Issues List for Security Assertion Markup Language (SAML) V1.1

Working Draft 01, 25 June 2003

Document identifier:
sstc-saml-1.1-issues-draft-01

Location:
http://www.oasis-open.org/committees/documents.php?wg_abbrev=security

Editor:
Rob Philpott, RSA Security <rphilpott@rsasecurity.com>

Contributors:
Hal Lockhart, BEA Systems (former editor)

Abstract:
This document catalogs issues for the Security Assertions Markup Language (SAML) V1.1, developed by the OASIS Security Services Technical Committee. It lists those issues deferred during work on the SAML V1.0 standard and any new issues raised during the SAML V1.1 effort.

Status:
This document is a draft working document of the OASIS Security Services Technical Committee. This document is updated periodically on no particular schedule. Send comments to the editor.

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/).

Colors: Gray Blue Yellow

Table of Contents

Colors: Gray Blue Yellow

Colors: Gray Blue Yellow

117

Colors: Gray Blue Yellow

Introduction

This document describes all issues deferred during work on the SAML V1.0 standard and any new issues that were raised during the SAML V1.1 effort. These issues have been raised on the SSTC mailing lists, in conference calls, and in other venues. The SAML V1.0 issues list is available at **[ISSUES-1.0]**. All issues in this document are deferred or closed. All deferred issues will be reviewed during the SAML V2.0 effort.

1.1 Notation

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 **[RFC2119]**.

Each issue includes the following information:

- **ISSUE: [Category-Issue Number: Short name]**
- **Source:** Location where the issue was initially raised (e.g. V1.0 Deferred Issue)
- **Champion:** None
- **Status:** Date - Decision
- **Description:** Long description of the issue
- **Resolution Alternatives:** With optional editor resolution

The following “Category” codes are defined for the issues:

- UC – Use Case issues
- DS – Design issues
- MS – Miscellaneous issues

The issues within each category are grouped according to general areas of concern. The "Issue Number" is thus specified as "group-nn", where “group” identifies the area group, and “nn” is the issue # within the group. To avoid reusing issue numbers from V1.0 issues that were closed and thus don’t appear in this document, the higest issue number used within each group in the V1.0 Issues List **[ISSUES-1.0]** is listed at the beginning of the group section in this document.

To make reading this document easier, the following convention has been adopted for shading sections in various colors. Modified text in updated sections of the current document revision is displayed in red font.

Gray sections indicate issues closed or deferred in previous revisions of this document.

Blue sections indicate issues closed or deferred in the current revision of this document.

Yellow sections indicate issues recently created or modified or that are actively being debated.

Other open issues are not marked, i.e. left white.

Colors: Gray Blue Yellow

2 Use Case Issues

2.0 Group 0: Document Format & Strategy

Highest V1.0 Issue Number: UC-0-03

No deferred or new issues.

2.1 Group 1: Single Sign-on Push and Pull Variations

Highest V1.0 Issue Number: UC-1-14

2.1.1 ISSUE:[UC-1-05:FirstContact]

Source: V1.0 Deferred Issue

Champion: None

Status: 25-Jun-2003 – Propose closing this issue.

Status: 29-Jan-2002 – Deferred by vote. Discussions at F2F#4 established that SAML 1.0 partially meets this requirement, but does not provide everything TC members could envisage.

Status: F2F #2 – Closed by explicit vote, Option 2 carries, however see UC-1-14

Description: A variation on the single sign on use case that has been proposed is one where the Web user goes directly to the destination Web site without authenticating with a definitive authority first.

[25-Jun-2003] Destination Site First use cases were again explored during V1.1. The Liberty Alliance's Liberty 1.1 ID Federation Framework provides use cases for this area. Now that the Liberty 1.1 ID-FF specifications have been contributed to the SSTC for our V2.0 effort, the committee should use the Liberty use cases and thus this issue can be closed.

[Text Removed to Archive]

Resolution Alternatives:

1. Add this use case scenario to the use case document.
2. Do not add this use case scenario to the use case document.
3. Address this issue using the Liberty use cases.

2.1.2 DEFERRED ISSUE:[UC-1-14: NoPassThruAuthnImpactsPEP2PDP]

Source: V1.0 Deferred Issue

Champion: None

Status: 5-Feb-2002 – Deferred by vote – Previously closed on 15-May-2002 telcon. Option 2 carries

Description: Stephen Farrell has argued that dropping PassThruAuthN prevents standardization of important functionality in a commonly used configuration.

The counter argument is the technical difficulty of implementing this capability, especially when both username/password and PKI AuthN must be supported.

Resolution Alternatives:

Colors: Gray Blue Yellow

1. Add this requirement to SAML 1.0
2. authorize a subgroup/task force to evaluate a suitable pass-through authN solution for eventual inclusion in V.next of SAML. If the TC likes the design once it is presented, it may choose to open up its scope to once again include pass-through authN in V1.0. Stephen is willing to champion this."
3. Do not add this requirement.

2.2 Group 2: B2B Scenario Variations

Highest V1.0 Issue Number: UC-2-08

2.2.1 DEFERRED ISSUE:[UC-2-05:EMarketplace]

Source: V1.0 Deferred Issue

Champion: None

Status: 29-Jan-2002 – Deferred by vote. This functionality is not directly supported by SAML 1.0 Bindings and Profiles, but could be constructed using the current core.

Description: Zahid Ahmed proposes the following additional use case scenario for inclusion in the use case and requirements document.

