

# 1 SAML Conformance Clause

## 3 This version:

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

---

---

## 8 Authors

- 9 o Krishna Sankar [ksankar@cisco.com]
  - 10 o Robert Griffin [Robert.Griffin@entrust.com]
  - 11 o
- 
- 

## 12 Contributors

- 13 o Lynne Rosenthal [lynne.rosenthal@nist.gov]
  - 14 o Eve Maler [eve.maler@east.sun.com]
  - 15 o Tony Palmer
  - 16 o Mark Skall
- 
- 

## 17 Abstract

18 This document describes the conformance clause for the SAML  
19 specification. The conformance clause is intended for inclusion within  
20 the SAML specification, rather than being maintained as a separate  
21 document.  
22

## 24 Referenced Documents

- 26 1. <http://www.itl.nist.gov/div897/ctg/conformProject.shtml>
- 27

28 2. <http://lists.oasis-open.org/archives/conformance/200104/msg00000.html>

29

30 3. XML Protocol specification conformance issues

## 31 **Notational Conventions**

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

## 36 **Status of this Document**

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

## 39 **Document Version History**

- 40 o Version 0.001: Initial version
- 41 o Version 0.002: First Review draft to conformance subgroup 21-May-2001
- 42 o Version 0.003: Internal Editor's version
- 43 o Version 0.004: Second review draft to SAML TC 11-June-2001
- 44 o Version 0.005: Third review draft to conformance subgroup 14-June-  
45 2001
- 46 o Version 0.006: Review draft For SAML f2f #3

47

48

48

48 **Table of Contents**

49 1 Conformance Clause.....4  
50 1.1 Introduction.....4  
51 1.1.1 Conformance Nomenclature.....5  
52 1.1.2 Mandatory/Optional :.....5  
53 1.1.3 Extensions :.....6  
54 1.1.4 Alternate approaches.....6  
55 1.2 Authorities.....6  
56 1.3 Roles 6  
57 1.4 Bindings.....6  
58 1.5 SAML Conformance Program.....7  
59 2 Things To Do.....8  
60  
61  
62

62

## 63 1 Conformance Clause

64

### 65 1.1 Introduction

66 The objectives of the SAML Conformance Clause are to:

- 67 a) Ensure a common understanding of conformance and what is required to
- 68 claim conformance;
- 69 b) Promote interoperability for the exchange of authentication and
- 70 authorization information
- 71 c) Promote uniformity in the development of conformance tests.

72

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

79

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

86

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

90

91 The SAML conformance is expressed by three orthogonal dimensions.

- 92 • The first dimension is a partition, (a.k.a. profile) which is a  
93 subset of the overall specifications that includes all of the  
94 functionality necessary to satisfy the requirements of a particular  
95 community of users. The authorities for SAML are authentication  
96 authority, authorization authority, attribute authority, session  
97 authority, Policy decision authority and policy enforcement  
98 authority.
- 99 • The second dimension is the role of a system - consumer, producer or  
100 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

104

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

107 1. Partition-Role Table :

108

<i>Partition</i>	<i>Consumer</i>	<i>Producer</i>	<i>Producer/Consumer</i>
<i>Authentication authority</i>	y	Y	y
<i>Authorization authority</i>	y	Y	y
<i>Attribute authority</i>	y	Y	y
<i>Session authority</i>	y	Y	y
<i>Policy decision authority</i>	y	Y	y
<i>Policy enforcement authority</i>	y	Y	y

109

110 2. Partition-Bindings Table:

111

<i>Partition</i>	<i>http</i>	<i>xmlp</i>	<i>SOAP</i>	<i>BEEP</i>
<i>Authentication authority</i>	y	y	y	Y
<i>Authorization authority</i>	y	y	y	Y
<i>Attribute authority</i>	y	y	y	Y
<i>Session authority</i>	y	y	y	Y
<i>Policy decision authority</i>	y	y	y	Y
<i>Policy enforcement authority</i>	y	y	y	Y

### 1.1.2 Mandatory/Optional :

113 A system can choose to implement any or all of the partitions as per table  
114 1, as a producer of SAML assertions, a consumer of SAML assertions or both.  
115 For each partition, role, binding combination (i.e., cell in the table) all  
116 functionality is mandatory. i.e. the system should support all SAML  
117 assertions related to that partition. It is optional as to which partition,  
118 role, binding combinations are supported (implemented).

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

123 **1.1.3 Extensions :**

- 124 • Extensions shall not re-define semantics for existing functions
  - 125 • Extensions shall not alter the specified behavior of interfaces
  - 126 defined in this standard
  - 127 • Extensions may add additional behaviors
  - 128 • Extensions shall not cause standard-conforming functions (i.e.,
  - 129 functions that do not use the extensions) to execute incorrectly.
- 130 SAML assertions can be extended so long as the above conditions are met. It
- 131 is requested that, if a system is extending the SAML assertions,
- 132 • The mechanism for determining application conformance and the
  - 133 extensions shall be clearly described in the documentation, and the
  - 134 extensions shall be marked as such;
  - 135 • Extensions shall follow the spirit, principles and guidelines of the
  - 136 SAML specification, that is, the specifications must be extended in a
  - 137 standard manner as defined in the extension fields.
  - 138 • In the case where an implementation has added additional behaviors,
  - 139 the implementation shall provide a mechanism whereby a conforming
  - 140 application shall be recognized as such, and be executed in an
  - 141 environment that supports the functional behavior defined in this
  - 142 standard
- 143 Note : Extensions are outside the scope of conformance. There are no
- 144 mechanisms specified to validate and verify the extensions. This section
- 145 contains the recommended guidelines for extensions.

146 **1.1.4 Alternate approaches**

147 The different transport mechanisms are covered under the bindings

148 dimension.

149 **1.2 Authorities**

150 <Describe the authorities and relevant use case sections>

151 **1.3 Roles**

152 <Describe the roles and relevant use case sections>

153 **1.4 Bindings**

154 <Describe the bindings and relevant use cases sections>

155 **1.5 SAML Conformance Program**

156 The Conformance Program is described in detail in the separate SAML  
157 Conformance Program Specification V1.0. This document describes the tests  
158 required for validation and/or certification at a given profile and level, the  
159 procedure for running those tests, and the resources available to assist in  
160 validating or certifying implementations and applications.  
161

161

## 162 **2 Things To Do**

163

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

166

2. Is partition right word ? subset ? profile ?

167

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