A Standard for Identity Management

Kai Lun Li

Software Design
Professor Brian Mitchell
November 8, 2006
Digital identity is a crucial element in the growth of sensitive data and confidential relationships online. All users create digital identities as they use the internet. At the same time, every organization creates identities to provide individuals with secure access to online resources and services. Unfortunately, there are more than one standard for communicating user authentication, entitlement, and attribute information to other entities, such as a partner company or another enterprise application. Single sign-on solutions are desirable to reduce the number of usernames and passwords that each user has to manage. Managing multiple accounts and multiple sites can be burdensome to the user and can lead to security exposure. SAML (Security Assertion Markup Language), is an OASIS (Organization for the Advancement of Structured Information Standards) standard combined with the previous efforts of Liberty Alliance; and WS-Federation, an effort by IBM, Microsoft Corp, and VeriSign, are emerging technologies for use in the allowing credential to be passed across systems and company boundaries. These protocols are open standards that can be used for creating solutions for credential passing in a distributed environment of multiple service providers.

SAML is developed by standard bodies and is much further ahead in the standards race. It has been used to implement Single Sign On and for Federating Identities. The line between it and WS-Federation has become very fuzzy. Even in the early stages of development of the two standards there where overlapping of the two. There has been talk about the possibility of a convergence. For now SAML continues to be more and more widely used and adopted.

The WS-Federation specification is designed to standardize the way companies share user and identities among disparate authentication and authorization systems spread
across corporate boundaries. Microsoft has announced they intend to stick by their WS-Federation protocol because SAML lacks messaging and transaction support. This is true, but according to Dr. John Gøtze, a Danish e-government consultant and OASIS Information Technology contractor, “neither does WS-Federation.” (http://www.xmlgrrl.com)

Microsoft, more often than not, tend to package their technology in with their new products. “Microsoft will soon start shipping a whole lot of servers that use WS-Federation protocols” (http://www.infoworld.com/article/05/11/17/HNmssaml2support_1.html). But there is no reason for SAML to step down to this especially when there are products from well know organization such as Oracle and Ping Identity that announced their Identity Management products support both specifications[4,5].

SAML’s various versions have been actively worked on and have had public interoperability testing done at regular intervals. SAML had been in existence since 2001 and many vendors supported it. In October of 2002 SAML 1.0 was ratified as an OASIS open standard. Then in early July of 2003 IBM, Microsoft Corp and VeriSign Inc. released the WS-Federation. However, since that time the two standards have evolved at a much different pace. Less than three years later a global consortium of vendors and end users started testing tools that incorporate SAML 2.0 in July of 2005. This rigorous testing program requires all participants to successfully demonstrate compliance with the SAML 2.0 standards through a number of interoperability tests with other compliant products. The new version unifies single sign-on capability of version 1.0 with the identity federation framework developed by Liberty Alliance in SAML 1.1. Having been developed and tested over five years SAML is the more mature and industry-proven standard.
SAML represents a convergence of efforts going on in the OASIS, Liberty Alliance, and Shibboleth communities. OASIS is a nonprofit, global consortium that drives the development, convergence and adoption of e-business standards, and the Liberty Alliance Project is an alliance of more then 150 not-for-profit and government organizations committed to developing an open standard for federated network identity[1]. Liberty Alliance donated the identity federation framework (ID-FF) standards to OASIS. It defines how data must be exchanged between identity providers and service providers [2]. In addition, many of the authors of the Liberty Alliance specifications began to participate in the OASIS security services technical committee.

WS-Federation came about in an entirely differently manner. It was developed in private. “IBM and Microsoft believe it is more efficient to develop specifications in a closed process, and then turn it over to standards body for its blessing. This has resulted in overlapping industry efforts.” (Joe Keller, vice president of marketing for Java Web services at Sun Microsystems http://www.leavcom.com)

Some organizations have made some progress in deploying single sign-on solutions within the confines of their own set of systems. These solutions are desirable to reduce the number of usernames and passwords that each user has to manage. Other benefits include consolidated account management and reduced system administration
overhead and response time in adding users or modifying access privileges. Both, SAML and WS-Federation purport to offer cross-domain single sign-on, single logout, and pseudonym-based identity federation. However, the amount of information on WS-Federation tends to be a little thin. Most companies see WS-Federation as more of a simple proprietary protocol while organizations have opted for SAML when implementing single sign-on as the standardized way of expressing authentication assertion in an XML format.

OASIS creates interoperable industry specifications based on public standards and the Liberty Alliance is committed to developing an open standard for federated network identity that supports all current and emerging network devices. The Liberty Alliance and OASIS standards body have been working together more closely to align their respective specifications[2], where as the WS-Federation authors have chosen to continue on their divergent path for the time being. SAML and WS-Federation are both built upon WS-* specifications. It is to no surprise that Microsoft and its consortium of 170 companies have not seen eye-to-eye. The consortium believe that there is room for WS-Federation and SAML to come together[3]. “Convergence is clearly best for everyone.” (Britta Glade, vice char of the Liberty Alliance Business and Marketing Expert group. internetnews.com)

SAML is out in front in the race to standardize the way to express authentication assertion in an XML format. Its time in existence and the amount of progress OASIS and Liberty Alliance has made is significantly more than what Microsoft and IBM has done for WS-Federation. SAML has been tested at regular interval where as WS-Federation has been developed much differently, in private. The two major bodies that developed SAML have dedicated themselves to develop an open standard for federated network
identity. It should not be surprising that the bodies that develop standards are the ones who set standards.

It is difficult to dismiss the likelihood of a convergence of the two standards. Even in the early stages of development of SAML at Liberty Alliance and WS-Federation beginning drafts there have been overlapping characteristics. Although convergence is a much welcomed possibility, having two standards is better than 10 standards.
REFERENCES


ACKNOWLEDGEMENT

OASIS contacts:
Hal Lockhart, hlockhar@bea.com, Chair
Eve Maler, eve.maler@sun.com, Secretary