Errata for the OASIS Security Assertion Markup Language (SAML) V1.1

Working Draft 14, 30 June 2003

Document identifier: sstc-saml-errata-1.1-draft-14
Editor: Jahan Moreh, Sigaba <jmoreh@sigaba.com>
Abstract: This document lists the reported errata and 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.

Copyright © 2003 The Organization for the Advancement of Structured Information Standards [OASIS]
Table of Contents

28

1 Introduction ..............................................................................................................................3
2 Errata .......................................................................................................................................3
2.1 E1: Section number inconsistencies ......................................................................................3
2.2 E2: Typo ................................................................................................................................3
2.3 E3: Section Formatting ..........................................................................................................3
2.4 E4: Font Inconsistencies ......................................................................................................3
2.5 E5: Spelling errors .................................................................................................................4
2.6 E6: Spelling errors .................................................................................................................4
2.7 E7: Normative use of MAY NOT ..........................................................................................4
2.8 E8: Extension types for <RespondWith> ...............................................................................5
2.9 E9: Incorrect identifier for alternative SAML Artifact Format .................................................5
3 Potential Errata ........................................................................................................................5
3.1 PE1: HTTPS for inter-site transfer service and artifact transmission ....................................5
3.2 PE2: Clarify the expectations of SubjectConfirmationData ...................................................6
3.3 PE3: Bearer and Holder of Key in POST profile ..................................................................6
3.4 PE4: Encoding of URI in “Alternative SAML Artifact Format” .............................................6
3.5 PE5: Signing Assertions ........................................................................................................7
3.6 PE6: Artifact and corresponding confirmation method ..........................................................7
3.7 PE7: Normative Language .....................................................................................................8
3.8 PE8: non-Normative Language .............................................................................................8
3.9 PE9: Reference to AuthorityKind ..........................................................................................8
3.10 PE10: Guidance on Element <RespondWith> .................................................................8
3.11 PE11: Processing rules for AssertionIDReference .............................................................9
3.12 PE12: Miscellaneous additions and clarifications .................................................................9
3.13 PE13: Miscellaneous additions and clarifications ...............................................................10
3.14 PE14: Requestor vs. Requester and glossary definition for Responder ............................10
3.15 PE15: Browser POST profile does not explicitly call out encoding .....................................11
3.16 PE16: Use of Qnames in <AuthorityKind> and <RespondWith> ......................................11
3.17 PE17: Non-normative clarification of status code ...............................................................12
3.18 PE18: SAML Versioning .....................................................................................................12
3.19 PE19: Clarification of status code for the case of no assertion ...........................................13
3.20 PE20: Description of <ConfirmationData> in Browser/POST ........................................13
3.21 PE21: Clarification of the AuthenticationMethod attribute in <AuthenticationQuery> ......14
3.22 PE22: Clarification of AuthenticationMethod attribute .....................................................14
3.23 PE23: Clarification of <Statement>, <SubjectStatement> and Nested Assertions ..........15

Appendix A. Revision History .........................................................................................................16
Appendix B. Summary of Disposition .............................................................................................17
Appendix C. Notices .......................................................................................................................18
1 Introduction
This document lists the reported errata and potential errata against the OASIS SAML 1.1 Committee Specifications and their status.

2 Errata

2.1 E1: Section number inconsistencies
First reported by: Fredrick Hirsch, Nokia
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: Make corrections as suggested.
Disposition: Accepted for correction during TC meeting on 2/18/03. Incorporated in Draft 01 of SAML 1.1 Bindings and Profiles.

2.2 E2: Typo
First reported by: Fredrick Hirsch, Nokia
Document: Bindings and Profiles
Description: There is an extra backslash on line 831.
Options: Make corrections as suggested.
Disposition: Accepted for correction during TC meeting on 2/18/03. Incorporated in Draft 01 of SAML 1.1 Bindings and Profiles.

2.3 E3: Section Formatting
First reported by: Rob Philpott, RSA Security
Document: Bindings and Profiles
Description: Line 291: The section number is not bolded as are all other section numbers.
Options: Change formatting
Disposition: Accepted for correction during TC meeting on 2/18/03. Incorporated in Draft 01 of SAML 1.1 Bindings and Profiles.

