Issues List for Security Assertion Markup Language (SAML) V2.0

Working Draft 045, 21 November 22 December 2003

Document identifier: sstc-saml-2.0-issues-draft-054


Editor: Eve Maler, Sun Microsystems (eve.maler@sun.com)

Abstract: This document catalogues issues for Security Assertion Markup Language (SAML) V2.0, which is developed by the OASIS Security Services Technical Committee. It is intended to record specific issues that potentially need to be implemented as changes or additions to a SAML specification. Also see the SAML V2.0 work items document, which provides information on the overall scope of the V2.0 effort and general work items that have been adopted.

Status: This document is a draft working document of the OASIS Security Services Technical Committee. The intention is to update it prior to every meeting of the committee until V2.0 is completed. See the Revision History for details of changes made in this revision.

Committee members should send comments on this specification to the security-services@lists.oasis-open.org list. Others should subscribe to and send comments to the security-services-comment@lists.oasis-open.org list. To subscribe, send an email message to security-services-comment-request@lists.oasis-open.org with the word "subscribe" as the body of the message.

For information on whether any patents have been disclosed that may be essential to implementing this specification, and any offers of patent licensing terms, please refer to the Intellectual Property Rights section of the Security Services TC web page (http://www.oasis-open.org/committees/security/).
# Table of Contents

1 Introduction........................................................................................................................................... 4  
2 Technical Deliverable Issues.................................................................................................................. 5  
   2.1OVER: Technical Overview Issues.................................................................................................... 5  
   2.2CORE: Assertions, Protocol, and Schema Issues............................................................................. 5  
   2.3BIND: Binding and Profile Issues.................................................................................................... 8  
   2.4META: Metadata Issues..................................................................................................................... 9  
   2.5TECH: Other Technical Issues.......................................................................................................... 10  
3 OUT: Outreach Deliverable Issues.......................................................................................................... 11  
4 MISC: Miscellaneous Issues.................................................................................................................. 12  
   A. Acknowledgments.............................................................................................................................. 13  
   B. Revision History............................................................................................................................... 14  
   C. Notices............................................................................................................................................... 15
<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>CORE-1</td>
<td>Remove AuthorityBinding Element (Closed)</td>
<td>5</td>
</tr>
<tr>
<td>CORE-2</td>
<td>Remove RespondWith Element (Closed)</td>
<td>5</td>
</tr>
<tr>
<td>CORE-3</td>
<td>Remove Deprecated NameIdentifier URIs (Closed)</td>
<td>5</td>
</tr>
<tr>
<td>CORE-4</td>
<td>Require URI References to Be Absolute (Closed)</td>
<td>6</td>
</tr>
<tr>
<td>CORE-5</td>
<td>Null Attribute Values (Open)</td>
<td>6</td>
</tr>
<tr>
<td>CORE-6</td>
<td>Assertion-Level Subject (Open)</td>
<td>6</td>
</tr>
<tr>
<td>CORE-7</td>
<td>SOAP Version in Protocol Binding (Open)</td>
<td>7</td>
</tr>
<tr>
<td>CORE-8</td>
<td>Signing Assertions vs. Responses (Open)</td>
<td>7</td>
</tr>
<tr>
<td>CORE-9</td>
<td>Wildcarding in the SAML Schemas (Open)</td>
<td>7</td>
</tr>
<tr>
<td>CORE-10</td>
<td>Fix Description of Evidence Element's Contents (Closed)</td>
<td>8</td>
</tr>
<tr>
<td>BIND-1</td>
<td>Disallow Status as Only Child of SOAP Body (Closed)</td>
<td>8</td>
</tr>
<tr>
<td>BIND-2</td>
<td>Remove Deprecated Artifact URI (Closed)</td>
<td>9</td>
</tr>
<tr>
<td>BIND-3</td>
<td>Establish a Mandatory Profile (Open)</td>
<td>9</td>
</tr>
<tr>
<td>TECH-1</td>
<td>Identity/Service Provider Terminology (Open)</td>
<td>10</td>
</tr>
<tr>
<td>TECH-2</td>
<td>Versioning of Elements (Open)</td>
<td>10</td>
</tr>
</tbody>
</table>
1 Introduction

This document catalogues issues for Security Assertion Markup Language (SAML) V2.0, which is
developed by the OASIS Security Services Technical Committee. It is intended to record specific issues
that potentially need to be implemented as changes or additions to a SAML specification. Also see the
SAML V2.0 work items document, which provides information on the overall scope of the V2.0 effort and
general work items that have been adopted.

