

Power Players Advance Web Services Security Standardization

Daniel Sholler, Charles Abrams, Ray Wagner

The commitment of key technology providers shows that Web services security standardization is rapidly coming of age. Prepare to implement upcoming standards, because real-world products using them are in development now.

NEWS ANALYSIS

Event

On 13 July 2005, IBM, Microsoft and a group of other technology providers — including Actional, BEA Systems, BMC Software's OpenNetwork Technologies, Computer Associates, Layer 7 Technology, Oracle, Ping Identity, Reactivity, RSA Security and VeriSign — announced that they plan to place three key Web services security specifications under the control of the Organization for the Advancement of Structured Information Standards (OASIS). The three specifications, which are all based on the core WS-Security specification, are:

- **WS-Trust** (which defines extensions for requesting security tokens and brokering trust relationships)
- **WS-SecureConversation** (which defines mechanisms for securing multiple messages)
- **WS-SecurityPolicy** (which defines security policy assertions for WS-Security, WS-Trust and WS-SecureConversation)

Analysis

The decision to place these three key Web services specifications under OASIS control reflects the growing maturity of Web services security standards. Most of the basic building blocks for secure Web services with a mechanism to represent trust relationship are now in place. The publication of these specifications as OASIS standards should help to advance interoperability, though further work — perhaps in the form of enhancements to the Web Services Interoperability (WS-I) Basic Security Profile — will likely be required to help enterprises make their deployments as compatible as possible.

This is a generally positive development, but some elements are missing from the announcement. One is that WS-Federation is not included. Another is that the basic security policy language will likely require extensions, which will be implemented in both proprietary and future standard versions. Still another concern is that there appear to be no new players involved. The vendors seem to be the same as in earlier versions of the specifications. Interested parties should, however, be able to comment on, and influence, future OASIS standards. Gartner believes the WS-I should begin adding best practices for these standards to the Basic Security Profile immediately.

Recommendations for enterprises:

- Expect the ratification and implementation of these specifications to move rapidly. The forthcoming standards will likely begin to appear in implementations by Web services security vendors by the end of 2005 and will be ubiquitous the end of 2006.
- Add WS-Security as a mechanism and upgrade infrastructure to support it. Demand that new products include WS-Security capabilities, as well as the WS-I Basic Profile and Basic Security Profile.

Analytical Sources: Dan Sholler, Charles Abrams and Ray Wagner, Gartner Research

Recommended Reading and Related Research

- "Making Sense of Web Services Security Standards" — Deal with the complexity of Web services security decisions by beginning with simple deployments. **By Ray Wagner**

- "WS-Security Provides Business Benefits Through Persistence" — Advanced Web services security mechanisms reduce enterprise risk by applying controls to transactions. **By Ray Wagner and Jay Heiser**

(You may need to sign in or be a Gartner client to access the documents referenced in this First Take.)

REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Level 7, 40 Miller Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Latin America Headquarters
Av. das Nações Unidas 12.551
9 andar—WTC
04578-903 São Paulo SP
BRAZIL
+55 11 3443 1509