SAMLNeedsMoreThanOASISApproval

RayWagner,CharlesAbrams,JohnPescatore,DavidMitchellSmith

SecurityAssertionMarkupLanguage(SAML)isnowanacceptedindustrystandard. But it will need broad vendor support to deliver real-world business value.
NEWS ANALYSIS

Event

On 14 March 2005, the Organization for the Advancement of Structured Information Standards (OASIS) announced that it has approved version 2.0 of SAML as an OASIS standard.

Analysis

OASIS approval is a positive step, but much more must be done before SAML can be considered anything more than just another security token format and yet another set of protocols. SAML has been in existence since 2001, and many vendors support it, but very few real-world production applications rely on it.

SAML offers enterprises the promise of multivendor interoperability for authentication, authorization and access control products. Real-world business environments need ways to allow a customer to log in at one commerce site and have that customer's authentication and authorization attributes passed on to business partners, without requiring the customer to log in multiple times. This can potentially benefit business by reducing the costs of identity management systems, and by limiting customer abandonment of electronic commerce due to complexity issues.

However, for this promise to be realized, all major vendors must support both SAML token formats and SAML protocols organically within their products. This certainly is not yet the case for most of the leading vendors, and not even the vendors that have developed SAML use it within the federation features of their own products. If those vendors did so, major platform vendors would have a much stronger incentive to focus on full SAML support.

Recommendations for enterprises: Require integrated SAML version 2.0 support in all identity and access management system procurements. Allow gateway/translator-type approaches as temporary measures, to be replaced no later than the end of 2006.

Analytical Sources: Ray Wagner, Charles Abrams, John Pescatore and David Mitchell Smith, Gartner Research

Recommended Reading and Related Research

- "Making Sense of Web Services Security Standards" — Enterprises should implement only those Web services standards that address their near-term needs. By Ray Wagner
- "Web Services Security Advances With Approval of Key Standard" — The formal adoption of a widely accepted standard marked a significant step forward for Web services security. By Ray Wagner

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