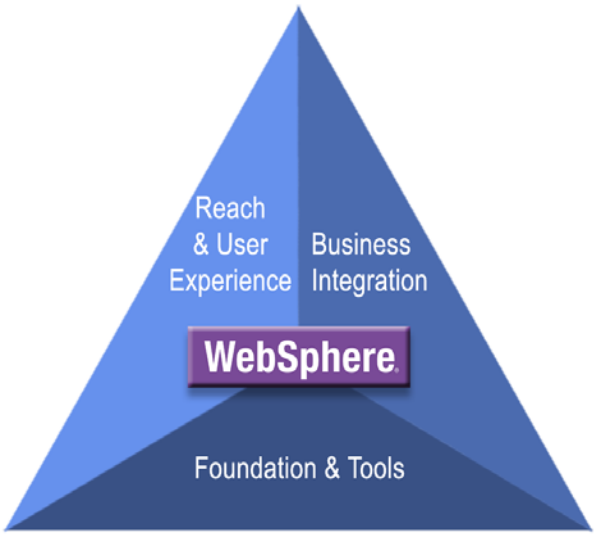
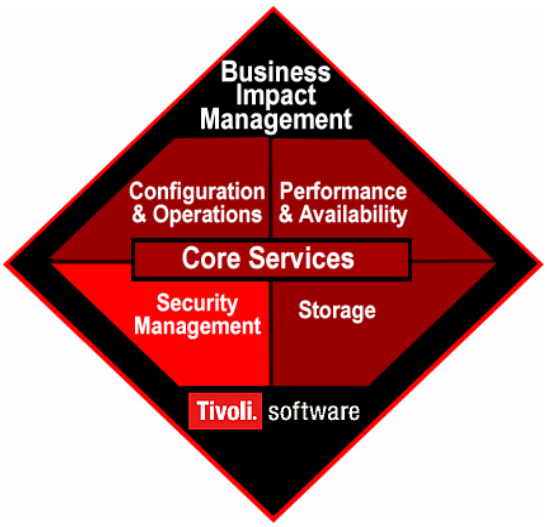
Open Solutions for Secure Business Integration

A Discussion of WebSphere's and Tivoli's Comprehensive Open Security Roadmap





Executive Overview

Though the "dot com" craze has ended, business use of the Web is going strong. Companies want real business benefits, such as increasing customer loyalty, creating and maintaining affinity with partners and suppliers in their value net, creating sustained competitive advantage, and reducing overall risk. Companies want to cost-effectively bridge systems to achieve direct – yet secure - application-to-application communication with partners, suppliers and customers, in a world that consists of heterogeneous environments, with varying approaches to security.

This paper will discuss IBM WebSphere's and Tivoli's open, standards-based approach to addressing secure e-business integration in a heterogeneous IT world, including the details of their unified, comprehensive, open security roadmap.

Open Security Roadmap

To demonstrate IBM's commitment to being #1 in e-business and #1 in security, WebSphere and Tivoli software have developed an open security roadmap for secure business integration. The unified offerings and roadmap discussed in this paper will extend their collective leadership in providing secure e-business infrastructure -- to meet the critical and evolving customer demand for open standards-based business integration.

Highlights of the joint WebSphere and Tivoli Open Security Roadmap are as follows:

- ***IBM is leading the industry in open Web services and Java security infrastructure*** -- from solutions available today to advanced integration and interoperability tomorrow. IBM extends its leadership by driving open standards, ensuring interoperability with competitive solutions, such as Microsoft.NET, and partnering effectively with key industry security players. Advancements, such as Federated Identity Management, which addresses the ability to securely share information about users (identity profiles, authentication data, attribute or other data) between trusted businesses across company boundaries, will bring even greater value to companies in the near future.

- ***IBM is delivering the most comprehensive portfolio for secure, integrated solutions*** -- with the breadth and depth of the WebSphere and Tivoli software portfolios, anchored by WebSphere Application Server Version 5, WebSphere Portal Server 4.1 and Tivoli Access Manager Version 4.1 delivering the unified security model across the WebSphere platform.

In a recent 2002 survey of corporate CIOs published by Merrill Lynch, business integration and security were ranked the top two strategic software priorities. Their interdependencies are becoming more important to companies as the market invests in open, flexible security infrastructures for e-business, designed to exploit the emerging value of open Web services and J2EE standards.