Scenario X: E-Marketplace

[Text Removed to Archive]

Resolution Alternatives:

1. The above scenario should be added to the use cases document.
2. The above scenario should not be added to the document.

2.3 Group 3: Sessions

Highest V1.0 Issue Number: UC-3-09

[At F2F #2, it was agreed to charter a sub group to “do the prep work to ensure that logout, timein, and timeout will not be precluded from working with SAML later; commit to doing these other pieces "next" after 1.0.” Therefore all the items in this section have been closed with the notation “referred to sub group.”]

[25-Jun-2003] Some of the session requirements discussed in this group have been addressed by the Liberty Alliance’s Liberty 1.1 ID Federation Framework. Now that the Liberty 1.1 ID-FF specifications have been contributed to the SSTC for our V2.0 effort, the committee should determine whether these issues need to be carried forward to V2.0.

The purpose of the issues/resolutions in this group is to provide guidance to the rest of the TC as to the functionality required related to sessions. Some of the scenarios contain some detail about the messages which are transferred between parties, but the intention is not to require a particular protocol. Instead, these details are offered as a way of describing the functionality required. It would be perfectly acceptable if the resulting specification used different messages to accomplish the same functionality.

2.3.1 DEFERRED ISSUE:[UC-3-01:UserSession]

Source: V1.0 Deferred Issue

Champion: None

Status: 5-Feb-2002 – Deferred by vote.

Description: Should the use cases of log-off and timeout be supported

Colors: Gray Blue Yellow

[Text Removed to Archive].

Resolution Alternatives:

1. Add this requirement and/or use cases to SAML.
2. Do not add this requirement and/or use cases.

2.3.2 DEFERRED ISSUE:[UC-3-02:ConversationSession]

Source: V1.0 Deferred Issue

Champion: None

Status: 5-Feb-2002 – Deferred by vote.

Description: Is the concept of a session between security authorities separate from the concept of a user session? If so, should use case scenarios or requirements supporting security system sessions be supported? [DavidO: I don't understand this issue, but I have left in for backwards compatibility]. [DarrenP: I think this issue arose out of a misunderstanding/miscommunication on the mailing list and has been resolved. This is more of a formality to vote this one to a closed status.]

Resolution Alternatives:

1. Do not pursue this requirement as it is not in scope.
2. Do further analysis on this requirement to determine what it is specifically.

2.3.3 DEFERRED ISSUE:[UC-3-03:Logout]

Source: V1.0 Deferred Issue

Champion: None

Status: 5-Feb-2002 – Deferred by vote.

Description: Should SAML support transfer of information about application-level logouts (e.g., a principal intentionally ending a session) from the application to the Session Authority ?

Candidate Requirement:

[CR-3-3-Logout] SAML shall support a message format to indicate the end of an application-level session due to logout by the principal.

Note that this requirement is implied by Scenario 1-3 (the second scenario 1-3 in straw man 3 - oops). This issue seeks to clarify the document by making the requirement explicit.

Resolution Alternatives:

1. Add this requirement to SAML.
2. Do not add this requirement to SAML.

2.3.4 DEFERRED ISSUE:[UC-3-05:SessionTermination]

Source: V1.0 Deferred Issue

Champion: None

Status: 5-Feb-2002 – Deferred by vote.

Description: For managing a SAML User Sessions, it may be useful to have a way to indicate that the SAML-level session is no longer valid. The logout requirement would invalidate a session based on user input. This requirement, for termination, would invalidate the SAML-level session based on other factors, such as when the user has not used any of the SAML-level sessions

Colors: Gray Blue Yellow

constituent application- level sessions for more than a set amount of time. Timeout would be an example of a session termination.

Candidate requirement:

> [CR-3-5-SessionTermination] SAML shall support a message format for timeout of a SAML-level session. Here, "termination" is defined as the ending of a SAML-level session by a security system not based on user input. For example, if the user has not used any of the application-level sub-sessions for a set amount of time, the session may be considered "timed out."

Note that this requirement is implied by Scenario 1-3, figure 6, specifically the last message labeled 'optionally delete/revoke session'. This issue seeks to clarify the document by making the requirement explicit.

Resolution Alternatives:

1. Add this requirement to SAML.
2. Do not add this requirement and/or use cases.

2.3.5 DEFERRED ISSUE:[UC-3-06:DestinationLogout]

Source: V1.0 Deferred Issue

Champion: None

Status: 5-Feb-2002 – Deferred by vote.

Description: Should logging out of an individual application-level session be supported? Advantage: allows application Web sites control over their local domain consistent with the model most widely implemented on the web. Disadvantage: potentially more interactions between the application and the Session Authority.

[Text Removed to Archive]

Resolution Alternatives:

1. Add this scenario and requirement to SAML.
2. Do not add this scenario or requirement.

2.3.6 DEFERRED ISSUE:[UC-3-07:Logout Extent]

Source: V1.0 Deferred Issue

Champion: None

Status: 5-Feb-2002 – Deferred by vote.

Description: What is the impact of logging out at a destination web site?

Possible Resolution:

1. Logout from destination web site is local to destination [DavidO recommendation]
2. Logout from destination web site is global, that is destination + source web sites.

2.3.7 DEFERRED ISSUE:[UC-3-08:DestinationSessionTermination]

Source: V1.0 Deferred Issue

Champion: None

Status: 5-Feb-2002 – Deferred by vote.

