Errata for the OASIS SAML 1.1 Committee Specifications

Working Draft 04, 18 March 2003

Document identifier:

TBD

Location:

http://www.oasis-open.org/committees/security/docs/

Editor:

Jahan Moreh, Sigaba <jmoreh@sigaba.com>

Abstract:

This document lists the reported potential errata against the OASIS SAML 1.1 Committee Specifications and their status.

Status:

This document will be updated alongside the SAML Committee Specifications until such time as the specifications are frozen against editorial changes and sent to the OASIS membership for voting.

Comments on issues with the SAML specifications are welcome. If you are on the security-services@lists.oasis-open.org list for committee members, send comments there. If you are not on that list, subscribe to the security-services-comment@lists.oasis-open.org list and send comments there. 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. If you have questions or comments on implementation issues, subscribe to the saml-dev@lists.oasis-open.org list and send comments there.

Table of Contents

1 Introduction

This document lists the reported errata against the OASIS SAML V1.1 release 00 Committee Specifications and their status..

2 Errata

2.1 E1: Section number inconsistencies

First reported by: Fredrick Hirsch, Nokia

Message: **http://lists.oasis-open.org/archives/security-services/200212/msg00000.html**

Document: Bindings and Profiles

Description: section numbers for the SOAP over HTTP need to be updated, namely 3.1.3.2 on line [258] for authentication, 3.1.3.3 on line [263] for integrity and 3.1.3.4 on line [267] for confidentiality

Options:

Disposition: Accepted for correction during TC meeting on 2/18/03.

2.2 E2: Typo

First reported by: Fredrick Hirsch

Message: http://lists.oasis-open.org/archives/security-services/200212/msg00000.html

Document: Bindings and Profiles

Description: There is an extra backslash on line 831.

Options:

Disposition: Accepted for correction during TC meeting on 2/18/03.

2.3 E3: Section Formatting

First reported by: Rob Philpott

Message: http://lists.oasis-open.org/archives/security-services/200301/msg00016.html

Document: Bindings and Profiles

Description: Line 291: The section number is not bolded as are all other section numbers.

Options:

1. Change formatting

Disposition: Accepted for correction during TC meeting on 2/18/03.

2.4 E4: Font Inconsistencies

First reported by: Rob Philpott

Message: **http://lists.oasis-open.org/archives/security-services/200301/msg00014.html**

Document: Assertions and Protocols

Description: Lines 722, 726: The font for the “Location” and “Binding” attributes is different from “AuthorityKind” on line 714.

Options:

1. Change formatting of line 714

Disposition: Accepted for correction during TC meeting on 2/18/03.

2.5 E5: Spelling errors

First reported by: Rob Philpott

Message: http://lists.oasis-open.org/archives/security-services/200301/msg00014.html

Document: Assertions and Protocols

Description: Line 887: interger should be integer

Options:

Correct spelling error

Disposition: Accepted for correction during TC meeting on 2/18/03.

2.6 E6: Spelling errors

First reported by: Prateek Mishra

Message: http://lists.oasis-open.org/archives/security-services/200302/msg00022.html

Document: Assertions and Protocols

Description: Line 1441 is in error and should be removed from this list.

Lines 1439-1444 state:

The following elements are intended specifically for use as extension points
in an extension schema; their 1439
types are set to abstract, so that the use of an xsi:type attribute with
these elements is REQUIRED: 1440
* <Assertion> 1441
* <Condition> 1442
* <Statement> 1443
* <SubjectStatement> 1444

An examination of the schema reveals that <Assertion> is of type
<AssertionType> which is a concrete type. Thus there is no requirement
that an xsi:type attribute must be used with assertions.

Options:

Correct error

Disposition: Accepted for correction during TC meeting on 2/18/03.

3 Potential Errata

.