Each issue includes the following information:

• A unique issue ID, such as TECH-42. This appears in the section heading. The possible categories
  are OVER for the technical overview, CORE for the assertions and protocol and their governing
  schemas, BIND for bindings and profiles, META for the metadata exchange format and protocol,
  TECH for other technical issues, OUT for the outreach materials, and MISC for all other issues.

• A short name for the issue. This appears in the section heading.

• The issue's status. This appears in the section heading. The possible statuses are Open for issues
  that still need a resolution, Deferred for issues that we have put off dealing with until the next
  version of SAML, Resolved for issues that we have resolved but that remain to be implemented,
  and Closed for issues that have a resolution and require no further action (for example, because the
  resolution has been implemented or because no action at all is necessary).

• The source of the issue, indicating where it was first raised or reported.

• The assigned owner of the issue. This person is responsible for proposing options and a preferred
  resolution.

• An arbitrarily long description of the issue, including any discussion history.

• Numbered options for resolving the issue, as appropriate.

• The resolution of the issue, once this information is available. It should include the date and
  circumstances of the resolution.
2 Technical Deliverable Issues

The following are issues related to the SAML V2.0 technical deliverables.

2.1 OVER: Technical Overview Issues

The following are issues related to the technical overview.

@@TBS

2.2 CORE: Assertions, Protocol, and Schema Issues

The following are issues related to the assertions and protocol and their governing schemas.

CORE-1 Remove AuthorityBinding Element (Closed)

Source:

oasis-sstc-saml-core-1.1.pdf lines 746-747.

Owner:

Eve Maler.

Description:

This impacts the core spec and the assertion schema. Section 2.4.3, Element <AuthenticationStatement>, needs to change to remove mention of <AuthorityBinding> from the text and the schema snippet and to note the element's removal in a comment, Section 2.4.3.2, Element <AuthorityBinding>, needs to be removed, and the assertion schema needs to change correspondingly.

Resolution:

This is a backwards-incompatible change decided and promised in the V1.0 timeframe but unable to be implemented until V2.0. Implemented in core-01.

CORE-2 Remove RespondWith Element (Closed)

Source:

oasis-sstc-saml-core-1.1.pdf lines 1012-1013.

Owner:

Eve Maler.

Description:

This impacts the core spec and the assertion schema. Section 3.2.1, Element Complex Type RequestAbstractType, needs to change to remove mention of <RespondWith> from the text and the schema snippet and to note the element's removal in a comment, Section 3.2.1.1, Element <RespondWith>, needs to be removed, and the assertion schema needs to change correspondingly.

Resolution:

This is a backwards-incompatible change promised in the V1.0 timeframe but unable to be implemented until V2.0. Implemented in core-01.

CORE-3 Remove Deprecated NameIdentifier URIs (Closed)

Source:


Owner:

Eve Maler.
Description:
This impacts the core spec. Section 7.3, NameIdentifier Format Identifiers, needs to change to merely mention that a few URIs have been deprecated in this version, and Sections 7.3.2 through 7.3.4, Email Address through Windows Domain Qualified Name, need to winnow down the URI choices to just the recommended URI in each case.

Resolution:
This is a backwards-incompatible change decided and promised in the V1.0 timeframe but unable to be implemented until V2.0. Implemented in core-01.

CORE-4 Require URI References to Be Absolute (Closed)
Source:
oasis-sstc-saml-core-1.1.pdf line 219.
Owner:
Eve Maler.
Description:
This impacts the core spec. Section 1.2.1, String and URI Values, needs to change to say “all URI reference values ... and are REQUIRED to be absolute [RFC 2396].” rather than “... strongly RECOMMENDED ...”.
Resolution:
This is a backwards-incompatible change decided in the V1.0 timeframe but unable to be implemented until V2.0. Implemented in core-01.

CORE-5 Null Attribute Values (Open)
Source:
Owner:
Rob Philpott.
Description:
How should an implementation send an empty value (i.e. like a NO-VALUE value in a database) for an attribute?
Options:
@@A number of reasonable options have already been proposed in the email thread.
Resolution:
@@

CORE-6 Assertion-Level Subject (Open)
Source:
Conor Cahill on the security-services list (see thread at http://lists.oasis-open.org/archives/security-services/200310/msg00135.html).
Owner:
Scott Cantor (if Conor can't own it himself).
Description:
When all statements within an assertion have the same subject, is it possible to factor out that subject information and provide it instead at the assertion level?
Options:
Conor lists two possibilities:
• Add an <Assertion>-level <Subject> element that applies to all statements without a <Statement>-level <Subject>.
• Barring this, add a subject reference mechanism so that a statement could refer to the <Subject> in another statement.