The WebSphere and Tivoli software brands already have a reputation as "trusted partners" with a long heritage of delivering leadership in business integration software and bulletproof security solutions. Now IBM is uniquely positioned, with their partners, to deliver highly modular and flexible, yet comprehensive secure enterprise environments, resulting in quicker company ROI, increased cost savings and peace of mind.

As illustrated in Figure 2 on page 9, the IBM WebSphere and Tivoli Open Security Roadmap is described using a phased approach, with the phases noted below and described in detail in the text to follow.

Phase I: Interoperability and Open Web Services/Java Adoption
Phase II: Advanced Business Integration and Vendor Interoperability
Phase III: Grid and Autonomic Security

Phase I: Interoperability and Open Web Services/Java Adoption

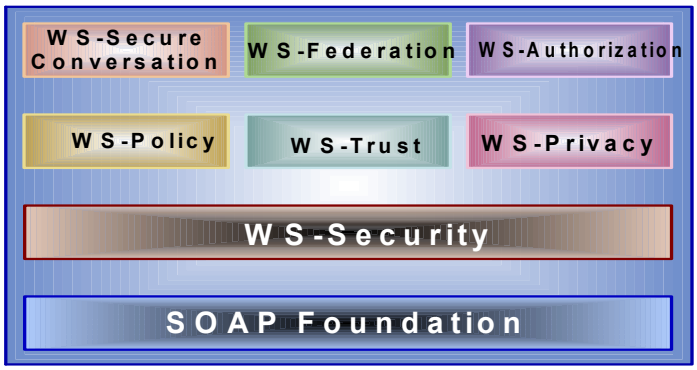
Phase I of the Open Security Roadmap represents WebSphere's and Tivoli's current and upcoming 2002 deliverables and interoperability proof points with vendors, beginning with their collective efforts in the Web Services space.

IBM has publicly demonstrated open Web Services standards leadership through its active participation in the standards organizations. IBM is committed to the advancement of Web Services technology and has led in the Universal Description, Discovery, and Integration (UDDI) project; founded Web Services Interoperability Organization (WS-I.org); chaired XML Protocol and Web Services Coordination Working Groups; co-authored SOAP and WSDL specifications, and contributed to SOAP4J to Apache Open source project, just to name a few.

From a security perspective, IBM is co-author with Microsoft of the Web Services Security Roadmap, and a key contributor and co-author of the April 2002 WS-Security specification with Microsoft and VeriSign. The Web Services Security Roadmap defines

a proposed strategy for addressing security within a Web services environment, including a comprehensive Web Services security model that supports, integrates and unifies several popular security models, mechanisms, and technologies. In addition, the roadmap defines a set of specifications and scenarios that show how these specifications might be used together, as illustrated in Figure 1 below. This security model brings together formerly incompatible security technologies, such as Public Key Infrastructure, Kerberos tokens (strong authentication for client/server applications using secret-key cryptography), and others to enable companies to build secure Web services in a heterogeneous IT world.

Figure 1. Web Services Security Specifications



As the foundation layer for secure Web Services, the WS-Security Specification defines a standard set of Simple Object Access Protocol (SOAP) extensions that can be used to implement integrity and confidentiality in Web Services applications. WS-Security lays the groundwork for higher-level facilities, such as policy, trust and federation that allow companies to establish secure interoperable Web services across trust domains.

Additionally, under the auspices of the OASIS standards body, IBM and a consortium of vendors developed an assertion language that can be carried over WS-Security. Security Assertions Markup Language (SAML) puts user identity and attribute information in "assertions" emitted by the user's origin site. SAML assertions are software tokens and as such could be carried in SOAP messages.

WS-Federation, a specification within the Web Services security roadmap, will provide a simple mechanism to identify and validate users from partner organizations and provide them with seamless access to Web sites within that trusted federation, across differing security authentication technologies and solutions, without requiring re-authentication. In essence, it addresses the need for secure single sign-on (SSO) and attribute assertions across diverse Web access management environments, thus enabling a new generation of e-commerce and e-business scenarios.

In addition to aggressive efforts in the standards area, IBM is also driving company acceptance of Web Services through early implementations, visibility of these emerging technologies, and interoperability demos. IBM AlphaWorks and IBM DeveloperWorks

offer tutorials, demos, and specification information, as well as Web Services toolkits and SDKs.