3.1 PE1: HTTPS for inter-site transfer service and artifact transmission

First reported by: Fredrick Hirsch, Nokia

Message: http://lists.oasis-open.org/archives/security-services/200212/msg00000.html

Document: Bindings and Profiles

Description: Since SSL/TLS is recommended for inter-site transfer and artifact transmission, perhaps https should be shown in the examples at line [443], [483].

Options:

Disposition: Agreed to change it at TC meeting 2/18/03

3.2 PE2: clarify the expectations of SubjectConfirmationData

First reported by: Fredrick Hirsch

Message: http://lists.oasis-open.org/archives/security-services/200212/msg00000.html

Document: Bindings and Profiles

Description: It might be helpful to clarify the expectations of `SubjectConfirmationData` and `ds:KeyInfo` usage for the different `ConfirmationMethods` in this profile. Is it true that only holder-of-key would be expected to have a `ds:KeyInfo SubjectConfirmation` element (For the assertion subject), and none would have `SubjectConfirmationData`?

Options:

1. Reject. The Holder-of-Key case is not involved in any of the web browser profiles. The Browser/Artifact profile does not require the use of `SubjectConfirmationData` or `ds:KeyInfo`.
2. 2/18/03: Add supplementary text to explain use of <SubjectConfrimationData>

Disposition:

3.3 PE3: Bearer and Holder of Key in POST profile

First reported by: Fredrick Hirsch

Message: http://lists.oasis-open.org/archives/security-services/200212/msg00000.html

Document: Bindings and Profiles

Description: Presumably the Bearer method would have a ds:KeyInfo element as part of the SAML response signature, but this is separate from ConfirmationMethod.

Options:

1. Reject. While there is a requirement that the SAML response message must be signed (694-695) there is no implication that the included assertions contain ds:KeyInfo element
2. 2/18/03: Add supplementary text to explain use of <SubjectConfrimationData>

Disposition:

3.4 PE4: Encoding of URI in “Alternative SAML Artifact Format”

First reported by: Yuji Sakata and Juergen Kremp

Message: http://lists.oasis-open.org/archives/security-services/200212/msg00002.html

Document: Bindings and Profiles

Description: chapter 9 of the Bindings document introduces an alternative format for the Assertion Artifact:

TypeCode := 0x0002

RemainingArtifact := AssertionHandle SourceLocation

AssertionHandle := 20-byte_sequence

SourceLocation := URI

To create the artifact, Base64 is to be applied to the concatenation of TypeCode and RemainingArtifact. Base64 uses Bytes as input.

Options:

1. Specify UTF-8 as default character set
2. ??

Disposition: 2/18/03 – during meeting of TC it was decided to correct this. Prateek to propose text changes.

3.5 PE5: Signing Assertions

First reported by: Ronald Monzillo

Message: http://lists.oasis-open.org/archives/security-services/200212/msg00003.html

Document: Assertions and Protocols

Description: Section 5, lines [1382-1387] indicate that a SAML assertion MUST be signed. The intent here is to strongly advocate the use of signature when assertions are passing through intermediaries. The use of "MUST" here is inappropriate, this is really only advice for profile developers.

Options:

1. Change the specification to read "MAY"
2. Change the specification to read "SHOULD"
3. ??

Disposition: 2/18/03 – during meeting of TC it was decided to correct this to "SHOULD".

3.6 PE6: Artifact and corresponding confirmation method

First reported by: Rob Philpott

Message: http://lists.oasis-open.org/archives/security-services/200301/msg00016.html

Document: Profiles and Bindings

Description: Section 5.3: Even though it isn't explicitly stated, I have been assuming that the "...:cm:artifact-01" refers to a type 1 artifact. If so, doesn't there need to be a corresponding confirmation method identifier for "...:cm:artifact-02"? Is there really a need to distinguish the artifact types (i.e. "just use "...:cm:artifact")? We should also be explicit as to whether providing the actual artifact in the ConfirmationData is required, optional, or not permitted – Which is it?