Resolution:

CORE-7 SOAP Version in Protocol Binding (Open)
Source:
Scott Cantor, comment at SAML F2F 22-24 October 2003.
Owner:
@@
Description:
The current protocol binding to SOAP is based on SOAP V1.1, but now SOAP V1.2 has been published as a W3C Recommendation. Should we use it? Concerns have been expressed about SOAP V1.2’s inability to do signatures properly.
Options:
The obvious options are:
1. Leave the binding as it is.
2. Change the current binding to use SOAP V1.2.
3. Keep the current binding and add an additional binding to SOAP V1.2.
There may be additional actions needed based on the fact that the protocol is being extended to encompass the new identity federation features. In the cases of options 2 and 3, the security considerations may be impacted.

Resolution:
@@

CORE-8 Signing Assertions vs. Responses (Open)
Source:
Owner:
@@(we think this will get addressed as part of the new profile work)
Description:
Currently we advise signing the whole response rather than individual assertions, but this is too inflexible to allow for the passing through of assertions from elsewhere ("the intermediary problem"). We need to consider the signing of individual assertions.

Options:
@@

Resolution:
@@

CORE-9 Wildcarding in the SAML Schemas (Open)
Source:
SAML telecon of 28 October 2003, as part of the discussion of the nameid-05 proposal.
Currently, the SAML assertion and protocol schemas allow for type-based extensibility, but have so far been extremely judicious about XML markup extensibility features that do not require the definition of derived types in an extension schema. Although NameIdentifier URIs – for example – provide extensibility of element string content, the schemas have no `<xsd:anyAttribute>` and few `<xsd:any>` wildcards.

Should we be adding `<xsd:anyAttribute>` everywhere on principle? Should we be adding `<xsd:any>` to additional (or all) complex types?

**CORE-10 Fix Description of Evidence Element’s Contents (Closed)**

**Source:** Frederic Deleon on saml-dev list (http://lists.oasis-open.org/archives/saml-dev/200310/msg00001.html)

**Owner:** Eve Maler

**Description:**
The description of the contents of the `<Evidence>` element is incorrect. The schema allows an unbounded number of `<AssertionIDReference>` and `<Assertion>` elements in any order, but the description says that it can contain only one subelement.

**Options:**
Correct the description on lines 912-917 in oasis-sstc-saml-core-1.1 to reflect the correct occurrence of these subelements.

**Resolution:** Implemented in sstc-saml-core-2.0-draft-02 (still to be released at the time of publishing this rev-05 issues list).

### 2.3 BIND: Binding and Profile Issues

The following are issues related to the Technical Overview deliverable.

**BIND-1 Disallow Status as Only Child of SOAP Body (Closed)**

**Source:** oasis-sstc-saml-bindings-1.1.pdf lines 316-317.

**Owner:** Frederick Hirsch.

**Description:**
This impacts the bindings spec. Section 3.1.3.6, Error Reporting, needs to change to winnow the two choices for inclusion of a `<Status>` element in a SOAP message down to the recommended one, and mention that one method was removed.

**Resolution:** This is a backwards-incompatible change decided and promised in the V1.0 timeframe but unable to be implemented until V2.0. Implemented in bindings-02.
BIND-2 Remove Deprecated Artifact URI (Closed)

Source:
oasis-sstc-saml-bindings-1.1.pdf line 426.

Owner:
Frederick Hirsch.

Description:
This impacts the bindings spec. Section 4.1.1.1, Required Information (for Browser/Artifact Profile of SAML), needs to change to remove the deprecated URI, and several subsequent subsections need to be edited (search for the word "deprecated") to remove mention of the deprecated option.

Resolution:
This is a backwards-incompatible change decided and promised in the V1.0 timeframe but unable to be implemented until V2.0. Implemented in bindings-02.