2.4 E4: Font Inconsistencies
First reported by: Rob Philpott, RSA Security
Document: Assertions and Protocols
Description: Lines 722, 726: The font for the “Location” and “Binding” attributes is different from “AuthorityKind” on line 714.
2.5 E5: Spelling errors

First reported by: Rob Philpott, RSA Security


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. Incorporated in Draft 02 of SAML 1.1 Assertions and Protocols.

2.6 E6: Spelling errors

First reported by: Prateek Mishra, Netegrity


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. Incorporated in Draft 02 of SAML 1.1 Assertions and Protocols.

2.7 E7: Normative use of MAY NOT

First reported by: Eve Maler, Sun Microsystems


Document: Assertions and Protocols

Description: There are two instances of the phrase “MAY NOT” in the core spec (lines 1050 and 1258). This phrase is not actually defined by RFC 2119; it is likely that what was meant was “MUST NOT”. For this reason, and because “may not” is a classic ambiguous phrase in technical documentation (“don’t do this”, as opposed to “you may or may not do this”), it is recommend that we change it to “MUST NOT” in both locations.

Options: Change lines 1050 and 1258 from MAY NOT to MUST NOT.
2.8 E8: Extension types for <RespondWith>

First reported by: Eve Maler, Sun Microsystems


Document: Assertions and Protocols

Description: In core 1.0 lines 971-973, it says: “To specify extension types, the <RespondWith> element MUST contain exactly the extension element type as specified in the xsi:type attribute on the corresponding element.”

There is a tiny bit of ambiguity in the sentence as it stands. The phrase “element type”, to XML DTD old-timers, means roughly an element declaration – it’s a model for element instances. With the advent of XML Schema and its OO-inspired design, we now have real “types” to which element declarations are bound. The xsi:type reference makes clear that what’s meant is the type name, not the element name, but it threw me off.

Given this, we have a seemingly inconsistent situation. When the statement is a native SAML element, the content of <RespondWith> is a qualified element name. But when the statement is a foreign extension element, the qualified type name has to be supplied instead.

Options: Fix the almost-ambiguity in V1.1 by saying “element’s type” rather than “element type”, and treat this as an editorial correction.

Disposition: Accepted during TC meeting of April 08, 2003. Incorporated in Draft 03 of SAML 1.1 Assertions and Protocols.

2.9 E9: Incorrect identifier for alternative SAML Artifact Format

First reported by: Rob Philpott, RSA Security


Document: Assertions and Protocols

Description: Line 941, lists the identifier for the alternative SAML Artifact Format as “urn:oasis:names:tc:SAML:1.0:draft-sstc-bindings-model-13:profiles:artifact-02”. The urn should be “urn:oasis:names:tc:SAML:1.0:profiles:artifact-02” to be consistent with the type 1 artifact profile.

Options: Make editorial correction.

Disposition: Make editorial correction as stated above. Incorporated in Draft 03 of SAML 1.1 Bindings and Profiles.

3 Potential Errata

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

First reported by: Fredrick Hirsch, Nokia


Document: Assertions and Protocols
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: Use https in the examples.

Disposition: Agreed to change it at TC meeting 2/18/03. Incorporated in Draft 01 of SAML 1.1 Bindings and Profiles.

3.2 PE2: Clarify the expectations of SubjectConfirmationData

First reported by: Fredrick Hirsch, Nokia


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.

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 <SubjectConfirmationData>

Disposition: April 01 TC meeting: TC voted to choose option 1.

3.3 PE3: Bearer and Holder of Key in POST profile

First reported by: Fredrick Hirsch, Nokia


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 <SubjectConfirmationData>

Disposition: April 01 TC meeting: TC voted to choose option 1.

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

First reported by: Yuji Sakata, and Juergen Kremp, SAP


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. Text proposed by Prateek on 18 April 2003: Insert at end of sentence on line 951:
The SourceLocation URI is mapped to a sequence of bytes based on use of the UTF-8
[RFC2279] encoding. Add to reference list: RFC 2279 UTF-8, a transformation
format of ISO 10646.
Disposition: 2/18/03 – during meeting of TC it was decided to correct this. Prateek to
propose text changes. During TC meeting of April 22, 2003 SSTC accepted text as
proposed by Prateek (option 2 above). Incorporated in Draft 02 of SAML 1.1 Bindings and
Profiles.