Colors: Gray Blue Yellow

Description: Having the Session Authority determine the timeout of a session is covered under [UC-3-5]. This issue covers the manner and extent to which systems participating in that session can initiate and control the timeout of their own sessions.

[Text Removed to Archive].

Resolution Alternatives:

1. Add this scenario and requirement to SAML.
2. Do not add this scenario or requirement.

2.3.8 DEFERRED ISSUE:[UC-3-09:Destination-Time-In]

Source: V1.0 Deferred Issue

Champion: None

Status: 5-Feb-2002 – Deferred by vote.

Description: In this scenario, a user has traveled from the source site (site of initial login) to some destination site. The source site has set a maximum idle-time limit for the user session, based on user activity at the source or destination site. The user stays at the destination site for a period longer than the source site idle-time limit; and at that point the user returns to the source site. We do not wish to have the user time-out at the source site and be re-challenged for authentication; instead, the user should continue to enjoy the original session which would somehow be cognizant of user activity at the destination site.

Candidate Requirement:

[CR-3-9:Destination-TimeIn] SAML shall support destination system time-in.

Resolution Alternatives:

1. Add this scenario and requirement to SAML.
2. Do not add this scenario or requirement to SAML.

2.4 Group 4: Security Services

Highest V1.0 Issue Number: UC-4-04

No deferred or new issues.

2.5 Group 5: AuthN Protocols

Highest V1.0 Issue Number: UC-5-03

2.5.1 DEFERRED ISSUE:[UC-5-02:SASL]

Source: V1.0 Deferred Issue

Champion: None

Status: 5-Feb-2002 – Deferred by vote. Was previously closed per F2F #2, Option 2 carries.

Description: Is there a need to develop materials within SAML that explore its relationship to SASL [SASL]?

Resolution Alternatives:

1. Yes
2. No

Colors: Gray Blue Yellow

2.6 Group 6: Protocol Bindings

Highest V1.0 Issue Number: UC-6-01

No deferred or new issues.

2.7 Group 7: Enveloping vs. Enveloped

Highest V1.0 Issue Number: UC-7-02

No deferred or new issues.

2.8 Group 8: Intermediaries

Highest V1.0 Issue Number: UC-8-05

2.8.1 DEFERRED ISSUE:[UC-8-02:IntermediaryAdd]

Source: V1.0 Deferred Issue

Champion: None

Status: 29-Jan-2002 – Deferred by vote. There is no support for intermediaries in SAML 1.0. In fact, the SOAP Profile was defined to explicitly omit interactions among more than two parties.

Description: One question that has been raised is whether intermediaries can make additions to SAML documents. It is possible that intermediaries could add data to assertions, or add new assertions that are bound to the original assertions.

[Text Removed to Archive]

Resolution Alternatives:

1. Add this use-case scenario to the document.
2. Don't add this use-case scenario.

2.8.2 DEFERRED ISSUE:[UC-8-03:IntermediaryDelete]

Source: V1.0 Deferred Issue

Champion: None

Status: 29-Jan-2002 – Deferred by vote. There is no support for intermediaries in SAML 1.0. In fact, the SOAP Profile was defined to explicitly omit interactions among more than two parties.

Description: Another issue with intermediaries is whether SAML must support allowing intermediaries to delete data from SAML documents.

[Text Removed to Archive]

Resolution Alternatives:

1. Add this use-case scenario to the document.
2. Don't add this use-case scenario.

2.8.3 DEFERRED ISSUE:[UC-8-04:IntermediaryEdit]

Source: V1.0 Deferred Issue

Champion: None

Status: 29-Jan-2002 – Deferred by vote. There is no support for intermediaries in SAML 1.0. In fact, the SOAP Profile was defined to explicitly omit interactions among more than two parties.

Colors: Gray Blue Yellow

Description: Similar to [UC-8-03:IntermediaryDelete] is the issue of whether SAML must support allowing intermediaries to edit or change SAML data as they pass it between parties.

[Text Removed to Archive]

Resolution Alternatives:

1. Add this use-case scenario to the document.
2. Don't add this use-case scenario.

2.9 Group 9: Privacy

Highest V1.0 Issue Number: UC-9-02

2.9.1 DEFERRED ISSUE:[UC-9-01:RuntimePrivacy]

Source: V1.0 Deferred Issue

Champion: None

Status: 29-Jan-2002 – Deferred by vote.

Description: Should protecting the privacy of the user be part of the SAML conversation? In other words, should user consent to exchange of data be given at run time, or at the time the user establishes a relationship with a security system?

An example of runtime privacy configuration would be use case scenario described in [UC-1-04:ARundgrenPush]. Because this scenario has been rejected by the use cases and requirement group, it makes sense to phrase this as a non-goal of SAML, rather than as a requirement.

[CR-9-01:RuntimePrivacy] SAML does not provide for subject control of data flow (privacy) at run-time. The determination of privacy policy is between the subject and security authorities and should be determined out-of-band, for example, in a privacy agreement.

Resolution Alternatives:

1. Add this proposed non-goal.
2. Do not add this proposed non-goal.

Voting Results:

Date	27 Mar 2001
Eligible	15
Resolution 1	9
Resolution 2	4

2.10 Group 10: Framework

Highest V1.0 Issue Number: UC-10-07

No deferred or new issues.

2.11 Group 11: AuthZ Use Case

Highest V1.0 Issue Number: UC-11-01

No deferred or new issues.