BIND-3 Establish a Mandatory Profile (Open)

Source:

Owner:
@@

Description:
Dan actually made several suggestions in his blog entry:

1) OASIS, or an appropriate third party, should arrange for a reference implementation, or test harness, of SAML to be created against which all implementers can freely test over the network. This alone may be sufficient to solve the brunt of the interoperability issue, and it should be possible to create such an implementation using OpenSAML or SourceID in less than 90 days. As a follow up OASIS or an appropriate third party could also arrange for recurring interoperability testing events similar to those Liberty Alliance has announced.

2) Since the majority of vendors we surveyed so far support unsigned SAML 1.0 requests using the artifact profile over SSL connections with client and server authentication, the test harness should support this use case ASAP, then the others. We also believe the SSTC should consider making the described use case mandatory so that all customers can be assured of a "lowest common denominator" SAML interaction mode regardless of the vendor they pick.

3) In addition, customers are generally finding federated identity business issues difficult. OASIS should publish a "SAML cookbook" that customers can read to categorize their required pattern of federation, assess their risks, and compose a workable strategy going forward."

This issue specifically relates to the second part of suggestion #2. His other suggestions are being taken up in other fashions: The co-chairs are looking into #1, and the editors are looking into #3 as an editorial matter.

Resolution:
@@

2.4 META: Metadata Issues

The following are issues related to the metadata exchange format and protocol deliverable.

@@TBS
2.5 TECH: Other Technical Issues

The following are technical issues related to areas not already covered above.

TECH-1 Identity/Service Provider Terminology (Open)


Owner: Eve Maler

Description: Currently we introduce terminology in the bindings spec about "source" and "destination" sites, which we’ve never been entirely happy with. Liberty uses “identity provider” and “service provider”, which are more meaningful. (Note that “identity provider” is broader than “authentication authority”.) We need to consider a wholesale change to our terminology, either in the Liberty direction or in some other direction. The solution should be able to be used globally across the specs, and not be specific just to the bindings. (We will likely still need the “asserting party”/“relying party” terminology because it has a different purpose.)

Options:
1. Keep the current terminology.
2. Change it over to an identity provider/service provider frame of reference in just the bindings document
3. Change it over in both bindings and core
4. Change it to yet another set of terms.

Resolution: @@

TECH-2 Versioning of Elements (Open)

Source: Ongoing issue.

Owner: @@

Description: We need to decide whether to support mixing, say, older-version assertions inside newer-version responses. The current relationship between the protocol and assertion schemas is relatively static regarding version association.

Options: @@

Resolution: @@
3 OUT: Outreach Deliverable Issues

The following are issues related to the outreach deliverables.

@@TBS
4 MISC: Miscellaneous Issues

The following are issues related to areas of the SAML V2.0 effort not already covered above.

@@TBS
A. Acknowledgments

The editors would like to acknowledge the contributions of the OASIS Security Services Technical Committee, whose voting members at the time of publication were:

@@TBS
# B. Revision History

<table>
<thead>
<tr>
<th>Rev</th>
<th>Date</th>
<th>By Whom</th>
<th>What</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>13 Oct 2003</td>
<td>Eve Maler</td>
<td>Initial draft.</td>
</tr>
<tr>
<td>02</td>
<td>20 Oct 2003</td>
<td>Eve Maler</td>
<td>Marked CORE-1 through CORE-4 and BIND-1 through BIND-2 as closed because they have been implemented. Added CORE-6.</td>
</tr>
<tr>
<td>03</td>
<td>26 Oct 2003</td>
<td>Eve Maler</td>
<td>Added CORE-7, CORE-8, TECH-1, and TECH-2.</td>
</tr>
<tr>
<td>04</td>
<td>21 Nov 2003</td>
<td>Eve Maler</td>
<td>Added CORE-9 and BIND-3.</td>
</tr>
<tr>
<td>05</td>
<td>22 Dec 2003</td>
<td>Eve Maler</td>
<td>Added CORE-10 (and promptly closed it).</td>
</tr>
</tbody>
</table>
C. Notices

OASIS takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on OASIS's procedures with respect to rights in OASIS specifications can be found at the OASIS website. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification, can be obtained from the OASIS Executive Director.

OASIS invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to implement this specification. Please address the information to the OASIS Executive Director.

Copyright © OASIS Open 2003. All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself does not be modified in any way, such as by removing the copyright notice or references to OASIS, except as needed for the purpose of developing OASIS specifications, in which case the procedures for copyrights defined in the OASIS Intellectual Property Rights document must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors or assigns.

This document and the information contained herein is provided on an “AS IS” basis and OASIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.