm

3.2.3 User life cycle management

Tivoli Identity Manager manages the life cycle of users and their accounts across a variety of systems. The interface between the Tivoli Identity Manager server and a managed system is an *adapter*.

Managing users in Active Directory

Tivoli Identity Manager provides an adapter for Active Directory. The Active Directory adapter provides connectivity between Tivoli Identity Manager and the network of systems running the Active Directory. The adapter runs as a Windows service. The following user account management tasks can be achieved using the Active Directory adapter and Tivoli Identity Manager:

- ▶ Adding Active Directory user accounts
- ▶ Creating a home directory for a user account
- ▶ Modifying attributes of Active Directory user accounts
- ▶ Changing passwords of Active Directory user accounts
- ▶ Suspending, restoring, and deleting Active Directory user accounts
- ▶ Retrieving user accounts from the Active Directory
- ▶ Managing mailboxes on the Exchange server
- ▶ Moving a user in the Active Directory hierarchy

For more information about the capabilities of the Tivoli Identity Manager adapter for Active Directory, consult the adapter's user guide, which is available at:

http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.itim.doc/pdf/usr_winad_50.pdf

Tivoli Identity Manager provides a password synchronization plug-in for Active Directory that is installed on all domain controllers in the Active Directory domains being managed by Tivoli Identity Manager. The plug-in intercepts password change operations from Active Directory (whether user or administrator initiated). The plug-in can optionally connect to Tivoli Identity Manager to validate the password against the Tivoli Identity Manager password policy. Tivoli Identity Manager can then propagate the new password to the user's accounts on other systems to complete the password synchronization process.

The Password Synchronization for Active Directory Plug-in Installation and Configuration guide provides more information about the password synchronization plug-in for Active Directory. It is available at:

<http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.itim.doc/pdf/adpwdsync50.pdf>

Managing user in Windows operating systems

Tivoli Identity Manager also provides an adapter for interfacing with standalone Windows systems (Windows XP, Windows 2000, and Windows 2003) that are not part of an Active Directory domain. This adapter is called the Windows Local Account adapter, and it is described at:

<http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.itim.doc/pdf/wla50.pdf>

Managing SQL Server users

SQL Server users can be defined at the operating system or database level. For operating system users, you can use the Tivoli Identity Manager adapters to manage the identity life cycle for those users. For users who are defined at the database level, there is a Tivoli Identity

Manager adapter for Microsoft SQL Server Adapter. You can use this adapter to automate the following administrative tasks:

- ▶ Creating an account to authorize access to SQL server.
- ▶ Modifying an existing account to access SQL server.
- ▶ Removing access to a user account. This deletes the account from the SQL server.
- ▶ Suspending a user account by temporarily denying access to SQL server.
- ▶ Changing a user account password on SQL server.
- ▶ Reconciling user account information of all current accounts on SQL server.
- ▶ Reconciling the account information of a particular user account on SQL server by performing a lookup.

For more information about the capabilities of the Tivoli Identity Manager adapter for Microsoft SQL Server, consult the adapter's installation and configuration guide:

<http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.itim.doc/pdf/sql50.pdf>

Managing users in a SQL Server database table

Some applications might maintain their own user registry (or user profiles) in a customized schema in the Microsoft SQL Server relational database. In these cases, a custom adapter for Tivoli Identity Manager can be implemented to manage account/profile information in the Microsoft SQL Server database. Construction of the Tivoli Identity Manager adapter is accelerated with a wizard based application called the Tivoli Identity Manager Adapter Development Tool:

<http://catalog.lotus.com/wps/portal/topal/details?catalog.label=1TW10IM0H>

Managing users from Microsoft .NET

In Microsoft .NET 2.0, the membership provider interface was introduced. The membership provider model offers a common interface to aspects of managing a user repository, including adding and removing users, password management capabilities, and simple user name and password authentication.

More information about the membership provider integration between Tivoli Access Manager and Microsoft .NET is available at:

<http://www.ibm.com/support/docview.wss?uid=swg24019168>

Managing users in Microsoft Office SharePoint Server

Managing users in Microsoft Office SharePoint® Server is a two-step process:

- ▶ Managing users in the user registry

A SharePoint environment is configured usually to use Active Directory as the user registry, though it can also be configured to use LDAP or any other Microsoft .NET 2.0 membership provider, as described in the preceding section. Standard Tivoli Identity Manager adapters for Active Directory, LDAP, or Tivoli Access Manager are used to managing these user accounts.

