Errata Working Document for SAML V2.0

Working Draft 44

6 May 2008

Document identifier:

sstc-saml-errata-2.0-draft-43

This Version:

(See the SSTC document repository: http://www.oasis-open.org/committees/documents.php?wg_abbrev=security)

Previous Version:

(See the SSTC document repository: http://www.oasis-open.org/committees/documents.php?wg_abbrev=security)

Technical Committee:

OASIS Security Services TC

Chairs:

Hal Lockhart, BEA
Brian Campbell, Ping Identity Corporation

Editor:

Abbie Barbir, Nortel, <abbieb@nortel.com>
Eve Maler, Sun Microsystems <eve.maler@sun.com>
Scott Cantor, Internet2 <cantor.2@osu.edu>

Related Work:

This specification is related to:

Security Assertion Markup Language (SAML) Version 2.0

Abstract:

This document lists the proposed errata against the OASIS SAML V2.0 Committee Specifications and details about their disposition. Each item describes options for resolving the issue and the resolution decided on by the SSTC, if any.

Status:

This document is work in progress and will be updated over time to reflect newly proposed errata. This is meant to be the working document that records the history of each item; there is a separate document for approved errata that is on a formal approval track, which summarizes only the errata with resolutions that prescribe specification changes.

Technical Committee members should send comments on this specification and proposed errata to security-services@lists.oasis-open.org. Others should send comments to the Technical Committee by using the "Send A Comment" button on the Technical Committee's web page at http://www.oasis-open.org/committees/comments/index.php?wg_abbrev=security.

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 Technical Committee web page at http://www.oasis-open.org/committees/security/ipr.php.

Notices

All capitalized terms in the following text have the meanings assigned to them in the OASIS Intellectual Property Rights Policy (the "OASIS IPR Policy"). The full Policy may be found at the OASIS website.

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 OWNERSHIP RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

OASIS requests that any OASIS Party or any other party that believes it has patent claims that would necessarily be infringed by implementations of this OASIS Committee Specification or OASIS Standard, to notify OASIS TC Administrator and provide an indication of its willingness to grant patent licenses to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification.

OASIS invites any party to contact the OASIS TC Administrator if it is aware of a claim of ownership of any patent claims that would necessarily be infringed by implementations of this specification by a patent holder that is not willing to provide a license to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification. OASIS may include such claims on its website, but disclaims any obligation to do so.

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' procedures with respect to rights in any document or deliverable produced by an OASIS Technical Committee can be found on 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 implementers or users of this OASIS Committee Specification or OASIS Standard, can be obtained from the OASIS TC Administrator. OASIS makes no representation that any information or list of intellectual property rights will at any time be complete, or that any claims in such list are, in fact, Essential Claims.

The name "OASIS" is a trademark of OASIS, the owner and developer of this specification, and should be used only to refer to the organization and its official outputs. OASIS welcomes reference to, and implementation and use of, specifications, while reserving the right to enforce its marks against misleading uses. Please see http://www.oasis-open.org/who/trademark.php for above guidance.

Table of Contents

1 Introduction

This document lists the proposed errata against the OASIS SAML 2.0 Committee Specifications and details about their disposition. It is a working document that may change over time. See also the formally approved SAML V2.0 Errata document and its associated "errata composite" documents, whose latest revisions are listed and linked at the SSTC web page (http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security).

2 Errata

The SSTC has determined that these reported problems have a solution that can be applied in erratum form. Their original number designations have changed from "PE*nn*" to "E*nn*" to reflect this status.

E0: Incorrect section reference

First reported by: Rob Philpot, RSA

Message: http://lists.oasis-open.org/archives/security-services/200503/msg00080.html

Document: Core

Description: Line 2660 refers back to section "3.6.3" for Reason codes. This should refer to section "3.7.3".

Options:

Disposition: During the conference call of March 28 the TC unanimously agreed to make this correction. (Note that this entry was originally number "E1" when there were separate "E" (agreed errata) and "PE" (potential errata) lists, where the "E" list had only this one entry in it. It has been renamed "E0" so that the two lists could be merged and a single number would suffice for unique identification across them.)

E1: Relay State for HTTP Redirect

First reported by: Ari Kermaier, Oracle

Message: http://lists.oasis-open.org/archives/security-services/200502/msg00003.html

Document: Bindings and Profiles

Description: Section 3.4.3 (Relay State for HTTP Redirect) lines 551-553 read

"Signing is not realistic given the space limitation, but because the value is exposed to third-party tampering, the entity SHOULD insure that the value has not been tampered with by using a checksum, a pseudo-random value, or similar means."

This language should probably be deleted or modified, as the RelayState parameter *is* covered by the query string signature described in 3.4.4.1 (DEFLATE Encoding).

The same language is correctly present in 3.5.3 (Relay State for HTTP POST), as no means of signing the POST form control data is defined.

Options: Replace first paragraph of section 3.4.3 at line 545 with: "RelayState data MAY be included with a SAML protocol message transmitted with this binding. The value MUST NOT exceed 80 bytes in length and SHOULD be integrity protected by the entity creating the message, either via a digital signature (see section [3.4.4.1]) or by some independent means."

Disposition: During the conference call of April 12 the TC accepted this option.

E2: Metadata clarifications

First reported by: Scott Cantor, OSU

Message: http://lists.oasis-open.org/archives/security-services/200501/msg00058.html

Document: Bindings and Profiles

Description: Clarify metadata requirements in the various profiles. For example, it's required by implication that if you support the Artifact binding for some profile that your role descriptor also needs an ArtifactResolutionService element, but this isn't stated anywhere.

