SAML Conformance Clause

This version:

File: SAMLConformance Clause-006.doc
Date: June 15, 2001

Authors

- Krishna Sankar [ksankar@cisco.com]
- Robert Griffin [Robert.Griffin@entrust.com]
- Lynne Rosenthal [lynne.rosenthal@nist.gov]
- Eve Maler [eve.maler@east.sun.com]
- Tony Palmer
- Mark Skall

Contributors

Abstract

This document describes the conformance clause for the SAML specification. The conformance clause is intended for inclusion within the SAML specification, rather than being maintained as a separate document.

Referenced Documents


3. XML Protocol specification conformance issues

### Notational Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in Key Words for Use in RFC’s to Indicate Requirement Levels (RFC 2119).

### Status of this Document

This document represents work in progress upon which no reliance should be made.

### Document Version History

- Version 0.001: Initial version
- Version 0.002: First Review draft to conformance subgroup 21-May-2001
- Version 0.003: Internal Editor’s version
- Version 0.004: Second review draft to SAML TC 11-June-2001
- Version 0.005: Third review draft to conformance subgroup 14-June-2001
- Version 0.006: Review draft For SAML f2f #3
# Table of Contents

1 Conformance Clause
   1.1 Introduction
      1.1.1 Conformance Nomenclature
      1.1.2 Mandatory/Optional
      1.1.3 Extensions
      1.1.4 Alternate approaches
   1.2 Authorities
   1.3 Roles
   1.4 Bindings
   1.5 SAML Conformance Program

2 Things To Do
1 Conformance Clause

1.1 Introduction

The objectives of the SAML Conformance Clause are to:

a) Ensure a common understanding of conformance and what is required to claim conformance;

b) Promote interoperability for the exchange of authentication and authorization information

c) Promote uniformity in the development of conformance tests.

The conformance clause specifies explicitly all the requirements that have to be satisfied to claim conformance to the SAML Specification. These requirements can be applied at varying levels, so that a given implementation or application of the SAML Specification can achieve clearly-defined conformance with all or part of the entire set of requirements.

SAML conformance provides for both validation and certification. Validation may be done without certification, especially for such purposes as self-test. An implementer who has validated SAML conformance by means of self-test cannot legitimately use the term “certified for SAML conformance”. However, validation may be all that is required for the particular purposes for which an implementer is using SAML.

Certification may require validation by a third-party or through self-test or by some automatic means e.g. by running thru a server in a lab, as determined by the certification authority.

The SAML conformance is expressed by three orthogonal dimensions.

- The first dimension is a partition, (a.k.a. profile) which is a subset of the overall specifications that includes all of the functionality necessary to satisfy the requirements of a particular community of users. The authorities for SAML are authentication authority, authorization authority, attribute authority, session authority, Policy decision authority and policy enforcement authority.

- The second dimension is the role of a system – consumer, producer or producer-consumer.
The third dimension is the mapping of the assertions to a binding viz http, xmlp, soap, ebXML et al.

1.1.1 Conformance Nomenclature

The nomenclature for expressing SAML conformance would be two SAML conformance matrices as follows:

1. Partition-Role Table:

<table>
<thead>
<tr>
<th>Partition</th>
<th>Consumer</th>
<th>Producer</th>
<th>Producer/Consumer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication authority</td>
<td>y</td>
<td>Y</td>
<td>y</td>
</tr>
<tr>
<td>Authorization authority</td>
<td>y</td>
<td>Y</td>
<td>y</td>
</tr>
<tr>
<td>Attribute authority</td>
<td>y</td>
<td>Y</td>
<td>y</td>
</tr>
<tr>
<td>Session authority</td>
<td>y</td>
<td>Y</td>
<td>y</td>
</tr>
<tr>
<td>Policy decision authority</td>
<td>y</td>
<td>Y</td>
<td>y</td>
</tr>
<tr>
<td>Policy enforcement authority</td>
<td>y</td>
<td>Y</td>
<td>y</td>
</tr>
</tbody>
</table>

2. Partition-Bindings Table:

<table>
<thead>
<tr>
<th>Partition</th>
<th>http</th>
<th>xmlp</th>
<th>SOAP</th>
<th>BEEP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication authority</td>
<td>y</td>
<td>y</td>
<td>y</td>
<td>Y</td>
</tr>
<tr>
<td>Authorization authority</td>
<td>y</td>
<td>y</td>
<td>y</td>
<td>Y</td>
</tr>
<tr>
<td>Attribute authority</td>
<td>y</td>
<td>y</td>
<td>y</td>
<td>Y</td>
</tr>
<tr>
<td>Session authority</td>
<td>y</td>
<td>y</td>
<td>y</td>
<td>Y</td>
</tr>
<tr>
<td>Policy decision authority</td>
<td>y</td>
<td>y</td>
<td>y</td>
<td>Y</td>
</tr>
<tr>
<td>Policy enforcement authority</td>
<td>y</td>
<td>y</td>
<td>y</td>
<td>Y</td>
</tr>
</tbody>
</table>

1.1.2 Mandatory/Optional:

A system can choose to implement any or all of the partitions as per table 1, as a producer of SAML assertions, a consumer of SAML assertions or both. For each partition, role, binding combination (i.e., cell in the table) all functionality is mandatory. i.e. the system should support all SAML assertions related to that partition. It is optional as to which partition, role, binding combinations are supported (implemented).

In short, as an example, if a system describes itself as conforming to a SAML Authorization authority, producer-consumer over http and SOAP, it has to consume and produce *all* SAML authentication assertions and be able to support the http and SOAP bindings described in the SAML specifications.
1.1.3 Extensions:

- Extensions shall not re-define semantics for existing functions.
- Extensions shall not alter the specified behavior of interfaces defined in this standard.
- Extensions may add additional behaviors.
- Extensions shall not cause standard-conforming functions (i.e., functions that do not use the extensions) to execute incorrectly.

SAML assertions can be extended so long as the above conditions are met. It is requested that, if a system is extending the SAML assertions,

- The mechanism for determining application conformance and the extensions shall be clearly described in the documentation, and the extensions shall be marked as such;
- Extensions shall follow the spirit, principles and guidelines of the SAML specification, that is, the specifications must be extended in a standard manner as defined in the extension fields.
- In the case where an implementation has added additional behaviors, the implementation shall provide a mechanism whereby a conforming application shall be recognized as such, and be executed in an environment that supports the functional behavior defined in this standard.

Note: Extensions are outside the scope of conformance. There are no mechanisms specified to validate and verify the extensions. This section contains the recommended guidelines for extensions.

1.1.4 Alternate approaches

The different transport mechanisms are covered under the bindings dimension.

1.2 Authorities

<Describe the authorities and relevant use case sections>

1.3 Roles

<Describe the roles and relevant use case sections>

1.4 Bindings

<Describe the bindings and relevant use cases sections>
1.5 SAML Conformance Program

The Conformance Program is described in detail in the separate SAML Conformance Program Specification V1.0. This document describes the tests required for validation and/or certification at a given profile and level, the procedure for running those tests, and the resources available to assist in validating or certifying implementations and applications.
2 Things To Do

1. There might be no bindings for an assertion, ie embedded assertions. How can we specify and validate conformance?

2. Is partition right word? subset? profile?

3. In each partition, should we define the core that is required and then the additional elements that a vendor can support for that partition? Now the granularity is a partition.