- ▶ Managing SharePoint-specific entitlements

Windows SharePoint Services Web services is a capability provided with SharePoint Server to perform a number of tasks in the SharePoint Server, including administrative methods such as creating and deleting sites and controlling user access to SharePoint.

3.2.4 Desktop single sign-on

Tivoli Access Manager for Enterprise Single Sign-on provides identity and access management capabilities directly on Windows desktops. Tivoli Access Manager for Enterprise Single Sign-on integrates with a variety of strong authentication devices and solutions to offer a choice in how high assurance desktops are accessed. Tivoli Access Manager for Enterprise Single Sign-on provides single sign-on and password management for Windows thick client, Web, mainframe and terminal emulation applications running on Windows desktops and from within remote access Windows environments such as those provided by Citrix. Tivoli Access Manager for Enterprise Single Sign-on supports a variety of desktop options, including shared, roaming, and private desktops.

Tivoli Access Manager for e-business offers an authentication mechanism using on the Simple and Protected GSS-API Negotiation mechanism (1.3.3, “SPNEGO” on page 4). This mechanism allows a user who has already authenticated to an Active Directory domain to identify themselves to a Tivoli Access Manager for e-business Web security component (for example, WebSEAL) without explicitly supplying their credentials. The trustworthiness of the identity is established through SPNEGO’s underlying use of the Kerberos authentication protocol (1.3.2, “Kerberos” on page 4).

An advantage of Tivoli Access Manager for e-business’s SPNEGO implementation is that the Web security component can run on any of the Tivoli Access Manager for e-business supported operating systems, not just Microsoft Windows. You can find more information about Tivoli Access Manager for e-business’s support for SPNEGO authentication in the WebSEAL Administration Guide, which is available at:

http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.itame.doc/am61_webseal_admin661.htm#chap-ss-windows-desktop

3.2.5 Web single sign-on

This section examines a few different aspects of a Web single sign-on approach.

SSO using Identity Assertion

In the Web context, Figure 3-1 shows the general pattern for single sign-on (SSO) with Tivoli Access Manager for e-business. A user authenticates to one of the Tivoli Access Manager for e-business Web security servers, such as WebSEAL or a plug-in for Web servers. In a Microsoft environment, Tivoli Access Manager for e-business provides a plug-in for Microsoft Internet Information Services (IIS).



Figure 3-1 Web single sign-on architecture

Asserting the identity of the authenticated user from a Tivoli Access Manager for e-business Web security server to a Web application is achieved by sending information about the authenticated user identity in HTTP headers to the Web environment being protected. The simplest and most commonly used example is to send the user ID in an HTTP header. The identity assertion is meaningful when the receiving Web application or Web application server environment can trust the asserted identity (see Figure 3-2). Tivoli Access Manager for

e-business's collection of Web SSO techniques offers different mechanisms to establish trust, each with different strength, administration and performance characteristics.

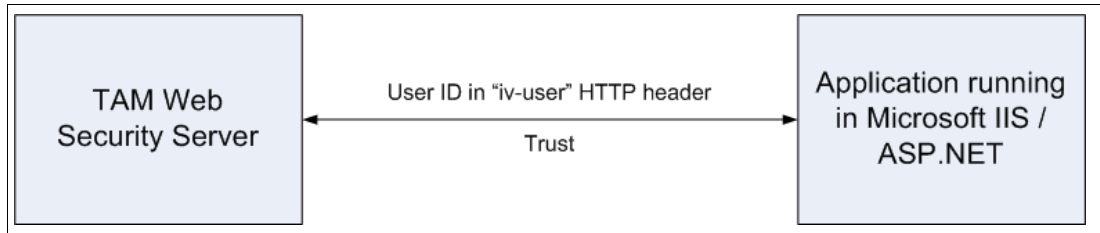


Figure 3-2 Trusted identity assertion

For applications running in Microsoft IIS or ASP.NET but not using Microsoft security, this form of identity assertion is often preferred. Additional identity information such as attributes from the user's entry in the Tivoli Access Manager directory or the set of group memberships can also be provided by the Tivoli Access Manager for e-business Web security server. Trust can be established at the transport layer through the use of SSL.