Colors: Gray Blue Yellow

2.12 Group 12: Encryption

Highest V1.0 Issue Number: UC-12-04

2.12.1 DEFERRED ISSUE:[UC-12-04:EncryptionMethod]

Source: V1.0 Deferred Issue

Champion: None

Status: 5-Feb-2002 – Deferred by vote. Previously closed per F2F #2, Resolution 3 Carries

Description: If confidentiality protection is included in the SAML assertion format (that is, you chose option 1 or 2 for [UC-12-02:AssertionConfidentiality]), how should the protection be provided?

Note that if option 2 (assertion confidentiality is required) was chosen for UC-12-02, resolution 1 of this issue implies that SAML will not be published until after XML Encryption is published.

Resolution Alternatives:

1. Add the requirement: [R-EncryptionMethod] SAML should use XML Encryption.
2. Add the requirement: [R-EncryptionMethod] Because there is no currently published standard for encrypting XML, SAML should define its own encryption format. Edit the existing non-goal of not creating new cryptographic techniques to allow this.
3. Add no requirement now, but include a note that this issue must be revisited in a future version of the SAML spec after XML Encryption is published.
4. Do not add any of these requirements or notes.

2.13 Group 13: Business Requirements

Highest V1.0 Issue Number: UC-13-07

2.13.1 DEFERRED ISSUE [UC-13-07: Hailstorm Interoperability]

Source: V1.0 Deferred Issue

Champion: None

Status: 29-Jan-2002 – Deferred by vote.

Description: Should SAML provide interoperability with the Microsoft Hailstorm architecture, including the Passport login system?

Resolution Alternatives: ???

2.14 Group 14: Domain Model

Highest V1.0 Issue Number: UC-14-01

2.14.1 DEFERRED ISSUE:[UC-14-01:UMLCardinalities]

Source: V1.0 Deferred Issue

Champion: None

Status: 29-Jan-2002 – Deferred by vote.

Description: The cardinalities in the UML diagrams in the Domain Model are backwards.

Frank Seliger comments: The Domain model claims to use the UML notation, but has the multiplicities according to the Coad method. If it were UML, the diagram would state that one Credential could belong to many Principals. I assume that we would rather want to state that one

Colors: Gray Blue Yellow

Principal can have many Credentials, similarly for System Entity, the generalization of User. One Principal would belong to several System Entities or Users according to the diagram. I would rather think we want one System Entity or User to have several Principals.

My theory how these wrong multiplicities happened is the following: As I can see from the change history, the tool Together has been used to create the initial version of this diagram. Together in its first version used only the Peter Coad notation. Later versions still offered the Coad notation as default. Peter Coad had the cardinalities (UML calls this multiplicities) just swapped compared to the rest of the world. This always caused grief, and it did again here.

Dave Orchard agrees this should be fixed.

Resolution Alternatives: ???

Colors: Gray Blue Yellow

3 Design Issues

3.1 Group 1: Naming Subjects

Highest V1.0 Issue Number: DS-1-13

3.1.1 DEFERRED ISSUE:[DS-1-02: Anonymity Technique]

Source: V1.0 Deferred Issue

Champion: None

Status: 29-Jan-2002 – Deferred by vote.

Description: How should the requirement of Anonymity of SAML assertions be met?

Resolution Alternatives:

1. Generate a new, random identified to refer to an individual for the lifetime of a session.
2. ???

3.2 Group 2: Naming Objects

Highest V1.0 Issue Number: DS-2-02

No deferred or new issues.

3.3 Group 3: Assertion Validity

Highest V1.0 Issue Number: DS-3-03

3.3.1 CLOSED ISSUE:[DS-3-01: DoNotCache]

Source: V1.0 Deferred Issue

Champion: Hal Lockhart

Status: 25-Jun-2003 – This issue was resolved in V1.1 and Resolution Alternative 2 was implemented.

Status: 29-Jan-2002 – Deferred by vote.

Description: It has been suggested that there should be a way in SAML to specify that an assertion is currently valid, but should not be cached for later use. This should not depend on the particular amount of variation between clocks in the network.

For example, a PDP may wish to indicate to a PEP that it should make a new request for every authorization decision. For example, its policy may be subject to change at frequent and unpredictable intervals. It would be desirable to have a SAML specified convention for doing this. This may interact with the position taken on clock skew. For example, if SAML takes no position on clock skew the PDP may have to set the NotAfter value to some time in the future to insure that it is not considered expired by the PEP.

Resolution Alternatives:

1. SAML will specify some combination of settings of the IssueInstant and ValidityInterval to mean that the assertion should not be cached. For example, setting all three datetime fields to the same value could be deemed indicate this.

Colors: Gray Blue Yellow

2. SAML will add an additional element to either Assertions or Responses to indicate the assertion should not be cached.
3. SAML will provide no way to indicate that an Assertion should not be cached.

3.4 Group 4: Assertion Style

Highest V1.0 Issue Number: DS-4-15

3.4.1 DEFERRED ISSUE:[DS-4-06: Final Types]

Source: V1.0 Deferred Issue

Champion: None

Status: 5-Feb-2002 – Deferred by vote. Was previously closed by vote on Sept 4. The Schema recommendations proposed by Eve and Phill at F2F#4 have been accepted.

Description: Does the TC plan to restrict certain types in the SAML schema to be final? If so, which types are to be so restricted?

This was identified as CONS-03.