Options: In [SAMLBind] replace paragraph in section 3.6.7 at lines 1188-1191 with:

"Support for receiving messages using the HTTP Artifact binding SHOULD be reflected by indicating URL endpoints at which requests and responses for a particular protocol or profile should be sent. Either a single endpoint or distinct request and response endpoints MAY be supplied. Support for sending messages using this binding SHOULD be accompanied by one or more indexed <md:ArtifactResolutionService> endpoints for processing <samlp:ArtifactResolve> messages."

Disposition: A thorough disposition requires a fairly careful review of Metadata and Profiles so that the requirements can be documented in various places. This work is deferred to SAML 2.x. However, during the conference call of April 12 the TC accepted the above text as clarification for SAML 2.0.

E4: SAML 1.1 Artifacts

First reported by: Scott Cantor, OSU

Message: http://lists.oasis-open.org/archives/security-services/200501/msg00058.html

Document: Bindings and Profiles

Description: Clarifying that SAML 1.1 artifacts have no place or use in SAML 2.0

Options: In [SAMLBind] add to line 1067:

"Although the general artifact structure resembles that used in prior versions of SAML and the type code of the single format described below does not conflict with previously defined formats, there is explicitly no correspondence between SAML 2.0 artifacts and those found in any previous specifications, and artifact formats not defined specifically for use with SAML 2.0 MUST NOT be used with this binding."

Disposition: During the conference call of April 12 the TC accepted this option.

E6: Encrypted NameID

First reported by: Rob Philpott, RSA

Message: Communicated during TC conference call of February 1, 2005.

Document: Core

Description: When using the nameid-format:encrypted type of name identifier in SAML assertions and protocol messages, it is not possible to communicate the format of the unencrypted identifier as part of the assertion or message. This concept was derived from Liberty which only used it for persistent identifiers. Since we also support other formats in SAML 2.0, the agreement on the unencrypted form (prior to encryption/after decryption) must be done out of band.

Options: In [SAMLCore] append to paragraph ending on line 2139:

"It is not possible for the service provider to specifically request that a particular kind of identifier be returned if it asks for encryption. The <md:NameIDFormat> metadata element (see [SAMLMeta]) or other out-of-band means MAY be used to determine what kind of identifier to encrypt and return."

Disposition: During the conference call of April 12 the TC accepted this option.

E7: Metadata attributes WantAuthnRequestsSigned and AuthnRequestsSigned

First reported by: Rob Philpott, RSA

Message: http://lists.oasis-open.org/archives/security-services/200502/msg00017.html

Document: Metadata

Description: In Metadata, the IDPSSODescriptor has the setting called "WantAuthnRequestsSigned" and the SPSSODescriptor has the setting called "AuthnRequestsSigned". But it's ambiguous about "how" this signing is to be done.

Note that the SP can also define "WantAssertionsSigned", where it means that the SP wants the IDP to sign the Assertion XML element by including a <ds:Signature> element in the assertion. That is, I do NOT believe it means that the assertion can also be "signed by inclusion" by putting it (unsigned) inside a <samlp:Response> element and signing that element. It is the Assertion XML element itself that is signed. I don't believe the same approach is what folks expect for the AuthnRequest settings however. I think it is ambiguous and needs to be clarified.

At the interop, folks were using a true setting for [Want]AuthnRequestsSigned to mean that the AuthnRequest message is signed only in the context of the HTTP Redirect Binding where the total URL with parameters is signed using the mechanism specified in that binding. The AuthnRequest XML element is NOT expected to contain a <ds:Signature> element. Now I don't think this interpretation would necessarily be the same if the message was carried in the POST or Artifact bindings. I assume that in those cases, the XML element itself would be signed and include the ds:Signature> element.

So the interpretation of the setting appears to be dependent on which binding is being used. This is clearly not the case for the WantAssertionsSigned setting. So we should at least clarify this for folks. That is, unless folks have a different interpretation of what the settings mean.

Options: Combine this with PE9 and in [SAMLMetadata] add text before line 710:

"The WantAuthnRequestsSigned attribute is intended to indicate to service providers whether or not they can expect an unsigned <AuthnRequest> message to be accepted by the identity provider. The identity provider is not obligated to reject unsigned requests nor is a service provider obligated to sign its requests, although it might reasonably expect an unsigned request will be rejected. In some cases, a service provider may not even know which identity provider will ultimately receive and respond to its requests, so the use of this attribute in such a case cannot be strictly defined.

Furthermore, note that the specific method of signing that would be expected is binding dependent. The HTTP Redirect binding (see [SAMLBind] sec XX) requires the signature be applied to the URL-encoded value rather than placed within the XML message, while other bindings generally permit the signature to be within the message in the usual fashion."

Add text to paragraph at lines 741-742:

"A value of false (or omission of this attribute) does not imply that the service provider will never sign its requests or that a signed request should be considered an error. However, an identity provider that receives an unsigned <samlp:AuthnRequest> message from a service provider whose metadata contains this attribute with a value of true MUST return a SAML error response and MUST not fulfill the request."

Add text to paragraph at lines 744-747:

"Note that an enclosing signature at the SAML binding or protocol layer does not suffice to meet this requirement, for example signing a <samlp:Response> containing the assertion(s) or a TLS connection."

Disposition: During the conference call of September 27 the TC accepted this option.

E8: SLO and NameID termination

First reported by: Thomas Wisniewski, Entrust

Message: http://lists.oasis-open.org/archives/security-services/200503/msg00034.html

Document: Core

Description: Combining SLO with NameID termination, we should clarify whether it's explicitly not required for the SP to continue to expect or process SLO messages for an active session following NameID termination. The spec implies pretty strongly that you don't because you can terminate your local session.