Microsoft ASP.NET application server provides an interface for integrating alternate authentication mechanisms. Tivoli Access Manager for e-business exploits this with an integration module (AMNET in Figure 3-3) that works in conjunction with a Tivoli Access Manager for e-business Web security server to establish the identity of the authenticated Tivoli Access Manager user in the ASP.NET container. Two choices are provided for how the identity is established in the ASP.NET environment.

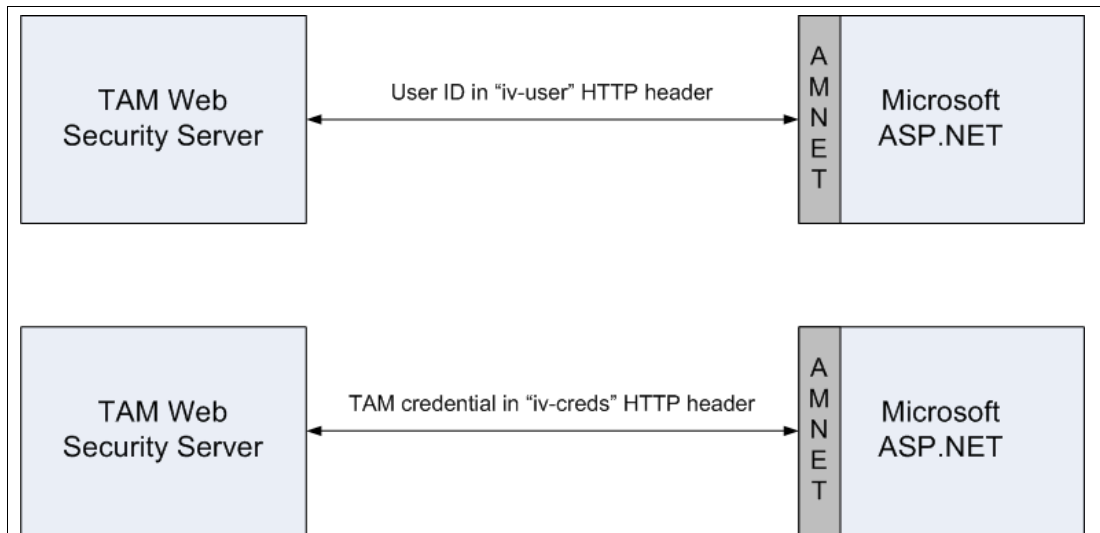


Figure 3-3 Single sign-on to Microsoft ASP.NET

Establishing the identity with the *iv-creds* HTTP header passes the entire Tivoli Access Manager credential to the AMNET authentication module as base 64 encoded data. This procedure makes the operation of the AMNET module more efficient because it does not have to contact the Tivoli Access Manager directory to retrieve additional user information such as group memberships. Users who are members of a large number of groups might have a Tivoli Access Manager credential large enough to exceed the maximum header size of the Microsoft IIS server. For these cases, the option to assert identity with the user ID is provided, though its use does require an additional interaction with the Tivoli Access Manager directory to establish the user's identity in the ASP.NET application server.

Trust between the Tivoli Access Manager for e-business Web security server and AMNET authentication module can be configured using one or more of these techniques:

- ▶ Verify use of server authenticated SSL.
- ▶ Verify use of mutually authenticated SSL.
- ▶ Verify the presence of one or more HTTP headers inserted by the Tivoli Access Manager Web security server.
- ▶ Verify the contents of the HTTP *Via* header.
- ▶ Authenticate the origin of the request by binding to the Tivoli Access Manager directory with a password supplied by the Tivoli Access Manager for e-business Web security server and an application identity configured in the AMNET authentication module's stanza of the ASP.NET application's configuration file.

You can find more information about the single sign-on integration between Tivoli Access Manager and Microsoft ASP.NET in the Integration Guide, which is available at:

<http://www.ibm.com/support/docview.wss?uid=swg24019168>

Some applications, such as Microsoft Office SharePoint Server, rely on operating system level security. So, it is important that the identity of the user be established in the request context in IIS, not just ASP.NET. In Active Directory domain environments, Tivoli Access Manager for e-business provides an integration with the Microsoft IIS server that uses a Microsoft extension to the Kerberos protocol to impersonate a user.