Resolution Alternatives: ???

3.4.2 DEFERRED ISSUE:[DS-4-15: Common XML Attributes]

Source: V1.0 Deferred Issue

Champion: Eve Maler

Status: 19-Mar-2002 – Deferred by vote.

Description: Factor out various common XML attributes used in various places. This is ELM-1 in:

http://lists.oasis-open.org/archives/security-services/200203/msg00042.html

Resolution Alternatives: ???

3.5 Group 5: Reference Other Assertions

Highest V1.0 Issue Number: DS-5-04

3.5.1 DEFERRED ISSUE:[DS-5-01: Dependency Audit]

Source: V1.0 Deferred Issue

Champion: None

Status: 29-Jan-2002 – Deferred by vote.

Description: One issue with draft-sstc-core-07.doc is a lack of support for audit of assertion dependency between co-operating authorities. As one explicit goal of SAML was to support inter-domain security (i.e., each authority may be administered by a separate business entity) this seems to be a serious "gap" in reaching that goal.

Consider the following example:

(1) User Ravi authenticates in his native security domain and receives

Assertion A:

```
<Assertion>
<AssertionID>http://www.small-company.com/A</AssertionID>
<Issuer>URN:small-company:DivisionB</Issuer>
<ValidityInterval> . . . </ValidityInterval>
```


Colors: Gray Blue Yellow

```
      <Claims>
        <subject>"cn=ravi, ou=finance, id=325619"</subject>
        <attribute>manager</attribute>
      </Claims>
    </Assertion>
```

(2) User Ravi authenticates to the Widget Marketplace using assertion A and based on the policy:

All entities with "ou=finance" authenticated thru small-company.com with attribute manager have purchase limit $100,000 receives Assertion B from the Widget Marketplace:

```
      <Assertion>
    <AssertionID>http://www.WidgetMarket.com/B<AssertionID>
    <Issuer>URN:WidgetMarket:PartsExchange</Issuer>
    <ValidityInterval>. . . </ValidityInterval>
    <Claims>
      <subject>"cn=ravi, ou=finance, id=325619"</subject>
      <attribute>max-purchase-limit-$100,000</attribute>
    </Claims>
  <Assertion>
```

(3) User Ravi purchases farm machinery from a parts provider hosted at the Widget Marketplace. The parts provider authorizes the transaction based on Assertion B.

Even though Assertion B has been issued by the Widget Marketplace in response to assertion A (I guess another way to look at this to view assertion A as the subject of B as in [1]) there is no way to represent this information within SAML.

If there is a problem with Ravi's purchases at the Widget Marketplace (Ravi wont pay his bills) there is nothing in the SAML flow that ties Assertion B to Assertion A. This appears to be a significant missing piece to me.

Resolution Alternatives: ???

3.6 Group 6: Attributes

Highest V1.0 Issue Number: DS-6-06

3.6.1 DEFERRED ISSUE:[DS-6-01: Nested Attributes]

Source: V1.0 Deferred Issue

Champion: None

Status: 29-Jan-2002 – Deferred by vote.

Description: Should SAML support nested attributes? This means that for example, a role could be a member of another role. This is one standard way of distinguishing the semantics of roles from groups.

There are many issues of semantics and pragmatics related to this. These include:

1. Limit of levels if any
2. Circular references
3. Distributed definition
4. Mixed attribute types.

Resolution Alternatives: ???

3.6.2 DEFERRED ISSUE:[DS-6-04: Negative Roles]

Source: V1.0 Deferred Issue

Colors: Gray Blue Yellow

Champion: None

Status: 29-Jan-2002 – Deferred by vote.

Description: Should there be a way to state that someone does not have a role?

Resolution Alternatives: ???

3.7 Group 7: Authentication Assertions

Highest V1.0 Issue Number: DS-7-06

3.7.1 DEFERRED ISSUE:[DS-7-06: DiscoverAuthNProtocols]

Source: V1.0 Deferred Issue

Champion: None

Status: 29-Jan-2002 – Deferred by vote.

Description: Should SAML provide a means to discover supported types of AuthN protocols?

Simon Godik has suggested: One way to do it is to use AuthenticationQuery with empty Authenticator subject. Then SAMLRequest will carry AuthenticationAssertion with Authenticator subject listing acceptable protocols.

The problem is that Authenticator element does not allow for 0 occurances of Protocol. Should we specify minOccurs=0 on Protocol element for that purpose?

Resolution Alternatives:

1. Declare AuthN Protocol discovery out of scope for SAML V1.0.
2. Support it in the way suggested.
3. Support it some other way.

3.8 Group 8: Authorities and Domains

Highest V1.0 Issue Number: DS-8-06

No deferred or new issues.

3.9 Group 9: Request Handling

Highest V1.0 Issue Number: DS-9-16

3.9.1 DEFERRED ISSUE:[DS-9-02: MultipleRequest]

Source: V1.0 Deferred Issue

Champion: None

Status: 29-Jan-2002 – Deferred by vote.

Description: Should SAML provide a means of requesting multiple assertion types in a single request? This has been referred to as “boxcaring.” In simplest form this could consist of concatenating several defined requests one message. However there are usecases in which it would convenient to have the second request use data from the results of the first.

For example, it would be useful to ask for an AuthN Assertion by ID and for and Attribute Assertion referring to the same subject.

