

SAML Approval Brings Secure Web Services a Step Closer

Ray Wagner, John Pescatore

The standards body OASIS approved Security Assertion Markup Language (SAML). Its widespread use will aid the creation of secure, interoperable Web services, but remaining challenges will require significant investments.

NEWS ANALYSIS

Event

On 6 November 2002, the Organization for the Advancement of Structured Information Standards (OASIS) announced that it has approved SAML, an XML security standard. SAML enables cross-domain authentication and authorization and single sign-on, and forms the technical basis for the Liberty Alliance federated identity initiative.

Analysis

The newly approved SAML standard will play a central role in Web services deployments because it supports complex workflow and new business models. In addition, SAML can encapsulate complex information for the multiple domains that characterize emerging Web services models. Most Web services vendors have announced plans to support SAML in the near future, and this widespread acceptance will simplify security integration across heterogeneous Web services environments.

Although Gartner forecasts rapid adoption of SAML, enterprises implementing Web services will still face serious security challenges, particularly in managing the public and private keys required to implement signing and encryption. SAML and the other leading Web services security initiatives — the proposed OASIS Web Services Security (WS-Security) specification and the World Wide Web Consortium's (W3C's) XML Digital Signature and XML Encryption specifications (the foundation for both WS-Security and SAML) — all assume that keys or digital certificates and the infrastructure to manage them are readily available. This is not yet the case for most enterprises, however.

The XML Key Management Specification (XKMS) does offer a simplified approach to integrating public key management capabilities with applications. However, enterprises and vendors must still create the infrastructure for effective long-term management of keys and certificates within the enterprise. The failure of public-key infrastructure to achieve significant market penetration means that enterprises typically lack the capacity to effectively use Web services platforms that apply the new standards. Enterprises should plan to make investments in the necessary base infrastructure and should demand that vendors' Web services offerings support XKMS public-key management capabilities as well as SAML, XML encryption and signing, and WS-Security (when approved).

Analytical Sources: Ray Wagner and John Pescatore, Gartner Research

Written by Terry Allan Hicks, Gartner News

Recommended Reading and Related Research

- "New W3C Standards for XML Will Enhance Web Service Security" — New encryption standards will enable improved security in complex Web services implementations. **By Ray Wagner and John Pescatore**
- "WS-Security Takes Good Step Toward Being Web Service Standard" — OASIS oversight of WS-Security will speed industry acceptance of this key specification. **By Ray Wagner**

(You may need to sign in or be a Gartner client to access all of this content.)

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