3.5 PE5: Signing Assertions
First reported by: Ronald Monzillo, Sun Microsystems
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”
Disposition: 2/18/03 – during meeting of TC it was decided to correct this to “SHOULD”.
Incorporated in Draft 02 of SAML 1.1 Assertions and Protocols.

3.6 PE6: Artifact and corresponding confirmation method
First reported by: Rob Philpott, RSA Security
Document: Bindings and Profiles
Description: Section 5.3: Even though it isn’t explicitly stated, one would assume 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 “....artifact-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.
Incorporated in Draft 02 of SAML 1.1 Assertions and Protocols.
4/29/03 – It was decided that to deprecate artifact-01 and simply use artifact. After line 528
of protocols and bindings add a brief normative note: SAML authorities SHOULD NOT
include SAML artifact in a Confirmation Data. Incorporated in Draft 03 of Binding and Profiles.

### 3.7 PE7: Normative Language

- **First reported by:** Rob Philpott, RSA Security
- **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.
  - Incorporated in Draft 02 of SAML 1.1 Assertions and Protocols.

### 3.8 PE8: non-Normative Language

- **First reported by:** Rob Philpott, RSA Security
- **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. Incorporated in Draft 02 of SAML 1.1 Assertions and Protocols.

### 3.9 PE9: Reference to AuthorityKind

- **First reported by:** Rob Philpott, RSA Security
- **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 sampl: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 sampl Qnames. Also, AuthorityKind is an attribute, while RespondWith is an element, so the methods for specifying the values are different. It is recommended that we remove 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. Incorporated in Draft 06 of SAML 1.1 Assertions and Protocols.

### 3.10 PE10: Guidance on Element <RespondWith>

- **First reported by:** Rob Philpott, RSA Security

Document: Assertions and Protocols

Description: Should provide better guidance on rationalizing use of RespondWith elements in a query and the associated Query type. There has been some discussion on this topic on the list, but the current text here is not 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: 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.

Disposition: In light of the decision to deprecate <RespondWith> it was decided to not make any changes.

3.11 PE11: Processing rules for AssertionIDReference

First reported by: Rob Philpott


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 asks why AssertionIDReference wasn’t described, at first one would think it was an omission since all of the other request and query types are discussed in 3.2 and 3.3. Then one would realize the saml/samlp distinction. But it might be clearer and avoid questions if there was a brief mention of processing rules for AssertionIDReference.

Options: Provide additional text to clarify as follows:

3.2.2.1 Requests for Assertions by Reference

In the context of a <Request> element, the <saml:AssertionIDReference> element is used to request an assertion by means of its ID. See Section 2.3.1 for more information on this element.

3. Element <AssertionArtifact>

The <AssertionArtifact> element is used to specify the assertion artifact that represents an assertion being requested. Its use is governed by the specific profile of SAML that is being used; see the SAML specification for bindings and profiles [SAMLBind] for more information on the use of assertion artifacts in profiles. The following schema fragment defines the <AssertionArtifact> element: <element name="AssertionArtifact" type="string"/>

Disposition: Accepted during TC meeting of April 08. Already incorporated in Draft 03 of SAML 1.1 Assertions and Protocols.

3.12 PE12: Miscellaneous additions and clarifications

First reported by: Rob Philpott, RSA Security


Document: Assertions and Protocols
Description:

1. 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.

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

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

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

Options: for (1), (2), (4) add cross reference in the respective sections to clarify. For (3) add text to strongly discourage use of empty URIs.

Disposition: April 01 TC meeting: Eve will make editorial changes. Incorporated in Draft 03 of SAML 1.1 Assertions and Protocols.

3.13 PE13: Miscellaneous additions and clarifications

First reported by: Rob Philpott, RSA Security


Document: Assertions and Protocols

Description:

1. 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, one could assume that the rules should apply to all <SubjectQuery> requests, including and extensions. Therefore, the section should be more general.

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

Options:

Disposition: April 01 TC meeting: For (1) see items 1, 2, and 4 in PE 12 (Eve will make editorial changes). Incorporated in Draft 03 of SAML 1.1 Assertions and Protocols.