The integration is implemented as an extension in IIS (Figure 3-4). It extracts the authenticated user identity from the HTTP request and contacts an Active Directory domain controller to get an impersonation security token for the user. This impersonation security token is used to set the current identity in the context of the request being processed by IIS.

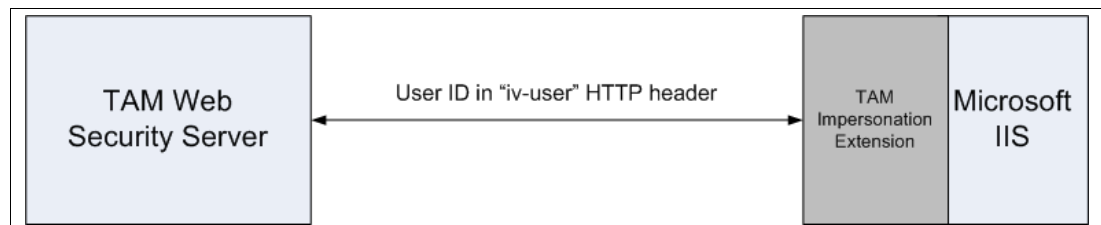


Figure 3-4 Single sign-on to Microsoft IIS

You can find more information about the impersonation integration between Tivoli Access Manager and Microsoft IIS in the Integration Guide, which is available at:

<http://www.ibm.com/support/docview.wss?uid=swg24016387>

Building on this integration is an additional SSO integration with Tivoli Access Manager for Microsoft SharePoint Services 3.0 and Microsoft Office SharePoint Server 2007. You can find more information at:

<http://www.ibm.com/support/docview.wss?uid=swg24006813>

An extension to this standard integration scenario is available on the IBM developerWorks site. It addresses the use case that allows Microsoft Office Client integration used with a variety of different Tivoli Access Manager for e-business authentication mechanisms. Consult the IBM developerWorks site for further information:

<http://www.ibm.com/developerworks/tivoli/library/t-socitam/index.html>

SSO using Kerberos

The Kerberos network authentication protocol is gaining popularity in many enterprises. Microsoft Active Directory operates as a Kerberos authentication server and key distribution server. The SPNEGO protocol is the basis of the Integrated Windows Authentication mechanism in Microsoft IIS and Microsoft Internet Explorer. When a Tivoli Access Manager for e-business WebSEAL server is configured to use SPNEGO (see 3.2.4, “Desktop single sign-on” on page 24), the Kerberos credentials of the user do not flow from WebSEAL back to Web applications.

For environments that require use of Kerberos for authentication to Web applications, Tivoli Access Manager for e-business Version 6.1 introduces a method to obtain a Kerberos credential on behalf of the authenticated Tivoli Access Manager user and send to a Web server such as Microsoft IIS to achieve SSO, as shown in Figure 3-5.

