MedBiquitous
Single Sign On Guidelines

Version 1

6 August 2004
MedBiquitous Technical Steering Committee

Revision History

Date	Version	Description	Author
6 Aug 2004	1	Initial version	Joel Farrell joelf@us.ibm.com Peter Greene peter.greene@medbiq.org

MedBiquitous Consortium XML Public License and Terms of Use

MedBiquitous XML (including schemas, specifications, sample documents, Web services description files, and related items) is provided by the copyright holders under the following license. By obtaining, using, and or copying this work, you (the licensee) agree that you have read, understood, and will comply with the following terms and conditions.

The Consortium hereby grants a perpetual, non-exclusive, non-transferable, license to copy, use, display, perform, modify, make derivative works of, and develop the MedBiquitous XML for any use and without any fee or royalty, provided that you include the following on ALL copies of the MedBiquitous XML or portions thereof, including modifications, that you make.

1. Any pre-existing intellectual property disclaimers, notices, or terms and conditions. If none exist, the following notice should be used: "Copyright © [date of XML release] MedBiquitous Consortium. All Rights Reserved. http://www.medbiq.org"
2. Notice of any changes or modification to the MedBiquitous XML files.
3. Notice that any user is bound by the terms of this license and reference to the full text of this license in a location viewable to users of the redistributed or derivative work.

In the event that the licensee modifies any part of the MedBiquitous XML, it will not then represent to the public, through any act or omission, that the resulting modification is an official specification of the MedBiquitous Consortium unless and until such modification is officially adopted.

THE CONSORTIUM MAKES NO WARRANTIES OR REPRESENTATIONS, EXPRESS OR IMPLIED, WITH RESPECT TO ANY COMPUTER CODE, INCLUDING SCHEMAS, SPECIFICATIONS, SAMPLE DOCUMENTS, WEB SERVICES DESCRIPTION FILES, AND RELATED ITEMS. WITHOUT LIMITING THE FOREGOING, THE CONSORTIUM DISCLAIMS ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY, EXPRESS OR IMPLIED, AGAINST INFRINGEMENT BY THE MEDBIQUITOUS XML OF ANY THIRD PARTY PATENTS, TRADEMARKS, COPYRIGHTS OR OTHER RIGHTS. THE LICENSEE AGREES THAT ALL COMPUTER CODES OR RELATED ITEMS PROVIDED SHALL BE ACCEPTED BY LICENSEE "AS IS". THUS, THE ENTIRE RISK OF NON-PERFORMANCE OF THE MEDBIQUITOUS XML RESTS WITH THE LICENSEE WHO SHALL BEAR ALL COSTS OF ANY SERVICE, REPAIR OR CORRECTION.

IN NO EVENT SHALL THE CONSORTIUM OR ITS MEMBERS BE LIABLE TO THE LICENSEE OR ANY OTHER USER FOR DAMAGES OF ANY NATURE, INCLUDING, WITHOUT LIMITATION, ANY GENERAL, DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, OR SPECIAL DAMAGES, INCLUDING LOST PROFITS, ARISING OUT OF ANY USE OF MEDBIQUITOUS XML.

LICENSEE SHALL INDEMNIFY THE CONSORTIUM AND EACH OF ITS MEMBERS FROM ANY LOSS, CLAIM, DAMAGE OR LIABILITY (INCLUDING, WITHOUT LIMITATION, PAYMENT OF ATTORNEYS' FEES AND COURT COSTS) ARISING OUT OF MODIFICATION OR USE OF THE MEDBIQUITOUS XML OR ANY RELATED CONTENT OR MATERIAL BY LICENSEE.

LICENSEE SHALL NOT OBTAIN OR ATTEMPT TO OBTAIN ANY PATENTS, COPYRIGHTS OR OTHER PROPRIETARY RIGHTS WITH RESPECT TO THE MEDBIQUITOUS XML.

THIS LICENSE SHALL TERMINATE AUTOMATICALLY IF LICENSEE VIOLATES ANY OF ITS TERMS AND CONDITIONS.

Table of Contents

Single Sign On Guidelines

1. Acknowledgements

These guidelines are based on a submission from Joel Farrell of IBM. Scott Hinkelman of IBM, Darin McBeath of Elsevier, Dan Rehak of Carnegie Mellon University, and Peter Greene and Valerie Smothers of MedBiquitous also contributed to this document.

2. Introduction

As Web applications increasingly require integration with a variety of distributed Web resources, the need for a robust approach to managing the identity of users across organizational boundaries has emerged. The issue of single sign on (SSO) is particularly important for enabling these applications, and MedBiquitous members have expressed an interest in developing a common approach to this problem. For example, when a clinician moves from a professional association Web site to the association's journal web site, there is often a need to log in with a different user ID and password. For readers, this is at least a nuisance and potentially a barrier to important information.

In order to articulate the need for SSO, the MedBiquitous Journal Working Group (JWG) developed a set of use cases and business requirements. These were provided as input to the MedBiquitous Technical Steering Committee (TSC), which is also working on common approaches to security for web services. The TSC has identified the Security Assertions Markup Language (SAML) as being a useful building-block technology for addressing a number of security requirements, including SSO. Outlined in this document are high-level guidelines for MedBiquitous members and other interested parties on how to use SAML to implement SSO.