From a vendor interoperability perspective, WebSphere and Tivoli are taking an active lead here as well. In August 2002, at the XML Web Services One Conference, IBM and Microsoft successfully demonstrated working Web Services security interoperability between the IBM WebSphere platform and Microsoft .NET technologies in the areas of WS-Security and WS-Attachments. And, Tivoli participated in cross-vendor SAML demonstrations sponsored by OASIS, with plans in place for another event in September.

As for product deliveries, WebSphere and Tivoli are also demonstrating Web Services leadership in this area. In 2001, WebSphere Application Server (WAS) Version 4 included support for SOAP Security. In 2002, WebSphere Application Server Version 5 will offer Web Services features that include a UDDI (which is a sophisticated service registry that provides one-stop shopping for information on businesses and electronic services), a Web Services Gateway (which addresses Web Services communication capabilities issues through Service Mapping, Import and Export mapping, Transformation, and UDDI publication and lookup features), and an implementation of the WS-Security specification that includes digital signature support and identity propogation capability. In 2002, Tivoli's Access Manager (TAM) offering will feature new Web Services federated identity management interfaces that enable customers to plug in support for identity standards, including out-of-the box support for the XML Key Management Specification (XKMS).

A key aspect of the WebSphere and Tivoli Open Security Roadmap is the ability to reap the benefits of an open standards-based architecture with a best-of-breed implementation, with plans for further interoperability tomorrow. Specifically, with the deployment of Tivoli Access Manager and WebSphere Application Server, customers *today* can build centralized identity management solutions with single sign-on capabilities and enforceable policies to secure J2EE, Portal, Web and legacy resources, with the ease of working with a single object namespace, representing the full set of security policies for the resources they want to protect. When T. Rowe Price needed to create secure Web-based access with single sign-on across 120 applications for over 1 million users, they chose an integrated WebSphere Application Server and Tivoli Access Manager solution. The result was a secure enterprise environment that greatly simplified administration and enhanced user experiences.

As for the integration aspect, Tivoli Access Manager is integrated and bundled with a number of WebSphere offerings including the Portal Server, Business Integration, Edge Server, and EveryPlace Server. Also, TAM provides container-level integration with WebSphere Application Server today.

From an interoperability perspective with third party vendors, Tivoli and WebSphere have demonstrated success here also. WebSphere Application Server includes facilities to plug in third party authentication solutions through a Trust Association Interceptor (TAI)

Service Provider Interface (SPI) and authorization solutions through an Authorization SPI, with authentication and single sign-on interoperability available today with Tivoli's Access Manager, RSA's ClearTrust and Netegrity's SiteMinder offerings.

Tivoli Access Manager today features integration with a number of ISV solutions including BEA WebLogic Server, Siebel, mySAP.com, Plumtree Corporate Portal, BroadVision One-To-One Enterprise, SAP Enterprise Portal, PeopleSoft, and Epicentric Foundation Server. In addition, Tivoli Access Manager's Cross Domain Authentication Service (CDAS) provides support for interoperability with third party authentication solutions, and implements the Open Group Authorization Service API (aznAPI) for integration with third party access control solutions, with out-of-the-box authentication support for RSA's SecurID Tokens.

Additionally, WebSphere Application Server and Tivoli Access Manager currently provide a robust public key infrastructure (PKI) that include support for certificates through a third party certificate authority. Both offerings can be configured to use certificates from numerous certificate authorities, such as Verisign, Entrust, and Baltimore Technologies, as well as configured to support third party accelerator cards, including nCipher's nForce and nFast and Rainbow's CryptoSwift solutions, for enhanced encryption performance.

As for directory options, WebSphere Application Server and Tivoli Access Manager support LDAP, including IBM Directory, Sun One Directory Server, Lotus Domino and Windows 2000 Active Directory, with added support for Novell eDirectory Server in 2002.

And, to emphasize completeness, IBM not only offers a comprehensive set of interoperable security software offerings, but also offers a wide range of security services. IBM Global Services provides market-leading security services, harnessing the worldwide expertise of 3,000 security consultants, implementation experts, engineers and technology architects, as well as nearly 100 researchers from IBM Research.

Phase II: Advanced Business Integration and Vendor Interoperability

Phase II of the Open Security Roadmap expands on the prior phase through the incorporation of evolving advanced security standards into both the Tivoli and WebSphere offerings.