For (2), Scott to propose text. Incorporated in Draft 06 of SAML 1.1 Assertions and Protocols.

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

First reported by: Rob Philpott


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. It is recommended that 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. The definition for Responder could be:
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: April 01 TC meeting: Use “Requester” throughout. Add “SAML Requester and SAML Responder”. Incorporated in Draft 03 of SAML 1.1 Assertions and Protocols.

Also reviewed SOAP definitions for “Requester” and “Responder” and modified as appropriate. Incorporated in Draft 01 of SAML 1.1 Glossary

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

First reported by: Jon Westbrook, Emerson Process Management


Document: Bindings and Profiles

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:

1. Explicitly call-out UTF-8 encoding

2. Reject based on the following reason. On reviewing the XML specification, it turns out that the issue of specifying and determining the character encoding of XML documents has been completely addressed therein. http://www.w3.org/TR/REC-xml#charencoding. My reading of this text suggests that SAML does not need to take a position on this issue and no additional text is required in the Browser/POST profile.

3. Adopt the following text as proposed by Scott: On line 692, replace the current sentence with this text:

   The notation B64(<response>) stands for the result of applying the Base64 Content-Transfer-Encoding to the response, as defined by RFC 1521, section 5.2, and SHOULD consist of lines of encoded data of up to 76 characters. The first encoded line begins after the opening quote signifying the “value” attribute of the SAMLResponse form element.

   The character set used to represent the encoded data is determined by the “charset” attribute of the Content-Type of the HTML document containing the form. The character set of the XML document resulting from decoding the data is determined in the normal fashion, and defaults to UTF-8 if no character set is indicated.

Disposition: April 08 TC meeting: Review proposal by Scott. April 22 TC meeting, adopted text by Scott as describe in option 3 above. Incorporated in Draft 02 of SAML 1.1 Bindings and Profiles.

3.16 PE16: Use of Qnames in <AuthorityKind> and <RespondWith>

First reported by: Eve Maler, Sun Microsystems

Document: Assertions and Protocols

Description: Near lines 716 (all line references in this message are to core 1.0) for AuthorityKind, and 968 for RespondWith, the text gives an example of a Qname in use and unfortunately implies (rather more strongly in the latter case) that the prefix must read “saml” when a natively defined construct is being referenced. But the prefix of a namespaced value is never fixed, and we don’t clarify that the appropriate namespace must have been defined in the scope of the relevant element where the QName appears.

It would be better to say something like this (underscores around new or changed material):

For AuthorityKind: “For example, an attribute authority would be identified by AuthorityKind=”samlp:AttributeQuery”, _where there is a namespace declaration in the scope of this attribute that binds the samlp: prefix to the SAML protocol namespace_.”

For RespondWith: “For example, a requestor that wishes to receive assertions containing only attribute statements _would_ [this was a lowercase “must”] specify <RespondWith>saml:AttributeStatement</RespondWith>, _where the prefix is bound to the SAML assertion namespace in a namespace declaration that is in the scope of this element_.”

Options: Incorporate changes as described.

Disposition: Accepted during TC meeting on April 08, 2003. Incorporated in Draft 04 of SAML 1.1 Assertions and Protocols.

3.17 PE17: Non-normative clarification of status code

First reported by: Eve Maler, Sun Microsystems


Document: Bindings and profiles

Description: In reviewing the bindings doc for typographical inconsistencies in the treatment of status code stuff, I found this in Section 3.1.3.6 Error Reporting:

“In the case of a SAML processing error, the SOAP HTTP server MUST respond with “200 OK” and include a SAML-specified error description as the only child of the <SOAP-ENV:Body> element.”

Should we be putting Major Version etc. attributes on StatusCode along with Assertion, Request, and Response? If we did, we’d want to make them optional, with default values inherited from the nearest SAML ancestor, if any.

Options: Add text to clarify that a Response is sent with the StatusCode.


3.18 PE18: SAML Versioning

First reported by: Scott Cantor, Ohio State University and Internet 2

Document: All documents

Description: The SAML specification is versioned in several, independent ways. This leads to possible confusion. We should have a clear and consistent versioning specification.


Disposition: Accepted during TC meeting on April 15, 2003. Incorporated in Drafts 05 and 06 of SAML 1.1 Assertions and Protocols.