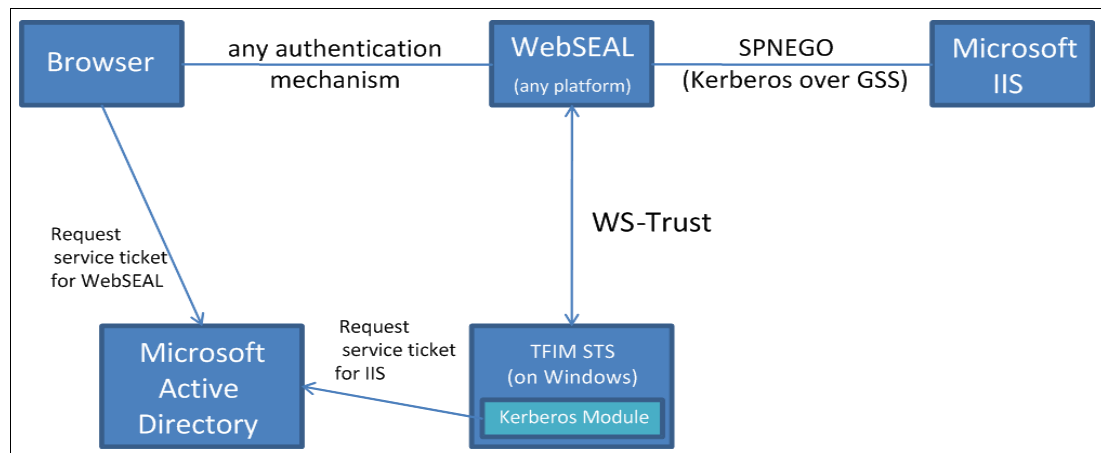


Figure 3-5 Single sign-on using end-to-end Kerberos

This SSO approach uses a Tivoli Federated Identity Manager environment (Version 6.2 or higher) to generate the Kerberos security tokens. An advantage of this approach is that the Tivoli Access Manager for e-business Web security server can run on any supported platform (not just Windows) and the ability to achieve SSO in this way is independent of the authentication mechanism used to authenticate to WebSEAL.

For more information about configuring WebSEAL for Kerberos based SSO to Microsoft IIS, consult the Tivoli Access Manager for e-business product documentation:

http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.itame.doc/am61_webseal_admin631.htm#sso-tfim-kerberos

3.2.6 Federated single sign-on

Microsoft Active Directory Federation Services (ADFS) and Tivoli Federated Identity Manager both implement the WS-Federation standard for identity federation. This specification allows users in a Microsoft Active Directory environment to seamlessly sign on to other applications that are protected by Tivoli Federated Identity Manager and Tivoli Access Manager for e-business and vice versa.

Microsoft and IBM collaborated on a step-by-step guide for integrating Microsoft ADFS and Tivoli Federated Identity Manager using the WS-Federation. The guide is available at:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=C6F6D212-5625-4922-896F-6B6A3921DFD4&displaylang=en>

Tivoli Federated Identity Manager also integrates with Microsoft Windows CardSpace, which is a user centric identity system. Tivoli Federated Identity Manager has the capability to act as an identity provider (that issues Information Cards to users) as well as a replying party (that requests Information Cards from users).

Tivoli Federated Identity Manager also supports additional industry specifications such as Security Assertion Markup Language (SAML), the Liberty Alliance's Identity Federation Framework (ID-FF), and OpenID. This support allows the Tivoli Federated Identity Manager solution to federate identities with other environments regardless of which industry specification they choose to implement or are able to support.

3.2.7 Identity propagation in service-oriented architecture

Service-oriented architecture (SOA) connects loosely coupled services to construct new applications. These services have their own user registries, which are often administered in isolation from those of other services in the SOA environment. Users and service entities in a homogeneous environment such as this are likely to have different identities in the various services that make up a composite application. Establishing the identity of the service requestor in each service request is a fundamental step in ensuring that business requirements such as authorization, audit and compliance can be implemented.

The IBM SOA identity propagation solution is built on open standards. The WS-Security family of standards ("WS-Security" on page 5) was co-authored by IBM, Microsoft, and others to describe how interoperable authentication, integrity, and confidentiality is provided for Web services. The WS-Trust standard ("WS-Trust" on page 7) is the open mechanism by which:

- ▶ Security tokens are validated, issued, and renewed.
- ▶ Trust relationships are established, assessed, and brokered.

WS-Trust is defined by a Web services interface. The service that implements the WS-Trust interface is known as a *Security Token Service* (STS). In the IBM SOA identity propagation solution, the STS is a component of the Tivoli Federated Identity Manager product.

The SAML security token is an XML identity representation that is particularly suited for use in identity propagation scenarios because:

- ▶ SAML is an open standard widely implemented by vendors.
- ▶ No password synchronization is required.
- ▶ Arbitrary attribute lists can be included, not just user name.
- ▶ Attribute data can be selectively protected through digital signatures and encryption.