Options: Replace the last sentence in 2479-2480 (section 3.6.3) with:

"In general it SHOULD NOT invalidate any active session(s) of the principal for whom the relationship has been terminated. If the receiving provider is an identity provider, it SHOULD NOT invalidate any active session(s) of the principal established with other service providers. A requesting provider MAY send a <LogoutRequest> message prior to initiating a name identifier termination by sending a <ManageNameIDRequest> message if that is the requesting provider's intent (e.g., the name identifier termination is initiated via an administrator who wished to terminate all user activity).The requesting provider MUST NOT send a <LogoutRequest> message after the <ManageNameIDRequest> message is sent.".

Disposition: During the conference call of April 12 the TC accepted this option.

E10: Logout Request *reason* Mismatch with Schema

First reported by: Rob Philpott, RSA

Message: http://lists.oasis-open.org/archives/security-services/200503/msg00080.html

Document: Core

Description: In core line 2540 it says that "Reason" on the LogoutRequest is "in the form of a URI reference". However, in the schema, the Reason attribute is type="string", not type="anyURI". All of the reason codes that we define (in section 3.7.3 and 3.7.3.2) are actually URI's. But, since the schema defines it as a string, the text should be changed to match the schema.

Options: Change line 2540 of core as follows: The Reason attribute is specified as a string in the schema. This specification further restricts the schema by requiring that the Reason attribute MUST be in the form of a URI reference.

Disposition: During the conference call of February 14, 2006 the TC accepted the text as stated here.

E11: Improperly Labeled Feature

First reported by: Rob Philpott, RSA

Message: http://lists.oasis-open.org/archives/security-services/200503/msg00080.html

Document: Conformance

Description: In table 2 of the conformance spec, the feature in the 8th row is improperly labeled. It currently says "Name Identifier Management, HTTP Redirect". It should say "Name Identifier Management, HTTP Redirect (SP-initiated)".

There are also minor inconsistencies in the labels since the parenthetical (xP-initiated) are listed with the binding in some, but with the profile in others. I suggest always listing it with the profile name.

Options: Correct the label as suggested in the description of the erratum above.

Disposition: During the conference call of June 7 the TC accepted this option.

E12: Clarification on ManageNameIDRequest

First reported by: Scott Cantor, OSU/Brian Campbell, Ping Identity

Message: http://lists.oasis-open.org/archives/security-services/200504/msg00107.html and **:** http://lists.oasis-open.org/archives/security-services/200501/msg00058.html

Document: Bindings and Profiles

Description: The schema defines the <NewID> element of a <ManageNameIDRequest> as a string. The implication of that is that a NIM request message from IDP to SP can only be used to inform the SP of a change in identifier value (not format – format is immutable once established). There are a few places in the spec where the text implies that the format can be changed. Additionally, the text about <NewEncryptedID> should be expanded to clarify that the encrypted element is just the encrypted <NewID> element and not a full <NameID> as in the more typical <EncryptedID> element used elsewhere

Options:

Change the schema to allow format and potentially qualifiers to be changed and make all necessary cascading changes to the spec.

Update the wording in the spec to bring it inline with the schema as is and clarify that only the value of the identifier can be managed with the Name Identifier Managenment profile.

Given the complexity and scope of change involved in option 1 and the consensus that option 2 is sufficient and not too limiting, text changes consistent with option 2 are proposed below.

In Profiles change the text on lines 1320-21 from “Subsequently, the identity provider may wish to notify the service provider of a change in the format and/or value that it will use to identify the same principal in the future” to “Subsequently, the identity provider may wish to notify the service provider of a change in the value that it will use to identify the same principal in the future”

In Core change the text on lines 2412-13 from “After establishing a name identifier for a principal, an identity provider wishing to change the value and/or format of the identifier that it will use when referring to the principal,…” to “After establishing a name identifier for a principal, an identity provider wishing to change the value of the identifier that it will use when referring to the principal, …”

In Core add the following text after line 2438, “In either case, if the <NewEncryptedID> is used, its encrypted content is just a <NewID> element containing only the new value for the identifier (format and qualifiers cannot be changed once established).”

Disposition: During the conference call of June 7 the TC approved option 2**.**

E13: Inaccurate description of Authorization Decision

First reported by: Jahan Moreh, Sigaba

Message: http://lists.oasis-open.org/archives/security-services/200504/msg0125.html

Document: Core

Description: Core 357-358 currently reads:

Authorization Decision: A request to allow the assertion subject to access the specified resource has been granted or denied.

It should say:

Authorization Decision: A request to allow the assertion subject to access the specified resource has been granted, denied, or is indeterminate.

Options: Make correction as described above.

Disposition: During the conference call of June 7 the TC approved the change as proposed here.

E14: AllowCreate

First reported by: Brian Campbell, Ping Identity

Message: http://lists.oasis-open.org/archives/security-services/200505/msg00014.html

Document: Core and Profiles

Description: AllowCreate needs more clear definition.

Options: Make the following corrections

In Profiles replace the current text there about AllowCreate with a statement that "this profile does not provide additional guidelines for the use of AllowCreate" and reference this text in core as governing.

In Core, replace definition of AllowCreate, lines 2123-2129:

"A Boolean value used to indicate whether the requester grants to the identity provider, in the course of fulfilling the request, permission to create a new identifier or to associate an existing identifier representing the principal with the relying party. Defaults to "false" if not present or the entire element is omitted."

In Core, replace lines 2143-2147 and insert new text at line 2130 (beginning of the explanatory text):

"The AllowCreate attribute may be used by some deployments to influence the creation of state maintained by the identity provider pertaining to the use of a name identifier (or any other persistent, uniquely identifying attributes) by a particular relying party, for purposes such as dynamic identifier or attribute creation, tracking of consent, subsequent use of the Name Identifier Management protocol (see section XX), or other related purposes.

When "false", the requester tries to constrain the identity provider to issue an assertion only if such state has already been established or is not deemed applicable by the identity provider to the use of an identifier. Thus, this does not prevent the identity provider from assuming such information exists outside the context of this specific request (for example, establishing it in advance for a large number of principals).