3.19 PE19: Clarification of status code for the case of no assertion

First reported by: Rob Philpott, RSA Security


Document: SAML 1.1 Bindings and Profiles, Draft 02

Description: Lines 505-507 (section 4.1.1.6) of the -02 draft B&P document states:

"If the source site is able to find or construct the requested assertions, it responds with a <samlp:Response> message with the requested assertions. Otherwise, it returns an appropriate status code, as defined within the selected SAML binding." This is not really clear and will probably be construed by the reader to mean either that a SAML error status code should be returned in a samlp:Response or that a SOAP fault error should be returned (assuming the "selected SAML binding" is SOAP over HTTPS).

We should clarify this as follows:

"If the source site is able to find or construct the requested assertions, it responds with a <samlp:Response> message with no assertions and a <samlp:StatusCode> element with the value Success."

Options: Make editorial change to clarify

Disposition: Adopted editorial change as suggested. Incorporated in Draft 03 of Bindings and Profiles

3.20 PE20: Clarification of <ConfirmationData> in Browser/POST

First reported by: Rob Philpott, RSA Security


Document: Bindings and Profiles

Description: Section 4.1.2.5 states that:

The <saml:ConfirmationMethod> element of each assertion MUST be set to urn:oasis:names:tc:SAML:1.0:cm:bearer. This absence of text regarding <saml:confirmationData> may lead to confusion.

We should clarify as follows:

Every subject-based statement in the assertion(s) returned to the destination site MUST contain a <saml:SubjectConfirmation> element. The <ConfirmationMethod> element in the <SubjectConfirmation> MUST be set to urn:oasis:names:tc:SAML:1.0:cm:bearer.
Additionally, section 4.1.1.6 should also be updated to reflect the same change for the Browser/Artifact, as follows:

Every subject-based statement in the assertion(s) returned to the destination site MUST contain a `<saml:SubjectConfirmation>` element as follows:

- The `<saml:ConfirmationMethod>` element MUST be set to either urn:oasis:names:tc:SAML:1.0:cm:artifact-01 (deprecated) or urn:oasis:names:tc:SAML:1.0:cm:artifact (RECOMMENDED).
- The `<SubjectConfirmationData>` element SHOULD NOT be specified.

Options: Make editorial change to clarify.

Disposition: Editorial change incorporated in Draft 03 of Bindings and Profiles. TC approval is expected at next available opportunity.

### 3.21 PE21: Description of the AuthenticationMethod attribute in `<AuthenticationQuery>`

**First reported by:** Rob Philpott, RSA Security


**Document:** Assertions and Protocols

**Description:** Draft 10 of Assertions and Protocols, lines 1114-1118 describing `AuthenticationQuery` states:

- This element is of type `AuthenticationQueryType`, which extends `SubjectQueryAbstractType` with the addition of the following element:
  
  - `<AuthenticationMethod>` [Optional]

  A filter for possible responses. If it is present, the query made is "What assertions containing authentication statements do you have for this subject with the supplied authentication method?"

- Lines 1123-1125 state:
  
  - If the `<AuthenticationMethod>` element is present in the query, at least one `<AuthenticationMethod>` element in the set of returned assertions MUST match. It is OPTIONAL for the complete set of all such matching assertions to be returned in the response.

- The problem is that the schema for `AuthenticationQueryType` defines "AuthenticationQuery" as an XML attribute of type anyURI. It is not defined as an element.

**Options:**

1. Make editorial change to state that `<AuthenticationMethod>` is an attribute not an element.
2. Make `<AuthenticationMethod>` an element and allow multiple occurrences of it in `<AuthenticationQuery>`.

**Disposition:** SSTC chose option 1 during its weekly conference call of 5/13. The SSTC concluded that this option is consistent with the usage of `<AuthenticationMethod>` in the rest of the specification. Change incorporated in draft 11 of Assertion and Protocols.