Microsoft ASP.NET and Web Services Enhancements (WSE) does not natively support the SAML security token in SOA identity propagation scenarios. Integrating SAML with ASP.NET can be implemented with a custom security filter that uses the Tivoli Federated Identity Manager STS to transform identities between native Microsoft identities and SAML security tokens. You can find more information about the custom security filter approach in the following developerWorks article:

http://www.ibm.com/developerworks/tivoli/library/t-samlwse/index.html?S_TACT=105AGX14&S_CMP=EDU

The Kerberos security token profile that is defined in the WS-Security specifications is implemented in Microsoft ASP.NET. Some integration scenarios with IBM WebSphere environments require additional identity transformation. You can enable this integration by Tivoli Federated Identity Manager as described in the following article:

http://www.ibm.com/developerworks/tivoli/library/t-tfim-kerberos/index.html?S_TACT=105AGX14&S_CMP=EDU

These techniques allow interoperable identity propagation in SOA scenarios involving Microsoft components (such as Microsoft Office SharePoint Server), IBM WebSphere Enterprise Service Buses, and enterprise information systems such as CICS® and Integrated Management System running on a mainframe.

3.2.8 Role-based access control

Role-based access control (RBAC) includes three cooperating processes:

- ▶ Managing user-role relationships for the user population
- ▶ Authoring security policy to define access relationships between roles and resources
- ▶ Enforcing role based access control

Many commercial and custom applications can use Active Directory as a user directory. In these cases, application roles are often associated with Active Directory groups. The Tivoli Identity Manager adapter for Active Directory can manage an account's group memberships, which contributes to the management of RBAC.

Tivoli Access Manager implements the standard interfaces that represent a principal and identity in Microsoft .NET. These allow Microsoft .NET applications to determine a user's role membership declaratively (Example 3-1) or programmatically (Example 3-2).

Example 3-1 Declarative example of Microsoft .NET RBAC

using System.Security.Permissions;

```
[PrincipalPermissionAttribute(SecurityAction.Demand, Role="Employee")]
public class HRRecord
{
    ...

    [PrincipalPermissionAttribute(SecurityAction.Demand, Role="Manager")]
    public void AdjustSalary(...)
    {
        ...
    }

    ...
}
```

Example 3-2 Programmatic example of Microsoft .NET RBAC

```
System.Security.Principal.IPrincipal prin = HttpContext.Current.User;
bool result = prin.IsInRole("rolename");
```

You can configure the Tivoli Access Manager evaluation of role membership so that it is based on Tivoli Access Manager group membership. This configuration can be equivalent to Active Directory group membership in the case that Tivoli Access Manager is configured to use Active Directory as its user registry. A second option provided by the Tivoli Access Manager integration is to perform a Tivoli Access Manager authorization decision to determine membership of a role. This option provides additional flexibility for roles whose membership is extremely dynamic.

The role provider interface provides a common interface to manage roles and their members, as well as provide role membership decisions.

You can find more information about the RBAC integration between Tivoli Access Manager and Microsoft .NET in the Integration Guide, which is available at:

<http://www.ibm.com/support/docview.wss?uid=swg24019168>

3.3 Information security

The IBM Information Security Management solution is a policy-based process that is focused on understanding that classes of data or information that exist and the type of security controls that need to be applied to that information. It continues with the implementation and enforcement of these controls and then the monitoring for the effectiveness of these controls and what is happening to the data and its supporting infrastructure on an ongoing basis.

Tivoli Compliance Insight Manager is the monitoring aspect of the IBM Information Security Management solution. Tivoli Compliance Insight Manager provides privileged user monitoring (PUMA) by collecting audit data from a wide variety of systems and applications. Access to enterprise's data (including unstructured data) stored on Windows file systems can be audited using native Windows auditing. Tivoli Compliance Insight Manager collects and centralizes this audit data, where it is translated into common business language for non-technical users. Alerts® can be established for activity deemed irregular according to the specific policies defined for the environment being monitored.

3.4 Application security

IBM Rational AppScan scans and tests for vulnerabilities in Web applications, including those developed using the Microsoft IIS and Microsoft ASP.NET platforms. IBM Rational AppScan provides remediation guidance when vulnerabilities are uncovered. IBM Rational AppScan can be used on an application during development, test or when running in a live production environment. More information about IBM Rational AppScan can be found at:

<http://www.ibm.com/software/awdtools/appscan/>

Tivoli Access Manager for e-business protects Web applications by providing a hardened reverse-proxy component (WebSEAL) that controls access to the applications. Tivoli Access Manager for e-business can immediately remediate many of the types of vulnerabilities identified in applications by IBM Rational AppScan.