A value of "true" permits the identity provider to take any related actions it wishes to fulfill the request, subject to any other constraints imposed by the request and policy (the IsPassive attribute, for example).

Generally, requesters cannot assume specific behavior from identity providers regarding the initial creation or association of identifiers on their behalf, as these are details left to implementations or deployments. Absent specific profiles governing the use of this attribute, it might be used as a hint to identity providers about the requester's intention to store the identifier or link it to a local value.

A value of "false" might be used to indicate that the requester is not prepared or able to do so and save the identity provider wasted effort.

Requesters that do not make specific use of this attribute SHOULD generally set it to "true" to maximize interoperability.

The use of the AllowCreate attribute MUST NOT be used and SHOULD be ignored in conjunction with requests for or assertions issued with name identifiers

with a Format of urn:oasis:names:tc:SAML:2.0:nameid-format:transient (they preclude any such state in and of themselves)."

In Core, change lines 2419-2420 to:

"This protocol MUST NOT be used in conjunction with the urn:oasis:names:tc:SAML:2.0:nameidformat:transient <NameID> Format."

In Core, replace lines 2475-2479 with:

"If the <Terminate> element is included in the request, the requesting provider is indicating that (in the case of a service provider) it will no longer accept assertions from the identity provider or

(in the case of an identity provider) it will no longer issue assertions to the service provider about the principal.

If the receiving provider is maintaining state associated with the name identifier, such as the value of the identifier itself (in the case of a pair-wise identifier), an SPProvidedID value, the sender's consent to the identifier's creation/use, etc., then the receiver can perform any maintenance with the knowledge that the relationship represented by the name identifier has been terminated.

Any subsequent operations performed by the receiver on behalf of the sender regarding the principal (for example, a subsequent <AuthnRequest>) SHOULD be carried out in a manner consistent with the absence of any previous state.

Termination is potentially the cleanup step for any state management behavior triggered by the use of the AllowCreate attribute in the Authentication Request protocol (see section XX). Deployments that do not make use of that attribute are likely to avoid the use of the <Terminate> element or would treat it as a purely advisory matter.

Note that in most cases (a notable exception being the rules surrounding the SPProvidedID attribute), there are no requirements on either identity providers or service providers regarding the creation or use of persistent state. Therefore, no explicit behavior is mandated when the <Terminate> element is received. However, if persistent state is present pertaining to the use of an identifier (such as if an SPProvidedID attribute was attached), the <Terminate> element provides a clear indication that this state SHOULD be deleted (or marked as obsolete in some fashion)."

Disposition: During the conference call of June 21 the TC approved the change as proposed here.

E17: Authentication Response IssuerName vs. Assertion IssuerName

First reported by: Thomas Wisniewski, Entrust

Message: http://www.oasis-open.org/apps/org/workgroup/security/email/archives/200506/msg00072.html

Document: Profiles

Description: Profiles document says issuer (for an AuthnRequest Response) MAY be omitted. "the <Issuer> element MUST be present and MUST contain the unique identifier of the" The main reason is that Issuer should be a MUST in the SSO Response protocol.

Options: Change lines 541-543 of profiles to:

If the <Response> message is signed or if an enclosed assertion is encrypted, then the <Issuer> element MUST be present. Otherwise it MAY be omitted. If present it MUST contain the unique identifier of the issuing identity provider; the Format attribute MUST be omitted or have a value of urn:oasis:names:tc:SAML:2.0:nameid-format:entity."

Disposition: During the conference call of July 5 the TC approved to make the changes as stated here.

E18: reference to identity provider discovery service in ECP Profile

First reported by: Prateek Mishra, Principal Identity

Message:http://www.oasis-open.org/apps/org/workgroup/security/email/archives/200507/msg00000.html

Document: Profiles

Description: The ECP does not directly interact with the identity provider discovery service, it may act as an intermediary for an IdP or SP that plan to utilize the service. Current text gives the

impression that it is a direct participant in the identity provider discovery service. Instead, the main issue is that it should not impede service interactions with an SP or IdP.

Options: Delete lines 725 and 726 from saml-profiles-2.0-os, starting at “The ECP MAY use…”.

Disposition: During the conference call of July 19 the TC approved to make the changes as stated here.

E19: Clarification on Error Processing

First reported by: Connor P. Cahill, AOL

Message: http://lists.oasis-open.org/archives/security-services/200507/msg00008.html

Document: Bindings

Description: Clarification on error processing

Options: The section numbers and line numbers are all from "saml-bindings-2.0-os.pdf"
Section 3.2.2.1, lines 310-317:

- Change the first sentence to read:
  - The SAML responder SHOULD return a SOAP message containing either a SAML response element in the body or a SOAP fault.
- Delete the 3rd sentence (If a SAML responder cannot, for some reason, process....). SOAP defines when a SOAP fault is required and SAML goes into detail about what we should return when in section 3.2.3.3 "Error Reporting".
- Change the 4th sentence to soften the "MUST NOT" and make it a "SHOULD NOT" as there can be sufficient security through obscurity reasons to do so in some cases.
- Add a new sentence at the end of the paragraph noting that details about error handling are covered in section 3.2.3.3 "Error Reporting" or something to that effect.

Section 3.2.3.3, lines 370-383: Change the MUST on line 378 to a SHOULD.

Disposition: During the conference call of August 2 the TC approved the changes as stated here.