Options:

1. Strike artifact-01
2. Add confirmation method identifier "….artificat-02"

3. Add a confirmation method ID (artifact) and indicate that either one can be used for 01, 03, or any other future.

Disposition: 2/18/03 – during meeting of TC it was decided to choose option 3

3.7 PE7: Normative Language

First reported by: Rob Philpott

Message: http://lists.oasis-open.org/archives/security-services/200301/msg00014.html

Document: Assertions and Protocols

Description: Line 961: change "may" to "MAY".

Line 966: change "success would normally" to "Success MUST".

Line 971: Change "must" to "MUST".

Line 1237: Change subcodes MAY be to "subcodes may be"

Options:

Disposition: 2/18/03 – during meeting of TC it was decided to choose correct 966. Line 971 remains as is because it was an example. Line 1237 also remains unchanged.

3.8 PE8: non-Normative Language

First reported by: Rob Philpott

Message: http://lists.oasis-open.org/archives/security-services/200301/msg00014.html

Document: Assertions and Protocols

Description: Line 967: change "to be found therein" to "will be included" **.**

Line 1219: Change "request. Top-most" to "request. The top-most"

Line 1417: Change "REQUIRES" to "requires"

Options:

Disposition: 2/18/03 – during meeting of TC it was decided to choose correct 967 and 1219. Keep 1417 as is.

3.9 PE9: Reference to AuthorityKind

First reported by: Rob Philpott

Message: http://lists.oasis-open.org/archives/security-services/200301/msg00014.html

Document: Assertions and Protocols

Description: Lines 969-970: "exactly as for saml:AuthorityKind attribute; see Section 2.4.3.2" – The AuthorityKind section is referring to samlp:Query references not saml:Statement references. Folks read the reference to AuthorityKind and sometime try to figure out a relationship between RespondWith and AuthorityKind, which of course does not exist. The section reference is intended to highlight the use of saml and samlp Qnames. Also, AuthorityKind is an attribute, while RespondWith is an element, so the methods for specifying the values are different. I recommend removing the section reference and simply insert similar text inline.

Options:

Disposition: 2/18/03 – during meeting of TC it was decided to dispose of this PE as suggested. Rob to propose replacement text.

3.10 PE10: Guidance on Element <RespondWith>

First reported by: Rob Philpott

Message: http://lists.oasis-open.org/archives/security-services/200301/msg00014.html

Document: Assertions and Protocols

Description: Should provide better guidance on rationalizing use of RespondWith elements in a query and the associated Query type. I know there's been some discussion on this topic on the list, but I don't think the current text here is very clear. For example, we should be explicit about what happens on an AuthenticationQuery that includes a RespondWith for a saml:AttributeStatement. Another example is when an authority has an existing Web SSO assertion that contains both AuthenticationStatements and an AttributeStatement (e.g. what we used in the Interop). Now if a later AuthenticationQuery arrives for the SAML Subject with a RespondWith of saml:AuthenticationStatement, this Web SSO assertion should NOT be returned according to lines 963-964. So we should be explicit that if an assertion contains multiple statement types, there must be a RespondWith in the query for every statement type in the assertion (assuming at least one RespondWith is specified).

Options:

Disposition: 2/18/03 – during meeting of TC it was decided to send an email to the list to discuss this. Jahan will send email to the list starting the discussion.

3.11 PE11: Processing rules for AssertionIDReference

First reported by: Rob Philpott

Message: http://lists.oasis-open.org/archives/security-services/200301/msg00014.html

Document: Assertions and Protocols

Description: Section 3.2 (Requests) – Section 3.3 (Queries) provides not only definitions of query elements, it also provides processing rules and interpretation info for the Queries. But we don't do that for the <AssertionArtifact> or <AssertionIDReference> request types. Section 3.2.3 defines the <AssertionArtifact> element but doesn't say how it is used (of course this is discussed in the Profiles). There is no section describing the RequestType "saml:AssertionIDReference" here since the element is defined in section 2.3.1. When someone asked me why AssertionIDReference wasn't described, I at first thought it was an omission since all of the other request and query types are discussed in 3.2 and 3.3. Then I realized the saml/samlp distinction. But it might be clearer and avoid questions if there was a brief mention of processing rules for AssertionIDReference.