Resolution Alternatives:

1. Do not specify a way to make requests for multiple assertions types in SAML V1.0.

Colors: Gray Blue Yellow

2. Allow simple concatenation of requests in one message.
3. Provide a more general scheme for multiple requests.

3.9.2 DEFERRED ISSUE:[DS-9-03: IDandAttribQuery]

Source: V1.0 Deferred Issue

Champion: None

Status: 29-Jan-2002 – Deferred by vote.

Description: Should SAML allow queries containing both an Assertion ID and Attributes?

Tim Moses comments: The need to convey an assertion id and attributes in the same query arises in the following circumstances.

[Text Removed to Archive]

Resolution Alternatives:

1. Allow queries to specify both an Assertion ID and Attributes
2. Only allow queries to specify one or the other.

3.9.3 DEFERRED ISSUE:[DS-9-05: RequestAttributes]

Source: V1.0 Deferred Issue

Champion: Simon Godik

Status: 12-Mar-2002 – Deferred by vote.

Description: We should be able to pass request attributes to the issuing party.

I would like to propose addition to the RequestType:

```
<complexType name="RequestType">
    <complexContent>
        <extension base="samlp:RequestAbstractType">
            <sequence>
                <element ref="saml:Attribute" minOccurs="0" maxOccurs="unbounded"/>
                <choice>
                    -- same as before --
                </choice>
            <sequence>
        </extension>
    </complexContent>
</complexType>
```

Resolution Alternatives: ???

3.10 Group 10: Assertion Binding

Highest V1.0 Issue Number: DS-10-01

No deferred or new issues.

3.11 Group 11: Authorization Decision Assertions

Highest V1.0 Issue Number: DS-11-08

3.11.1 DEFERRED ISSUE:[DS-11-01: MultipleSubjectAssertions]

Source: V1.0 Deferred Issue

Colors: Gray Blue Yellow

Champion: None

Status: 29-Jan-2002 – Deferred by vote.

Description: It has been proposed (WhiteboardTranscription-01.pdf section 4.0) that an Authorization Decision Assertion Request (and presumably the Assertion sent in response) may contain multiple subject Assertions (or their Ids). Must these assertions all refer to the same subject or may they refer to multiple subjects.

One view is that the assertions all provide evidence about a single subject who has requested access to a resource. For example, the request might include a Authentication Assertion and one or more Attribute Assertions about the same person.

Another view is that for efficiency or other reasons it is desirable to ask about access to a resource by multiple individuals in a single request. This raises the question of how the PDP should respond if some subjects are allowed and others are not.

The PDP might have the freedom to return a single, all encompassing Assertion in response or reduce the request in order to give a positive response or return multiple Assertions with positive and negative indications.

Identified as F2F#3-30 and F2F#3-31.

Resolution Alternatives:

1. Require that all the assertions and assertion ids in a request refer to the same subject.
2. Treat assertions with different subjects as requesting a decision for each of the subjects mentioned.
3. Treat assertions with different subjects and a question about the collective group, i.e. true only if access is allowed for all.
4. Allow multiple subjects, but assign some other semantic to such a request.

3.12 Group 12: Attribute Assertions

Highest V1.0 Issue Number: DS-12-08

3.12.1 DEFERRED ISSUE:[DS-12-03: AttrSchemaReqs]

Source: V1.0 Deferred Issue

Champion: None

Status: 29-Jan-2002 – Deferred by vote.

Description: Should it be possible to request only the Attribute schema?

This was identified as F2F#3-22.

Resolution Alternatives:

1. Allow Attribute Schema Requests.
2. Do not allow Attribute Schema Requests.

3.12.2 DEFERRED ISSUE:[DS-12-04: AttrNameReqs]

Source: V1.0 Deferred Issue

Champion: None

Status: 29-Jan-2002 – Deferred by vote.

Description: Should it be possible to request only attribute names and not values? It is not clear whether these would be all the attributes the Attribute Authority knows about or just the ones

Colors: Gray Blue Yellow

pertaining to a particular subject. It is not clear what this would be used for. No usecase seems to require it.

This was identified as F2F#3-23.

This was identified as PRO-04.

Resolution Alternatives:

1. Allow Attribute Name Requests.
2. Do not allow Attribute Name Requests.

3.12.3 DEFERRED ISSUE:[DS-12-08: Delegation]

Source: V1.0 Deferred Issue

Champion: Hal Lockhart

Status: Deferred.

Description: Should SAML provide assertion statements concerning delegation? Proposed by Nell Rehn on the public comment list.

http://lists.oasis-open.org/archives/security-services-comment/200202/msg00009.html

Resolution Alternatives: ???

3.13 Group 13: Dynamic Sessions

Highest V1.0 Issue Number: DS-13-01

3.13.1 DEFERRED ISSUE:[DS-13-01: SessionsinEffect]

Source: V1.0 Deferred Issue

Champion: None

Status: 29-Jan-2002 – Deferred by vote.

Description: How can a relying party determine if dynamic sessions are in effect? If dynamic sessions are in effect it will be necessary to determine if the session has ended, even if the relevant Assertions have not yet expired. However, if dynamic sessions are not in use, attempting to check session state is likely to increase response times unnecessarily.

This was identified as F2F#3-3.

Resolution Alternatives:

1. Define a field in Assertion Headers to indicate dynamic sessions.
2. Configure the implementation based on some out of band information.