E20: ECP SSO Profile and Metadata

First reported by: Thomas Wisniewski, Entrust

Message: http://lists.oasis-open.org/archives/security-services/200506/msg00106.html

Document: Profiles

Description: There is no metadata consideration in ECP profile

Options: In SAML Profiles specification add new section 4.2.6 as follows:

The rules specified in the browser SSO profile in Section 4.1.6 apply here as well. Specifically, the indexed endpoint element <md:AssertionConsumerService> with a binding of urn:oasis:namees:tc:SAML:2.0:bindings:PAOS, MAY be used to describe the supported binding and location(s) to which an identity provider may send responses to a service provider using this profile. And, the endpoint <md:SingleSignOnService> with a binding of urn:oasis:namees:tc:SAML:2.0:bindings:SOAP, MAY be used to describe the supported binding and location(s) to which an service provider may send requests to an identity provider using this profile

Disposition: During the conference call of July 19 the TC approved to make the changes as stated here.

E21: PAOS Version

First reported by: Thomas Wisniewski, Entrust

Message: http://www.oasis-open.org/apps/org/workgroup/security/email/archives/200507/msg00028.html

Document: Bindings

Description: It's unclear what the word minimum implies in the line '... PAOS version with "urn:liberty:paos:2003-08" at a minimum."

Options: Strike the words “at a minimum”

Disposition: During the conference call of July 19 the TC approved to make the changes as stated here.

E22: Error in Profile/ECP

First reported by: Rob Philpott, RSA Security

Message: http://www.oasis-open.org/apps/org/workgroup/security/email/archives/200507/msg00040.html

Document: Profiles

Description: Line 907 of Profiles says the responseConsumerURL must be the same as the “AssertionServiceConsumerURL” in an <AuthnRequest> message. The attribute’s name should be “AssertionConsumerServiceURL”.

Options: Make changes as specified.

Disposition: During the conference call of August 2 the TC approved the changes as stated here.

E24: HTTPS in URI Binding

First reported by: Nick Ragouzis, Enosis Group

Message: http://lists.oasis-open.org/archives/security-services/200507/msg00037.html

Document: Bindings

Description: Section 3.7, starting at line 1349 the text states:
“Like SOAP, URI resolution can occur over multiple underlying transports. This binding has transport-independent aspects, but also calls out the use of HTTP with SSL3.0 [SSL3] or TLS 1.0 [RFC2246] as REQUIRED (mandatory to implement)”

Options: Replace the current text with the following:

“Like SOAP, URI resolution can occur over multiple underlying transports. This binding has protocol-independent aspects, but also calls out as mandatory the implementation of HTTP URIs.”

Disposition: During the conference call of August 2 the TC approved the changes as stated here.

E25: Metadata Structures Feature in Conformance

First reported by: Nick Ragouzis, Enosis Group

Message: http://lists.oasis-open.org/archives/security-services/200507/msg00038.html

Document: Conformance

Description: Conformance document does not specify any requirements with respect to metadata.

Change to Table 2: Feature Matrix

	IdP	IdPLite	SP	SPLite	ECP
FEATURE					
Metadata Structures	OPT	OPT	OPT	OPT	N/A
Metadata Interoperation	OPT	OPT	OPT	OPT	N/A

Change to Table 4: SAML Authority and Requester Matrix

	AuthnAuth	AttribAuth	AuthZDcsnAuth	Requester
FEATURE				
Metadata Structures	OPT	OPT	OPT	OPT
Metadata Interoperation	OPT	OPT	OPT	OPT

New sub-sections to Section 3 (Conformance):

3.6 Metadata Structures

Implementations claiming conformance to SAMLv2.0 may declare each operational mode's conformance to SAMLv2.0 Metadata [SAMLMeta] through election of the Metadata Structures option.

With respect to each operational mode, such conformance entails the following:

* Implementing SAML metadata according to the extensible SAMLv2.0 Metadata format in all cases where an interoperating peer has the option, as stated in SAMLv2.0 specifications, of depending on the existence of SAMLv2.0 Metadata. Electing the Metadata Structures option has the effect of requiring such metadata be available to the interoperating peer. The Metadata Interoperation feature, described below, provides a means of satisfying this requirement.

* Referencing, consuming, and adherence to the SAML metadata, according to [SAMLMeta], of an interoperating peer when the known metadata relevant to that peer and the particular operation, and the current exchange, has expired or is no longer valid in cache, provided the metadata is available and is not prohibited by policy or the particular operation and that specific exchange.

3.7 Metadata Interoperation

Election of the Metadata Interoperation option requires the implementation offer, in addition to any other mechanism, the well-known location publication and resolution mechanism described in SAML metadata [SAMLMeta].

Options: Make changes as suggested here

Disposition: During the TC conference call on 9/27 the TC accepted the changes as suggested here.

E26: Ambiguities around Multiple Assertions and Statements in the SSO Profile

First reported by: Scott Cantor, OSU

Message: http://lists.oasis-open.org/archives/security-services/200508/msg00056.html

Document: Profiles

Description: SSO Profile need clarifications.

Section 4.1.4.2, <Response> Usage, replace the list at lines 541-572, with the following list:

