WS-I November Meeting Report: WS Security Specs advance; Deutsche Bank presents Secure WS Application

Alan J Weissberger
Data Communications Technology
aweissberger@sbcglobal.net

I. Summary: At the Nov 2-4, 2004 Miami, FL meeting of the Web Services Interoperability (WS-I) Organization, excellent progress was made on several WS Basic Security Profile specifications, sample applications and test tools. When packaged together, these will be used (by vendors, systems integrators, and users) to provide the underlying security functionality for GGF compliant Grid Computing.

In a Technical Showcase presentation on how member companies are using WS-I deliverables, Deutsche Bank (DB) described a web services application running on their enterprise grid of servers. DB's use cases were later presented to the Sample Apps WG, which will include them in future sample applications demonstrating the WS-I Basic Security Profile. End users from BT, IBM, Ford Motor, Daimler Chrysler, Fidelity Investments also participated at this productive and stimulating WS-I meeting

II. WS-I Backgrounder: The **WS-I Organization** mission is to generate specifications that provide vendors, system integrators, and developers with guidelines for creating interoperable Web Services solutions. Working with standards from W3C and OASIS TC's, the WS-I organization creates three pillars for each of its activities: profiles, sample applications, and test tools. Each of these has its own WS-I Working Group (WG). WS-I has three plenary or "community" meetings per year, with interim meetings scheduled by each WG separately, based on their respective workloads.

More information on WS-I may be obtained from: http://www.ws-i.org/

WS-I has already published **Basic Profiles 1.0 and 1.1, SOAP with Attachments Profile 1.0, and Simple SOAP Binding (with HTTP) Profile 1.0:**

http://www-106.ibm.com/developerworks/views/webservices/standards.jsp

http://www-106.ibm.com/developerworks/webservices/library/ws-basicprofile11.html

http://searchwebservices.techtarget.com/originalContent/0,289142,sid26_gci1002084,00.html

III. WS-I Security Activities – 3 WGs are involved:

The next major work item for WS-I, ongoing for the last 18 months, has been the **Basic Security Profile (BSP).** This work, based on the **OASIS WS-Security standard**, aims to provide a package of a security scenarios document, a basic profile specification, test tools, and sample applications that demonstrate interoperable web services security.

Any company that intends to use web services beyond its firewall- for inter-departmental or inter-company communications will need to ensure that all SOAP messages are secure and not tamper able or decipherable by "the man in the middle." Interoperable WS Security capabilities will be essential for all eBusiness and eCommerce applications, as well as for grid computing.

http://www.eweek.com/article2/0,1759,1658922,00.asp

A. The **WS-I BSP WG** is working on two deliverables:

1] **Security Scenarios document**- includes a Glossary, Security Challenges and Threats, Security Solutions and Mechanisms, Generic Security Requirements and Security Scenario Descriptions. WS-I Board approval is expected this December.

2] **Basic Security Profile 1.0** – profiles the OASIS WS Security standard in order to promote interoperability. It includes user name and X.509 tokens, and references the WS-I BP 1.0, 1.1, and SOAP with Attachments profile. Initial drafts for SAML and REL Token Profiles have been completed, while drafts for Kerberos Token Profile will be done after OASIS Security TC interoperability testing. These Token Profiles may be separate documents, or folded into the Basic Security Profile document at a later date- when all the token profiles have been completed.

There are three sections of the **WS-I Basic Security Profile 1.0 document**:

- Section 1 introduces the Profile, and relates the philosophy that it takes with regard to interoperability.
- Section 2, "Scope of the Profile," delimits the areas where the Profile improves interoperability.
- Section 3, "Profile Conformance," explains what it means to be conformant to the Profile.

→**A new editors draft was produced at this meeting, with WS-I Board approval for the completed document expected in 1Q 2005.**

B. The **WS-I Sample Apps WG** is working on a **Security Architecture** document to guide development of source code for sample applications, which will demonstrate use of the BSP 1.0 as well as the Token Profiles (see description above). Currently, the sample applications are based on a supply chain business scenario.

C. The **WS-I Test Tools WG** is developing a **Test Assertion Document (TAD)** that will be used to test conformance to the BSP 1.0. This document contains the test assertions for the WS-I SOAP Message Security Profile definition. These test assertions are used by the analyzer testing tool to determine if a Web service is conformant to the Basic Security Profile. The Test

WG voted to make the current BSP 1.0 TAD public, inorder to gather further comments. As such, it will soon be available on the WS-I Web site for public review.