3.5 Infrastructure security

Tivoli Security Operations Manager provides a sensor to collect data from the Windows event log. The event data (for example, application, system and security events) are collected by the Universal Collection Module and sent to the Event Aggregation Module for forwarding on to the Central Management Server.

Tivoli Security Operations Manager provides a sensor that can monitor a file system directory for new log files. This feature is used when collecting logs from Microsoft Internet Information Server.

Tivoli Security Operations Manager provides a sensor that can monitor relational databases. This enables collection of audit events for applications that store their audit data in a table in a Microsoft SQL Server database.

Tivoli Security Compliance Manager provides collectors that integrate with Microsoft software to identify:

- ▶ Operating system information
 - Operating system version, service pack and build level
 - Legal notices at sign in and whether the Ctrl+Alt+Delete key combination is required
 - Installed hot fixes
 - The contents and permissions of registry entries
 - Windows services and their status
- ▶ Active Directory information
 - Kerberos configuration settings
 - Active Directory domain trust relationships
- ▶ User and group information
 - User information, including rights and password settings
 - Users whose password are set to never expire
 - Group and group membership information
- ▶ File system information
 - Directories being shared
 - Permissions and audit configuration for file system resources
- ▶ Networking information
 - Directories accessible using anonymous FTP
 - Network configuration (including DHCP client and server)
 - Active network connections and listening ports
- ▶ Audit and policy information
 - Failed login attempts on a system within a time period, obtained from the Microsoft Windows security event log
 - Audit policy
 - Password policy

You can combine the information from these collectors with information from other collectors in a heterogeneous environment to provide the raw system data that is required to evaluate the system configurations against policies that are also defined in Tivoli Security Compliance Manager.

Some collectors have generic capabilities that can collect data for a variety of different purposes. For example, the registry entry collector could collect information about what third-party software products are installed to assist in verifying compliance with an enterprise's standard operating environment (SOE) policy. The Tivoli Security Compliance Manager registry entry collector could also be used to verify advanced TCP/IP parameter configuration on Windows server machines to verify that they have been correctly tuned for optimal performance.

You can find more information about the standard Tivoli Security Compliance Manager collectors in the Collector and Message Reference, which is available at:

http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.itscm.doc_5.1/scm5102_devref.htm

You can also develop custom collectors for Tivoli Security Compliance Manager for more fine-grained or application-specific data collection in a Microsoft software environment. Consult the Collector Development Guide for more information:

http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.itscm.doc_5.1/scm51_devguide.html

3.6 Conclusion

This concludes our discussion about the integration aspects for the Tivoli Security and Microsoft software solution world.

As a reminder, be aware that this paper provides a snapshot in time. However, it provides a very good understanding of where we are today as well as what we can expect in the future.



Redpaper™

IBM Tivoli Security Solutions for Microsoft Software Environments

Explaining common architecture and standards

You can use IBM Tivoli Security products to build open, flexible, and scalable solutions to address business requirements in the areas of:

- ▶ Identity and access management
- ▶ Security information and event management

Deploying on Microsoft operating systems

One of the many strengths of the IBM Tivoli Security offerings is that they are designed and implemented as cross-platform solutions. This design enables broad adoption of the solutions across the range of disparate platforms typically found in an enterprise. IBM Tivoli Security solutions are, therefore, an excellent choice as organizations move further towards service-oriented architecture (SOA) and the security integration challenges present in SOA.

Securing Microsoft software environments

In many enterprises, software solutions from Microsoft are important components of the IT strategy. In this IBM Redpaper publication, we consider the use of IBM Tivoli Security solutions in Microsoft environments from a number of perspectives. In this paper, we discuss:

- ▶ Architectures and standards that are common to IBM Tivoli Security and Microsoft software.
- ▶ IBM Tivoli Security solutions running on Microsoft operating systems utilizing Microsoft middleware.
- ▶ How to secure a Microsoft software environment with IBM Tivoli Security solutions.
- ▶ IBM Tivoli Security solutions providing improved security and security management for Microsoft operating systems, middleware, and applications through integration.

INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION

BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

For more information:
ibm.com/redbooks