### 3.22 PE22: Clarification of AuthenticationMethod attribute

**First reported by:** Rob Philpott, RSA Security

Assertions and Protocols

Description: Draft 10 of Assertions and Protocols, section 7.1 uses the form <AuthenticationMethod>, which leads to it being interpreted as an element. We should modify the text to clearly indicate that AuthenticationMethod is an attribute. The proposed text is as follows:

The AuthenticationMethod attribute of an <AuthenticationStatement> and the <SubjectConfirmationMethod> element of a SAML subject perform different functions, although both can refer to the same underlying mechanisms. An authentication statement with an AuthenticationMethod attribute describes an authentication act that occurred in the past. The AuthenticationMethod attribute indicates how that authentication was done. Note that the authentication statement does not provide the means to perform that authentication, such as a password, key, or certificate.

Options: Make editorial change.

Disposition: Based on the disposition of PE21, the SSTC approved this editorial change via email exchanges. Incorporated in Draft 11.

3.23 PE23: Clarification of <Statement>, <SubjectStatement> and Nested Assertions

First reported by: John Kemp, Project Liberty


Document: Assertions and Protocols

Description:

Lines 324-326 note that three kinds of assertion are specified by SAML. When reading the schema, <Statement> and <SubjectStatement> are treated as if they might appear independently of these three kinds of assertion, which is not in fact the case - they are for extensions that specify additional kinds of assertion. It is recommended that this distinction be made clear in this introductory text.

2. Line 331 states that "Assertions have a nested structure". 'Nesting' implies that one assertion may be contained within another, which as far as I can tell from the schema is not possible. It is recommended that this sentence be changed to note that an "assertion acts as a container for a number of assertion statements" or some similar text.

Options: Make editorial change.

Disposition: During the SSTC conference call of 6/10, the co-chairs were directed to make editorial changes to the document to clarify as suggested. These changes were made to final version of core before submitting the document as OASIS standard.
## Appendix A. Revision History

<table>
<thead>
<tr>
<th>Rev</th>
<th>Date</th>
<th>By Whom</th>
<th>What</th>
</tr>
</thead>
<tbody>
<tr>
<td>Draft-00</td>
<td>2002-12-10</td>
<td>Jahan Moreh</td>
<td>Initial version based on emails to the list</td>
</tr>
<tr>
<td>Draft-01</td>
<td>2003-01-22</td>
<td>Jahan Moreh</td>
<td>Additions from Rob Philpott</td>
</tr>
<tr>
<td>Draft-02</td>
<td>2003-02-14</td>
<td>Jahan Moreh</td>
<td>Additions from Prateek Mishra</td>
</tr>
<tr>
<td>Draft-03</td>
<td>2003-02-18</td>
<td>Jahan Moreh</td>
<td>Updated based on discussions during SSTC meeting of 2/18/03.</td>
</tr>
<tr>
<td>Draft-04</td>
<td>2003-03-18</td>
<td>Jahan Moreh</td>
<td>Updated based on a message from Jon Westbrock and Prateek’s response to that message</td>
</tr>
<tr>
<td>Draft-05</td>
<td>2003-03-31</td>
<td>Jahan Moreh</td>
<td>Added possible resolution to PE 15 per Prateek’s email</td>
</tr>
<tr>
<td>Draft-06</td>
<td>2003-04-01</td>
<td>Jahan Moreh</td>
<td>Modifications and dispositions based on TC meeting of April 01, 2003</td>
</tr>
<tr>
<td>Draft-07</td>
<td>2003-04-07</td>
<td>Jahan Moreh</td>
<td>Added new erratum reported by Eve Maler. Added potential erratum reported by Eve Maler regarding editorial changes to make clear the use of Qname in <code>&lt;AuthorityKind&gt;</code> and <code>&lt;RespondWith&gt;</code>. Updated Option’s section of PE11 per Eve Maler’s suggestion.</td>
</tr>
<tr>
<td>Draft 13</td>
<td>2003-06-13</td>
<td>Jahan Moreh</td>
<td>Added PE23</td>
</tr>
<tr>
<td>Draft 14</td>
<td>2003-06-30</td>
<td>Jahan Moreh</td>
<td>Recorded final disposition of PE23</td>
</tr>
</tbody>
</table>
### Appendix B. Summary of Disposition

