

Southwest Airlines Shows SAML's Promise

Ray Wagner, Roberta J. Witty

Southwest Airlines' decision to use Security Assertion Markup Language (SAML) to authenticate communications with external business partners is a sign of things to come.

NEWS ANALYSIS

Event

On 12 August 2003, Oblix, which develops identity-based security solutions, announced that Southwest Airlines has completed a large-scale implementation of the Oblix NetPoint identity management and access control product. The NetPoint implementation uses single sign-on based on the SAML standard to secure communications within Southwest's internal networks and with its suppliers and other external business partners.

Analysis

Southwest is one of the first to use SAML-enabled identity management on a large scale to perform cross-domain trust. This implementation also marks an early step in the movement toward federated identity management. However, this approach appears to deliver many of the real-world benefits of federated identity management without the use of additional technologies or standards, such as Liberty and WS-Federation.

The Oblix system enables Southwest to vouch for the identity of an employee who accesses external partners' networks (for example, an aircraft mechanic looking for technical documentation). The partner grants session access to the Southwest employee without performing authentication on its own site. With this approach, Southwest enjoys enhanced employee productivity, and the external partner does not need to manage credentials for large numbers of outside users.

According to some estimates, identity management solutions deliver an average three-year return on investment of as much as 300 percent. The use of standards such as SAML may drive up return on investment still further by offering cost savings for security administration, help desk support and application development. Through 2005, 80 percent of federated identity projects will be simple cross-domain trust initiatives between two enterprises with established partnerships (0.8 probability). SAML will be the leading standard for business-to-business single sign-on through 2006 (0.8 probability).

Bottom Line: Enterprises that manage large numbers of external identities should consider SAML-based cross-domain trust.

Analytical Sources: Ray Wagner and Roberta Witty, Gartner Research

Written by Terry Allan Hicks, Gartner News

Recommended Reading and Related Research

- "ROI Drives Identity and Access Management Implementation" — Identity and access management systems show great promise for enterprises that need to control account and access rights. **By Roberta J. Witty**
- "Banks Largely Disinterested in Passport and Liberty" — A Gartner survey shows virtually no bank interest in the leading identity services. **By Avivah Litan and John Pescatore**

(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

Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters

Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters

Gartner do Brazil
Av. das Nações Unidas, 12551
9º andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509