3.14 Group 14:General – Multiple Message Types

Highest V1.0 Issue Number: DS-14-20

3.14.1 DEFERRED ISSUE:[DS-14-04: Aggregation]

Source: V1.0 Deferred Issue

Champion: None

Status: 29-Jan-2002 – Deferred by vote.

Description: Do we need an explicit element for aggregating multiple assertions into a single object as part of the SAML specification? If so, what is the type of this element?

Colors: Gray Blue Yellow

This was identified as CONS-01.

Resolution Alternatives: ???

3.14.2 DEFERRED ISSUE:[DS-14-14: ErrMsg in Multiple Languages]

Source: V1.0 Deferred Issue

Champion: Eve Maler

Status: 9-Apr-2002 – Deferred by vote.

Description: Should SAML allow status messages to be in multiple natural languages?

In core-25, StatusMessage is defined (Section 3.4.3.3, lines 1183-1187) as being of type string. Its inclusion in the Status element (lines 1114-1115) allows multiple occurrences, that is, zero or more messages per status returned. In the call on Tuesday we discussed the potential need to allow for multiple natural-language versions of status messages.

If the StatusMessage element can't contain markup, then it makes it hard for someone to provide, say, both English and Japanese versions of an error message. Here are two obvious different ways to do this, both using the native xml:lang attribute to indicate the language in which the message is written.

(See also a possible SEPARATE issue at the bottom of this message.)

==========

Option 1: Multiple StatusMessage elements, each with language indicated

Currently, multiple StatusMessages are already allowed, but we say nothing in the spec to explain how they're supposed to be used or interpreted. The description just says (lines 1105-1106):

<StatusMessage> [Any Number]

> A message which MAY be returned to an operator.

(Hmm, not sure what "operator" means here..) This option would place a specific interpretation on the appearance of multiple StatusMessage elements related to language differentiation, and would allow for an optional xml:lang attribute on the element:

<StatusMessage> [Zero or more]

> A natural-language message explaining the status in a human-readable way. If more than one <StatusMessage> element is provided, the messages are natural-language equivalents of each other; in this case, the xml:lang attribute SHOULD be provided on each element.

```
<element name="StatusMessage">
  <complexType>
    <simpleContent>
      <extension base="string">
        <attribute name="xml:lang" type="language"/>
      </extension>
    </simpleContent>
  </complexType>
</element>
```

I prefer this option because it has less markup overhead, as long as the multiple <StatusMessage> elements already allowed in the schema weren't intended to have some other meaning instead (in which case, that meaning needs to be documented). If they weren't, then if this option *isn't* picked, I think we need to shut down multiple occurrences of <StatusMessage>, changing it to minOccurs="0" and maxOccurs="1".

==========

Colors: Gray Blue Yellow

Option 2: One StatusMessage element, with partitioned content indicating language

This option isn't all that different from option 1. It would invent a new subelement to go into the content of <StatusMessage> like so:

<StatusMessage>

A natural-language message explaining the status in a human-readable way. It contains one or more <MessageText> elements, each providing different natural-language equivalents of the same message.

```
<element name="StatusMessage" type="StatusMessageType" />
<complexType name="StatusMessageType">
  <sequence>
    <element ref="MessageText" maxOccurs="unbounded" />
  </sequence>
</complexType>
```

<MessageText>

The text of the status message. If more than one <MessageText> element is provided, the messages are natural-language equivalents of each other; in this case, the xml:lang attribute SHOULD be provided on each element.

```
<element name="MessageText">
  <complexType>
    <simpleContent>
      <extension base="string">
        <attribute name="xml:lang" type="language"/>
      </extension>
    </simpleContent>
  </complexType>
</element>
```

I think this option is necessary *if* multiple occurrences of <StatusMessage> were already intended to have some other meaning. If they weren't, then I prefer option 1.

==========

Digression on xml:lang

You can read about this attribute here:

Brief description of the xml: namespace:

http://www.w3.org/XML/1998/namespace.html

Section of the XML spec itself that defines xml:lang:

http://www.w3.org/TR/REC-xml#sec-lang-tag

There is also a non-normative but helpful schema module that defines the items in the xml: namespace. You can find it here:

http://www.w3.org/XML/1998/namespace.xsd

This schema module can be useful if you want to slurp those definitions into the SAML schemas to make sure that SAML instances can be fully validated. Alternatively, we can legally cook up our own schema code for this as shown in the two options above, which would avoid importing another schema module into both of ours, with attendant code and documentation. If we do that, note that we'll still need to declare the xml: namespace at the tops of our schema modules.

==========

Final thoughts

Even if the issue of multiple-language support is deferred until a future release, I believe that <StatusMessage> and the fact that it's repeatable is underspecified at the moment. I would like

Colors: Gray Blue Yellow

to see it restricted to an optional single occurrence, or alternatively, I would like to have its semantics explained when multiple occurrences are used. This can be listed as a separate issue if you like.

http://lists.oasis-open.org/archives/security-services/200201/msg00265.html

Resolution Alternatives: ???

3.14.3 CLOSED ISSUE:[DS-14-15: Version Synchronization]

Source: V1.0 Deferred Issue

Champion: Rob Philpott

Status: 25-Jun-2003 – This issue was resolved in V1.1

Status: 9-Apr-2002 – Deferred by vote.

Description: What is the relationship between the version of the Assertions, Requests and Responses? Should the values always be the same or can they change independently of each other?