Options:

Disposition:

3.12 PE12: Miscellaneous additions and clarifications

First reported by: Rob Philpott

Message: http://lists.oasis-open.org/archives/security-services/200301/msg00014.html

Document: Assertions and Protocols

Description:

Lines 1061-1065: In addition to subject and authn method matching rules, we should indicate that the assertion processing rules are also impacted by the presence of RespondWith elements in the Query.

Section 3.3.4 AttributeQuery – Should also mention the subject-matching rules as described in section 3.3.3

Line 1085: “the start of the current document” – In a query, the samlp:Request is the **current** document, so what does it mean to use a Resource with an empty URI?

Section 3.3.5 AuthorizationDecisionQuery – Should also mention the subject-matching rules as described in section 3.3.3

3.13 PE13: Miscellaneous additions and clarifications

First reported by: Rob Philpott

Message: http://lists.oasis-open.org/archives/security-services/200301/msg00014.html

Document: Assertions and Protocols

Description:

Section 3.4.4 (Responses to <AuthnQuery> and <AttrQuery>) – Don’t the saml:Subject matching rules described in this section also apply to <AuthzQuery>? In fact, I assume the rules should apply to all <SubjectQuery> requests, including and extensions. So I think the section should be more general.

Section 5.4.2 (C14n) – We should mention the preference for Exclusive C14N and refer to the external Dsig Guidelines document.

3.14 PE14: Requestor vs. Requester and glossary definition for Responder

First reported by: Rob Philpott

Message: http://lists.oasis-open.org/archives/security-services/200302/msg00014.html

Document: Assertions and Protocols

Description: In core, we use both spellings. The only normative use is in the definition of <Status> where it the “requester” spelling is used. I recommend we change all “requestor” spellings to “requester”. If folks want to use the “requestor” spelling, then it would be an issue since it introduces a compatibility issue with the current spec. Note that the glossary uses the “Requester” spelling”. There are about 15 uses of “requestor” in core, although one of them is in the references section pointing to “*The Kerberos Network Authentication Requestor (V5)*” that we wouldn’t want to change.

Also – we need to add a definition for “Responder” to the glossary. We use it in the specs. I’ll provide a first shot at it (based on Requester):

Responder – A *system entity* that utilizes a protocol to respond to a request for services from another system entity. The term “server” for this notion is not used because many system entities simultaneously or serially act as both clients and servers.

Options:

Disposition:

3.15 PE15: Browser POST profile does not explicitly call out encoding

First reported by: Jon Westbrock, Emerson Process Management

Message: sent to saml-dev list

Document: Profiles and Bindings

Description: In step 2 of this profile, the base64 encoding of a SAML response is embedded in a HTML form. In order to do this you must first serialize the SAML response to a sequence of octets, which can then be base64 encoded. What character encoding is supposed to be used to serialize the SAML response to a sequence of octets? lines 692-694 of the bindings document it appears that we haven't explicitly called out the use of UTF-8. This seems to be standard technique used, for example, in c14n canonicalization.

Options: Explicitly call-out UTF-8 encoding

Disposition:

Appendix A. Revision History

Rev	Date	By Whom	What
Draft-00	2002-12-10	Jahan Moreh	Initial version based on emails to the list
Draft-01	2003-01-22	Jahan Moreh	Additions from Rob Philpott
Draft-02	2003-02-14	Jahan Moreh	Additions from Prateek Mishra
Draft-03	2003-02-18	Jahan Moreh	Updated based on discussions during SSTC meeting of 2/18/03.
Draft-04	2003-03-18	Jahan Moreh	Updated based on a message from Jon Westbrock and Prateek's response to that message

Appendix B. 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.