- If the response is unsigned, the <Issuer> element MAY be omitted, but if present (or if the response is signed) it MUST contain the unique identifier of the issuing identity provider; the Format attribute MUST be omitted or have a value of urn:oasis:names:tc:SAML:2.0:nameid-format:entity
- It MUST contain at least one <Assertion>. Each assertion's <Issuer> element MUST contain the unique identifier of the responding identity provider; the Format attribute MUST be omitted or have a value of urn:oasis:names:tc:SAML:2.0:nameid-format:entity. Note that this profile assumes a single responding identity provider, and all assertions in a response MUST be issued by the same entity.
- If multiple assertions are included, then each assertion's <Subject> element MUST refer to the same principal. It is allowable for the content of the <Subject> elements to differ (e.g. using different <NameID> or alternative <SubjectConfirmation> elements).
- Any assertion issued for consumption using this profile MUST contain a <Subject> element with at least one <SubjectConfirmation> element containing a Method of urn:oasis:names:tc:SAML:2.0:cm:bearer. Such an assertion is termed a bearer assertion. Bearer assertions MAY contain additional <SubjectConfirmation> elements.
- Assertions without a bearer <SubjectConfirmation> MAY also be included; processing of additional assertions or <SubjectConfirmation> elements is outside the scope of this profile.
- At lease one bearer <SubjectConfirmation> element MUST contain a <SubjectConfirmationData> element that itself MUST contain a Recipient attribute containing the service provider's assertion consumer service URL and a NotOnOrAfter attribute that limits the window during which the assertion can be delivered. It MAY also contain an Address attribute limiting the client address from which the assertion can be delivered. It MUST NOT contain a NotBefore attribute. If the containing message is in response to an <AuthnRequest>, then the InResponseTo attribute MUST match the request's ID.
- The set of one or more bearer assertions MUST contain at least one <AuthnStatement> that reflects the authentication of the principal to the identity provider. Multiple <AuthnStatement> elements MAY be included, but the semantics of multiple statements is not defined by this profile.
- If the identity provider supports the Single Logout profile, defined in Section 4.4, any authentication statements MUST include a SessionIndex attribute to enable per-session logout requests by the service provider
- Other statements MAY be included in the bearer assertion(s) at the discretion of the identity provider. In particular, <AttributeStatement> elements MAY be included. The <AuthnRequest> MAY contain an AttributeConsumingServiceIndex XML attribute referencing information about desired or required attributes in [SAMLMeta]. The identity provider MAY ignore this, or send other attributes at its discretion.
- Each bearer assertion MUST contain an <AudienceRestriction> including the service provider's unique identifier as an <Audience>
- Other conditions (and other <Audience> elements) MAY be included as requested by the service provider or at the discretion of the identity provider. (Of course, all such conditions MUST be understood by and accepted by the service provider in order for the assertion to be considered valid.
- The identity provider is NOT obligated to honor the requested set of <Conditions> in the <AuthnRequest>, if any.

In Section 4.1.4.3, <Response> Message Processing Rules:

- Line 576, change "any bearer" to "the bearer"
- Line 578, change "any bearer" to "the bearer"
- Line 583, change to: "Verify that any assertions relied upon are valid in other respects. Note that while multiple bearer <SubjectConfirmation> elements may be present, the successful evaluation of a single such element in accordance with this profile is sufficient to confirm an assertion. However, each assertion, if more than one is present, MUST be evaluated independently."
- Line 584, change "any bearer" to "the bearer"
- Append to paragraph ending on line 591: "Note that if multiple <AuthnStatement> elements are present, the SessionNotOnOrAfter value closest to the present time SHOULD be honored."

Section 4.1.4.5, POST-Specific Processing Rules:

- Replace lines 600-601 with: "If the HTTP POST binding is used to deliver the <Response>, each assertion MUST be protected by a digital signature. This can be accomplished by signing each individual <Assertion> element or by signing the <Response> element."

Options:

Disposition: During the conference call of August 30 the TC approved the changes as stated here.

E27: Error in ECP Profile

First reported by: Scott Cantor, OSU

Message: http://lists.oasis-open.org/archives/security-services/200509/msg00001.html

Document: Profiles

Description: Profiles, line 947, the ECP RelayState header definition refers to step 5 as the one in which the response is issued to the SP. It should be step 7.

Options:

Disposition: During the conference call of September 13 the TC approved the changes as stated here

---

E28: Conformance Table 1

First reported by: Rob Philpott, RSA Security

Message: http://lists.oasis-open.org/archives/security-services/200509/msg00002.html

Document: Conformance

Description: The first column is labeled “Profile”, yet several of the entries are technically not “profiles”. The same applies to the section title and the paragraph above the table.

Options:
Column 1:
Combine Artifact Resolution, Authentication Query, Attribute Query, Authorization Decision Query entries into a single entry labeled:

Assertion Query/Request

Column 2

Label each set of message flows with relevant protocol description:
Artifact Resolution, Authentication Query, Attribute Query, Authorization Decision Query

Column 3

No change

(2) Remove the following rows from the table:

SAML URI binding
Metadata

Disposition: During the conference call of September 27 the TC approved the changes as stated here

E29: Conformance Table 2

First reported by: Rob Philpott, RSA Security

Message: http://lists.oasis-open.org/archives/security-services/200509/msg00002.html

Document: Conformance

Description: The table is missing feature rows for performing a “Request for Assertion by Identifier” over SOAP and for “SAML URI Binding”. These features are clearly permissible for IDP’s, since the IDPSSODescriptor includes an element for zero or more <AssertionIDRequestService> elements.

Options: Add two rows table 2; row #1 is labeled Request for Assertion Identifier; row #2 is labeled SAML URI binding; both are optional for IdP row and N/A for all the rest.

Disposition: During the conference call of September 27 the TC as stated here.

E30: Considerations for key replacement

First reported by: Rob Philpott, RSA Security

Message: http://lists.oasis-open.org/archives/security-services/200509/msg00002.html

Document: Core

Description: Line 3110 states: “optionally one or more encrypted keys…”

Options: Replace “optionally one or more” with “zero or more”.

Disposition: During the conference call of September 13 the TC approved the changes as stated here

E31: Various minor errors in Binding

First reported by: Rob Philpott, RSA Security

Message: http://lists.oasis-open.org/archives/security-services/200509/msg00002.html

Document: Bindings

Description:

1. Line 511: “security at the SOAP message layer is recommended.” It should be capitalized as in “RECOMMENDED”.

2. Line 785: “If no such value is included with a SAML request message” – “value” is ambiguous. It’s referring to the RelayState parameter, which itself is a name/value pair. This should be changed to “If no RelayState parameter is included…”
3. Line 1136: “using a direct SAML binding”. There is no definition for what a “direct” SAML binding is. Other documents have referred to the SOAP binding as a “synchronous” binding.
4. Line 1397: “Note that use of wildcards is not allowed on such ID queries”. This should be changed to: “Note that the URI syntax does not support the use of wildcards in such queries.”