2.1 Key Definitions

A common understanding of certain security-related terms is essential. **Identification** refers to the process of determining who someone (a user or computer, often called a **subject**) actually is. **Authentication** refers to the process of an individual proving that he or she is someone who has already had their identity established. Typically authentication involves something that the user *knows* (a password or PIN), *has* (a token or key), or *is* (a biometric). **Authorization** is the process of establishing what an authenticated subject is allowed to do or access. An **attribute** identifies certain properties of a subject. **Assertions** are statement about the authentication status (authentication assertion) or authorization status (authorization assertion) or attributes (attribute assertion) of a particular subject, and SAML provides a way of expressing these assertions in XML documents. **Single sign-on** (SSO) allows a user to log in once with a recognized security authority and use the returned login credentials to access multiple resources.

3. What SAML Is and Is Not

SAML is an XML-based framework for exchanging security information. It is unlike other approaches to security because it expresses security information in the form of assertions about subjects. In the realm of authentication, this involves assertions about prior acts of authentication.

It is important to understand that SAML is not an entire approach to identity management, which involves a collection of services for provisioning of new user identities, password management, and access control. SAML is useful when two servers need to share authentication information, but it does not include the actual authentication service, which is typically provided by an LDAP or other directory server product. This aspect of SAML makes it particularly useful for inter-organizational communication and has enabled SAML to be a useful building block inside a number important security standards (such as WS-Security) and efforts (Liberty and Shibboleth).

SAML's emphasis on assertions also makes it different from other cross-industry approaches to security in which there is a central certificate authority that issues and guarantees certificates that multiple participants recognize. SAML can use such certificates and convey information about them within assertions, but they are not required. With SAML, any entity within a network can assert that it knows the identity, entitlements, or data about a user, and it is up to the receiving application to decide whether it trusts this assertion.

4. Industry Traction

SAML has been developed within the OASIS Security Services Technical Committee. The committee has been actively working on SAML since January of 2001, with active participation by most leading vendors of security products. Their work merged two earlier standards efforts, Security Services Markup Language (S2ML) and AuthXML. SSO was one of the earliest SAML requirements. Version 1.0 was ratified by OASIS in November of 2002, and version 1.1 was ratified in September of 2003. Version 2.0 is at a last-call working draft stage.

Many commercial and open source products are available to simplify the process of implementing SAML. These include:

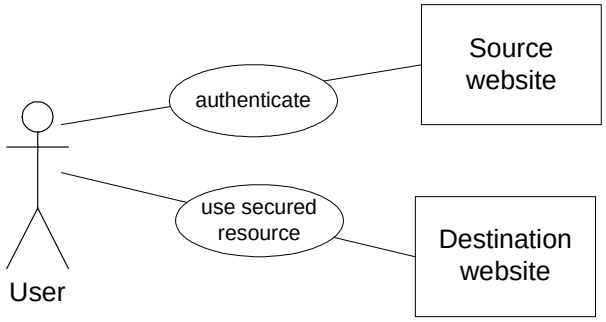
- Baltimore SelectAccess
- Entrust GetAccess
- IBM Tivoli Access Manager
- Internet2 OpenSAML
- Netegrity SiteMinder
- Oblix Netpoint
- Ping Networks SourceID
- RSA Security ClearTrust
- SunONE Identity Server
- VeriSign Trust Integration Toolkit

When selecting a product, implementers should consider asking about which specific SAML bindings and protocols are supported for SAML messages and whether an application acts as a producer, consumer, or both. Details and test suites are provided in the SAML Conformance Program Specification provided by OASIS. In regard to SSO requirements, verify that the Browser/Artifact and Browser/Post capabilities are supported, since both may be important for browser-based SSO implementations. The test suites also enable the testing of custom software tools if implementers choose to develop their own software tools.

5. Recommendations

The MedBiquitous Technical Steering Committee has conducted significant research into Single Sign On solutions and has conferred with a number of industry experts to develop a pragmatic approach for a particular vertical industry. Based this research, the committee recommends that MedBiquitous members use the OASIS Security Assertion Markup Language (SAML) version 1.1 to achieve SSO for projects that are being implemented in 2004 or Q1 of 2005. The committee will track the early experience of version 2.0 once it is ratified by OASIS and may change this version recommendation early in 2005.

More specifically, implementers of SSO should use the SAML 1.1 Web Browser Single Sign On Profile. This Profile describes two main scenarios for how SAML can be implemented, “pull” and “push” scenarios. Both scenarios allow a user to authenticate with one website (a Source website), and then have that Source website send authentication assertions to a second website (a Destination website).



In the "pull" scenario, SAML artifacts are passed between sites by the web browser as a part of an HTTP Get request in the URL query string, and the subsequent assertions about the user are "pulled" by the Destination website from the Source site.

In the "push" scenario, an HTML form is used on the Source website to include SAML assertions in a hidden field, and these assertions are "pushed" to the Destination website as a part of an HTTP Post.

The TSC believes that both of these scenarios within the Web Browser SSO Profile may be important to implementers within MedBiquitous, although some implementations may use only one of these approaches. To secure these web-based communications, the committee recommends using Secure Sockets Layer (SSL) 3.0.

5.1 Other Uses of SAML

The MedBiquitous TSC also recommends that SAML be used to specify binary security tokens within Web services. When used in this capacity, the SAML identification token should be carried within the Web Services Security header as defined by the OASIS Web Services Security standard and the OASIS WS-Security SAML Token Profile.

Beyond this recommendation, the MedBiquitous TSC has not yet recommended a general SSO approach for Web services. WS-Federation and the Liberty project, as well as other approaches, are both being tracked carefully.

As MedBiquitous members begin to implement SAML, there may arise a need to make Attribute and Authorization Assertions. SAML has the capacity to enable transmission of vertical industry-specific attributes, and MedBiquitous will likely need to work with its members to define these requirements for more complex security assertions that can be generally recognized throughout the healthcare education industry.