In addition to an implementation of the WS-Security specification, Tivoli will extend Access Manager's federated identity management interface support delivered in 2002, to include additional advanced federated capabilities in 2003. Web Services Trust Proxy, Trust Broker and Security Token Service, new Tivoli Access Manager components, will offer trust "brokering" with external trust providers, such as Microsoft's Windows-based Trustbridge federation technology, allowing companies to automate the process of entering into trusted business relationships. IBM plans to support the broadest range

of brokering methods, such as Microsoft TrustBridge, Kerberos tokens, Public Key Infrastructure credentials, SAML and other means of delegated trust, that develop in the future.

Additionally, Tivoli Access Manager will implement cross-enterprise, federated identity management that includes validating and asserting cross-enterprise credentials, generating cross-enterprise federated identity tokens, such as Kerberos tokens, SAML, PKI and securely linking or mapping external identities to internal identity definitions. Added capabilities will consist of an Identity and Credential Mapping service, for handling identity translations between companies, and an Identity Profile Service, for managing attribute profiles of users from trusted organization within the federation.

Tivoli also plans to provide fine-grained authorization for SOAP transactions in Web services environments. This new feature will allow businesses to control access to Web services applications based on a user's identity and associated roles and entitlements.

In Phase II, WebSphere will further drive implementations of the open J2EE and Web Services specifications into the WebSphere Family of Offerings, with WebSphere Application Server as the foundation platform. WebSphere Application Server's Service Provider Interface (SPI) infrastructure will be expanded into the development of an open security model. Standards-based, third party pluggability for authentication (including trust interceptors for both HTTP and SOAP channels), authorization through support for the J2EE Authorization Contract for Containers SPI, and identity and credential mapping will be upcoming WAS features. Tivoli Access Manager will leverage these SPIs, as an embedded component of the WebSphere Application Server, that will provide secure access of J2EE resources. This will allow the IBM WebSphere family of offerings, including Portal Server, Business Integration, Commerce, and others, to establish trust associations and thus interoperate with third party vendor offerings, such as those built using Microsoft's TrustBridge technology.

And, in addition to our extended Web Services security capabilities in the WebSphere Application Server foundation offering and in the Tivoli Access Manager product, IBM will enhance the features in the WebSphere Studio Development tools offerings to enable developers to incorporate security in Web Services applications, and IBM will offer Metamerge Integrator for directory integration across LDAP servers including Microsoft Active Directory. With these new features, coupled with IBM's extensive set of security services, IBM plans to deliver the most comprehensive portfolio for secure, Business Integration.

Phase III: Grid and Autonomic Security

Grid and Autonomic Computing will be the next – but not too distant - generation of Web Services, enabling customers to deploy infrastructures *that think*. Intelligent software capabilities, such as self-healing, self-protecting, dynamically allocating (and

re-allocating) of resources - on demand, will become elements of industry-leading offerings.

And, critical to the deployment and success of Autonomic and Grid Computing environments is, again, open standards-based technology. To achieve this, IBM is aggressively driving specifications and participating in standards organizations. IBM is a co-author of the Open Grid Services Architecture (OGSA) Specification, and a co-chair of the Security WorkGroup at the Global Grid Forum (GGF).

By 2004, customers can begin to realize the benefits of secure, standards-based Grid and Autonomic Computing through deployments that enable them to further simplify their system administration, intelligently tap into unlimited access to information, and achieve rapid returns on their investments.

Summary

The IBM WebSphere and Tivoli Open Security Roadmap is more than a vision. The benefits of open, secure business solutions are real *today* with IBM's comprehensive portfolio of e-business and security software and services. And, *tomorrow*, through the implementation phases of this open security roadmap, WebSphere and Tivoli – together with their business partners - will continue to develop and deploy advanced, open, interoperable solutions that will enable companies to easily and securely communicate with partners, suppliers and customers, thus reaping the true financial benefits of business integration.

This document contains information relating to future or anticipated releases of products and represents IBM's current intentions, goals and objectives. The information in this document is subject to change or withdrawal without additional or prior notice. These Products will be available in multiple configurations, and for that reason not all functions discussed in this document are included in all configurations of these Products or will be available upon the initial release of a configuration of these Products

Figure 2: IBM WebSphere and Tivoli Open Security Roadmap