Resolution Alternatives:

1. Requests and Responses each have Major/Minor version info attributes, which implies that, in theory, they could be upgraded independently (I didn't see where this is explicitly prohibited). If so, Line 1228-1229 should be explicit: "This document defines SAML Assertions 1.0, SAML Request Protocol 1.0, and SAML Response Protocol 1.0".
2. If the intent is to keep the request and response protocols synchronized with a single SAML protocol version (separate from the assertion version), then the RequestAbstractType type (3.2.1) and the ResponseAbstractType type (3.4.1) should replace the MajorVersion and MinorVersion attributes with a new <ProtocolVersionInfo> element defined something like:

```
<element name="ProtocolVersionInfo" type="samlp:ProtocolVersionInfoType"/>
<complexType name="ProtocolVersionInfoType">
    <attribute name="MajorVersion" type="integer" use="required"/>
    <attribute name="MinorVersion" type="integer" use="required"/>
</complexType>
```

3. If the intent is to keep the version info synchronized for assertions, request protocol, and response protocol, then we could use the following in the <assertion> element (2.3.3) and the request/response abstract types could include the <VersionInfo> element:

```
<element name="VersionInfo" type="saml: VersionInfoType"/>
<complexType name="VersionInfoType">
        <attribute name="MajorVersion" type="integer" use="required"/>
        <attribute name="MinorVersion" type="integer" use="required"/>
</complexType>
```

The above alternatives were taken from: http://lists.oasis-open.org/archives/security-services/200201/msg00163.html.

[25-Jun-2003] The adopted resolution in V1.1 was to clarify via specification text rather than schema changes. The spec now requires Protocol versions in Request and Response messages to be synchronized. Assertion versions may deviate from Protocol versions. See V1.1 spec for details.

Colors: Gray Blue Yellow

3.14.4 DEFERRED ISSUE:[DS-14-16: Version Positive]

Source: V1.0 Deferred Issue

Champion: Eve Maler

Status: 9-Apr-2002 – Deferred by vote.

Description: It is intended that Major and Minor version numbers must be positive. It was discussed that this could be enforced by using facets. We would want to make a VersionNumberType simple type for this.

This issue was identified as Low Priority Issue - L2 from Sun.

http://lists.oasis-open.org/archives/security-services/200202/msg00012.html

Resolution Alternatives: ???

3.15 Group 15: Elements Expressing Time Instants

Highest V1.0 Issue Number: DS-15-03

No deferred or new issues.

Colors: Gray Blue Yellow

4 Miscellaneous Issues

4.1 Group 1: Terminology

Highest V1.0 Issue Number: MS-1-03

No deferred or new issues.

4.2 Group 2: Administrative

Highest V1.0 Issue Number: MS-2-02

No deferred or new issues.

4.3 Group 3: Conformance

Highest V1.0 Issue Number: MS-3-03

No deferred or new issues.

4.4 Group 4: XMLDSIG

Highest V1.0 Issue Number: MS-4-02

No deferred or new issues.

4.5 Group 5: Bindings

Highest V1.0 Issue Number: MS-5-08

4.5.1 DEFERRED ISSUE:[MS-5-08: Publish WSDL]

Source: V1.0 Deferred Issue

Champion: Eve Maler

Status: 19-Mar-2002 – Deferred by vote. Needs more review and a decision where to publish it.

Description: Publish Irving's WSDL for SAML 1.0, even if it is non-normative. Where? Perhaps in Bindings doc? This is ELM-8 in:

http://lists.oasis-open.org/archives/security-services/200203/msg00042.html

Resolution Alternatives: ???

Colors: Gray Blue Yellow

5 References

5.1 Normative

[RFC2119] S. Bradner, *Key words for use in RFCs to Indicate Requirement Levels*, http://www.ietf.org/rfc/rfc2119.txt, IETF RFC 2119, March 1997.

[ISSUES-1.0] H.Lockhart, *Security Assertions Markup Language Issues List Version 12*, http://www.oasis-open.org/committees/security/, OASIS, April 16, 2002.

Colors: Gray Blue Yellow

Appendix 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:

- Frank Siebenlist, Argonne National Laboratory
- Irving Reid, Baltimore Technologies
- Hal Lockhart, BEA Systems
- Steven Lewis, Booz Allen Hamilton
- John Hughes, Entegrity Solutions
- Carlisle Adams, Entrust
- Jason Rouault, HP
- Maryann Hondo, IBM
- Anthony Nadalin, IBM
- Scott Cantor, Individual
- Bob Morgan, Individual
- Trevor Perrin, Individual
- Padraig Moloney, NASA
- Prateek Mishra, Netegrity (co-chair)
- Frederick Hirsch, Nokia
- Senthil Sengodan, Nokia
- Timo Skytta, Nokia
- Charles Knouse, Oblix
- Steve Anderson, OpenNetwork
- Simon Godik, OverXeer
- Rob Philpott, RSA Security (co-chair)
- Dipak Chopra, SAP
- Jahan Moreh, Sigaba
- Bhavna Bhatnagar, Sun Microsystems
- Jeff Hodges, Sun Microsystems
- Eve Maler, Sun Microsystems (coordinating editor)
- Emily Xu, Sun Microsystems
- Phillip Hallam-Baker, VeriSign

Colors: Gray Blue Yellow

936 # Appendix B. Revision History

Rev	Date	By Whom	What
Draft-01	200-06-24	Rob Philpott	Initial draft for SAML V1.1

937

Colors: Gray Blue Yellow

Appendix 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.

Colors: Gray Blue Yellow