Options:

Disposition: During the conference call of September 13 the TC approved the changes for items 2 and 3. During the conference call of September 27 the TC approved the changes for items 1 and 4.

E32: Missing section in Profiles

First reported by: Rob Philpott, RSA Security

Message: http://lists.oasis-open.org/archives/security-services/200509/msg00002.html

Document: Profiles

Description: Section 4.3. This profile is missing a subsection for “Required Information”, which is present in all other profiles.

Options: Beginning at line 1092, insert the following text:

> 4.3.1 Required Information
>
> **Identification:** urn:oasis:names:tc:SAML:2.0:profiles:SSO:idp-discovery
>
> **Contact information:** security-services-comment@lists.oasis-open.org
>
> **Description:** Given below.
>
> **Updates:** None.

Disposition: During the conference call of December 5 the TC approved the changes.

E33: References to Assertion Request Protocol

First reported by: Rob Philpott, RSA Security

Message: http://lists.oasis-open.org/archives/security-services/200509/msg00002.html

Document: Metadata

Description: Lines 700, 871, and 904 state: “profile of the Assertion Request protocol defined in [SAMLProf]”. References to “Assertion Request” should be changed to “Assertion Query/Request”.

Options:

Disposition: During the conference call of September 13 the TC approved the changes.

E34: Section Heading

First reported by: Rob Philpott, RSA Security

Message: http://lists.oasis-open.org/archives/security-services/200509/msg00002.html

Document: Metadata

Description: Line 809: the section 2.4.4.2 should be indented so that it is 2.4.4.1.1 since <RequestedAttribute> is part of the <AttributeConsumingService> defined in section 2.4.4.1.
.

Options:

Disposition: During the conference call of September 13 the TC approved the change.

E35: Example in Profiles

First reported by: Rob Philpott, RSA Security

Message: http://lists.oasis-open.org/archives/security-services/200509/msg00023.html and
http://www.oasis-open.org/archives/security-services/200602/msg00008.html

Document: Profiles

Description: The example on page 29 line 964 uses a ResponseConsumerURL of http://identity-service.example.com/abc. Since this value must be an AssertionConsumerService at the SP and must match (according to the rules in 4.2.4.4) the value of the resonseConsumerURL, the example would result in an error condition.

Options: Change the value of the responseConsumerURL in the example on page 29 line 964 to https://ServiceProvider.example.com/ecp_assertion_consumer.

Change the sentence on page 27 lines 906-908 to: “This value MUST be the same as the AssertionServiceConsumerURL (or the URL referenced in metadata) conveyed in the <AuthnRequest> and SHOULD NOT be a relative URL.”

Disposition: During the conference call of February 28 TC approved the change as stated here.

E36: Clarification on Action Element

First reported by: Emily Xu, Sun Microsystems

Message: http://lists.oasis-open.org/archives/security-services/200509/msg00053.html

Document: Core

Description:
In section 2.7.4.2 of core spec, Namespace is marked as "Optional". It says: "If this element is absent, the namespace urn:oasis:names:tx:SAML:1.0:action:rwedc-negation specified in Section 8.1.2 is in effect." But in the following schema definition, attribute Namespace is marked as required:
<attribute name="Namespace" type="anyURI" use="required"/>

A clarification is needed to resolve this apparent conflict.

Options: In line 1359 change “Optional” to “Required” and strike the sentence starting at line 1361-1363 (“If this element is absent….”)

Disposition: During the conference call of October 25 the TC approved the change.

E37: Clarification in Metadata on Indexed Endpoints

First reported by: Rob Philpot, RSA Security

Message: http://lists.oasis-open.org/archives/security-services/200510/msg00025.html

Document: Metadata

Description: Metadata line 272 says “In any such sequence of like endpoints based on this type, the default…”. It is a bit ambiguous what “of like endpoints” means. Are two endpoints alike if they are of the same binding type (e.g. SOAP)? Or are they alike because they are assigned to the same service endpoint.

Options: Modify Metadata, line 272 as follows:

"In any such sequence of indexed endpoints that share a common element name and namespace (i.e. all instances of <md:AssertionConsumerService> within a role), the default endpoint is..."

Disposition: During the conference call of November 22 the TC approved the changes as stated here

---

E38: Clarification regarding index on <LogoutRequest>

First reported by: Conor P. Cahill, AOL

Message: http://lists.oasis-open.org/archives/security-services/200511/msg00000.html

Document: Core, Profiles

Description: The language surrounding session index on the <LogoutRequest> (line 2546) is unclear.

Options: The following two changes are suggested:

1. Change Core, line 2546 as follows:

   The index of the session between the principal identified by the <saml:BaseID>, <saml:NameID>, or <saml:EncryptedID> element, and the session authority. This must correlate to the SessionIndex attribute, if any, in the <saml:AuthnStatement> of the assertion used to establish the session that is being terminated."

2. Change Profiles, line 1302-1304 to:

   "If the requester is a session participant, it MUST include at least one <SessionIndex> element in the request. (Note that the session participant always receives a SessionIndex attribute in the <saml:AuthnStatement> elements that it receives to initiate the session, per section 4.1.4.2 of the Web Browser SSO Profile.) If the requester is a session authority (or acting on its behalf), then it MAY omit any such elements to indicate the termination of all of the principal's applicable sessions."

Disposition: During the conference call of November 22 the TC approved the changes as stated here

---

E39: Error in SAML profile example

First reported by: Greg Whitehead, HP

Message: http://www.oasis-open.org/archives/security-services/200601/msg00015.html

Document: Profiles

Description In section 8.5.6 of the SAML 2.0 profiles doc the ldapprof:Encoding="LDAP" attribute should be AttributeValue not Attribute, according to section 8.2.4 of the spec.