Also at this meeting, a new document on **Enhanced Logging for Security** was produced by the Test Tools WG**.** The intent is to test clear text versions (no encryption) of SOAP/XML messages that have had the BSP 1.0 applied. "Reverse security" functions are done prior to logging the messages. These might include functions such as: decrypting relevant portions of SOAP/XML messages, removing XML signature elements, or making reverse transformations to the SOAP/XML messages where WS Security was applied. Procedures for reverse security and crypto key management are out of scope of WS-I and hence not specified in this document.

IV. Deutsche Bank presentation on Use of WS-I Deliverables, by Kieron Drake

DB uses web services for four principal reasons:
1] Enabling secure access for external clients to post trade data
2] Improving automation of trade processing
3] Trade entry (capture) for structured financial products
4] It support the move to a (System Oriented Architecture (SOA)

Web Services enables DB to accept and process complex transactions from customers and internal traders, while protecting their users confidentiality. In essence, trade confirmations are replaced by a web service that provides a signed agreement of the financial transaction or trade (e.g. between a broker dealer and investment bank or between two banks directly).

Web Services helps support the move to SOA, internally within DB. They standardized on **WS-I BP 1.0** and are now moving to **WS-I BP 1.1** (see references above). The WS-I basic profiles are augmented by a secure WS infrastructure, which is based on DB developed "XML firewalls." Those firewalls provide "secure plumbing" and expose "compensating bugs" in WS vendor solutions. The XML firewalls isolates Java and .NET clients from the J2EE and .NET servers that they access. [These servers collectively form an **enterprise compute grid**, which is accessed by the client PC's.] DB noted one problem with a secure WS: it involves heavy use of asynchronous encryption algorithms, which adds a tremendous amount of overhead to messages.

Editors Note: While the XML firewalls provide the secure WS now, DB will standardize on the WS-I BSP when it has been completed. They later presented their WS Security requirements to the Sample Apps WG.

DB uses **WS-I Test Tools** to validate conformance to BP 1.0 Those tools have been particularly valuable with respect to validating WS vendor supplied WSDL (Web Services Description Language). The testing of vendor WSDL's drives an XML schema based, data centric approach to transaction processing at DB.

The trades capture system now being implemented by DB is faster and cheaper than the previous system, while permitting them to reuse existing servers. DB clients may access their post trade data over a secure environment that protects their confidentiality requirements.

Postscript: This editor suggested to the WS-I President and several board members that profiling of selected WS Security related specifications (that have not yet been submitted to a standards committee) might be a very useful work item. These specifications include: WS Federation, WS-Trust, and WS-Secure Conversation. WS-Policy would also be involved. It remains to be seen if the WS-I Board of Directors will consider this suggestion.

Appendix: WS-I Deliverables

WS-I Deliverables consists of Profiles, Sample Applications, and Testing Tools

WS-I's deliverables provide resources for Web services developers to create interoperable Web services and verify that their results are compliant with WS-I guidelines. **Key WS-I deliverables include Profiles, Sample Applications and Testing Tools, based on Web Services standards (from W3C and/or OASIS TCs)**

Profiles provide implementation guidelines for how related Web services specifications should be used together for best interoperability. To date, WS-I has finalized the Basic Profile, Attachments Profile and Simple SOAP Binding Profile. Work on a Basic Security Profile is currently underway.

Sample Applications demonstrate Web services applications that are compliant with WS-I guidelines. These implementations are developed using multiple platforms, languages and programming tools, demonstrating interoperability in action, and providing readily usable resources for the Web services developer. Sample applications serve as working examples for developers looking to follow the WS-I guidelines in their programming environment of choice. To date, WS-I has delivered eleven implementations of the WS-I Sample Application for the Basic Profile.

Testing Tools are used to determine whether the messages exchanged with a Web service conform to WS-I guidelines. These tools monitor the messages and analyze the resulting log to identify any known interoperability issues. These testing capabilities are important for developers to ensure that their implementations comply with the current interoperability guidelines for the use of Web services specifications. Tests are self administered and aimed at uncovering unconventional usage or errors in specification implementations, thus improving interoperability between applications and across platforms. To date, WS-I has developed tests for developers to verify their conformance with the Basic Profile 1.0, and work on the other WS-I profiles is underway.

IBM-Microsoft WS Security Roadmap

Current/proposed specs
Building on the SOAP Foundation

WS-Secure Conversation	WS-Federation	WS-Authorization
WS-Policy	WS-Trust	WS-Privacy

WS-Security

SOAP Foundation

This is a composable Architecture

"only use what you need"

today

time