<table>
<thead>
<tr>
<th>Erratum #</th>
<th>Status</th>
<th>Document</th>
<th>Draft</th>
</tr>
</thead>
<tbody>
<tr>
<td>E1</td>
<td>Disposed</td>
<td>Bindings and Profiles</td>
<td>01</td>
</tr>
<tr>
<td>E2</td>
<td>Disposed</td>
<td>Bindings and Profiles</td>
<td>01</td>
</tr>
<tr>
<td>E3</td>
<td>Disposed</td>
<td>Bindings and Profiles</td>
<td>01</td>
</tr>
<tr>
<td>E4</td>
<td>Disposed</td>
<td>Assertions and Protocols</td>
<td>02</td>
</tr>
<tr>
<td>E5</td>
<td>Disposed</td>
<td>Assertions and Protocols</td>
<td>02</td>
</tr>
<tr>
<td>E6</td>
<td>Disposed</td>
<td>Assertions and Protocols</td>
<td>02</td>
</tr>
<tr>
<td>E7</td>
<td>Disposed</td>
<td>Assertions and Protocols</td>
<td>04</td>
</tr>
<tr>
<td>E8</td>
<td>Disposed</td>
<td>Assertions and Protocols</td>
<td>03</td>
</tr>
<tr>
<td>E9</td>
<td>Disposed</td>
<td>Bindings and Profiles</td>
<td>03</td>
</tr>
<tr>
<td>PE1</td>
<td>Disposed</td>
<td>Bindings and Profiles</td>
<td>01</td>
</tr>
<tr>
<td>PE2</td>
<td>Disposed; No action required</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PE3</td>
<td>Disposed; No action required</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PE4</td>
<td>Disposed</td>
<td>Bindings and Profiles</td>
<td>02</td>
</tr>
<tr>
<td>PE5</td>
<td>Disposed</td>
<td>Assertions and Protocols</td>
<td>02</td>
</tr>
<tr>
<td>PE6</td>
<td>Disposed</td>
<td>Bindings and Profiles</td>
<td>03</td>
</tr>
<tr>
<td>PE7</td>
<td>Disposed</td>
<td>Assertions and Protocols</td>
<td>02</td>
</tr>
<tr>
<td>PE8</td>
<td>Disposed</td>
<td>Assertions and Protocols</td>
<td>02</td>
</tr>
<tr>
<td>PE9</td>
<td>Disposed</td>
<td>Assertions and Protocols</td>
<td>06</td>
</tr>
<tr>
<td>PE10</td>
<td>Disposed; No action required</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PE11</td>
<td>Disposed</td>
<td>Assertions and Protocols</td>
<td>03</td>
</tr>
<tr>
<td>PE12</td>
<td>Disposed</td>
<td>Assertions and Protocols</td>
<td>03</td>
</tr>
<tr>
<td>PE13</td>
<td>Disposed</td>
<td>Assertions and Protocols 03 and 06</td>
<td></td>
</tr>
<tr>
<td>PE14</td>
<td>Disposed</td>
<td>Assertions and Protocols</td>
<td>03</td>
</tr>
<tr>
<td>PE15</td>
<td>Disposed</td>
<td>Glossary</td>
<td>01</td>
</tr>
<tr>
<td>PE16</td>
<td>Disposed</td>
<td>Bindings and Profiles</td>
<td>02</td>
</tr>
<tr>
<td>PE17</td>
<td>Disposed</td>
<td>Assertions and Protocols</td>
<td>04</td>
</tr>
<tr>
<td>PE18</td>
<td>Disposed</td>
<td>Bindings and Profiles</td>
<td>03</td>
</tr>
<tr>
<td>PE19</td>
<td>Disposed</td>
<td>Assertions and Protocols</td>
<td>05 and 06</td>
</tr>
<tr>
<td>PE20</td>
<td>Disposed</td>
<td>Bindings and Profiles</td>
<td>03</td>
</tr>
<tr>
<td>PE21</td>
<td>Disposed</td>
<td>Assertions and Protocols</td>
<td>11</td>
</tr>
<tr>
<td>PE22</td>
<td>Disposed</td>
<td>Assertions and Protocols</td>
<td>11</td>
</tr>
<tr>
<td>PE23</td>
<td>Disposed</td>
<td>Assertions and Protocols</td>
<td>sstc-saml-core-1.1-cs-02</td>
</tr>
</tbody>
</table>
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. Copyright © The Organization for the Advancement of Structured Information Standards [OASIS] 2002 and 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.