Options:

Disposition: During the conference call of 1/17/2006 the TC approved the clarification as stated here.

E40: Holder of Key

First reported by: Prateek Mishra, Oracle

Message: http://www.oasis-open.org/archives/security-services/200601/msg00027.html

Document: Core

Description: HoK described a key that required proof of possession by a attesting entity vs. being held by the subject, Appropriate text does appear in lines 781-783 of saml2-core. However,

lines 335-337 of saml2-profiles reads:

“As described in [XMLSig], each <ds:KeyInfo> element holds a key or information that enables an application to obtain a key. The holder of a specified key is considered to be the subject of the assertion by the asserting party”

The last sentence should be replaced by:

"The holder of a specified key is considered to be an acceptable attesting entity for the assertion by the asserting party"

Options:

Disposition: During the conference call of February 28th the TC approved the change as stated here.

E41: EndpointType ResponseLocation clarification in Metadata

First reported by: Eric Tiffany, Project Liberty

Message: http://www.oasis-open.org/archives/security-services/200601/msg00034.html

Document: Metadata

Description Implementer interpreted the metadata spec to mean that ResponseLocation should only be omitted for the SOAP binding, and that the ResponseLocation be specified in metadata for other bindings.

Options: Proposed text to resolve this:

At line 238 in Metadata we have now:

“The ResponseLocation attribute is used to enable different endpoints to be specified for receiving request and response messages associated with a protocol or profile, not as a means of load-balancing or redundancy (multiple elements of this type can be included for this purpose). When a role contains an element of this type pertaining to a protocol or profile for which only a single type of message (request or response) is applicable, then the ResponseLocation attribute is unused.

The proposal is to add the following:

“If the ResponseLocation attribute is omitted, any response messages associated with a protocol or profile may be assumed to be handled at the URI indicated by the Location attribute."

Disposition: During the conference call of 1/31/06 TC voted to approve changes as stated here.

E42: Conformance Table 4

First reported by: Thomas Wisniewski, Entrust

Message: http://lists.oasis-open.org/archives/security-services/200601/msg00041.html

Document: Conformance

Description: Table 4 has a cell for SAML <x> Authority responding to an <y> Query. That is, an Attribute Authority responding to an Authentication or Authorization Decision Query. This doesn't seem to make sense as authorities should respond to their respective queries. So the OPTIONAL items under the authorities should be N/A."

Options: Change the reference from "OPTIONAL" to "N/A" under the columns SAML Authentication Authority, SAML Attribute Authority, and SAML Authorization Decision Authority in Table 4: SAML Authority and Requester Matrix.

Disposition: During the conference call of 1/31/06 TC voted to approve changes as stated here.

E43: Key location in saml:EncryptedData

First reported by: Heather Hinton, IBM

Message:

Document: Core

Description: The specification in core does not properly follow XML Encryption standards with respect to key location.

Options: Replace section 6 of core with the following text:

6.1 General Considerations

Encryption of the <Assertion>, <BaseID>, <NameID> and <Attribute> elements is provided by use of XML Encryption [XMLEnc]. Encrypted data and optionally one or more encrypted keys MUST replace the plaintext information in the same location within the XML instance. The <xenc:EncryptedData> element's Type attribute SHOULD be used and, if it is present, MUST have the value http://www.w3.org/2001/04/xmlenc#Element.

Any of the algorithms defined for use with XML Encryption MAY be used to perform the encryption. The SAML schema is defined so that the inclusion of the encrypted data yields a valid instance.

6.2 Key and Data Referencing Guidelines

If an encrypted key is NOT included in the XML instance, then the relying party must be able to locally determine the decryption key, per [XMLEnc].

Implementations of SAML MAY implicitly associate keys with the corresponding data they are used to encrypt, through the positioning of <xenc:EncryptedKey> elements next to the associated <xenc:EncryptedData> element, within the enclosing SAML parent element. However, the following set of explicit referencing guidelines are suggested to facilitate interoperability.

If the encrypted key is included in the XML instance, then it SHOULD be referenced within the associated <xenc:EncryptedData> element, or alternatively embedded within the <xenc:EncryptedData> element. When an <xenc:EncryptedKey> element is used, the <ds:KeyInfo> element within <xenc:EncryptedData> SHOULD reference the <xenc:EncryptedKey> element using a <ds:RetrievalMethod> element of Type http://www.w3.org/2001/04/xmlenc#EncryptedKey.

In addition, an <xenc:EncryptedKey> element SHOULD contain an <xenc:ReferenceList> element containing a <xenc:DataReference> that references the corresponding <xenc:EncryptedData> element(s) that the key was used to encrypt.

In scenarios where the encrypted element is being “multicast” to multiple recipients, and the key used to encrypt the message must be in turn encrypted individually and independently for each of the multiple recipients, the <xenc:CarriedKeyName> element SHOULD be used to assign a common name to each of the <xenc:EncryptedKey> elements so that a <ds:KeyName> can be used from within the <xenc:EncryptedData> element’s <ds:KeyInfo> element.

Within the <xenc:EncryptedData> element, the <ds:KeyName> can be thought of as an ”alias” that is used for backwards referencing from the <xenc:CarriedKeyName>

element in each individual <xenc:EncryptedKey> element. While this accommodates a "multicast" approach, each recipient must be able to understand (at least one) <ds:KeyName>. The Recipient attribute is used to provide a hint as to which key is meant for which recipient.

The SAML implementation has the discretion to accept or reject a message where multiple Recipient attributes or <ds:KeyName> elements are understood. It is RECOMMENDED that implementations simply use the first key they understand and ignore any additional keys.

6.3 Examples

In the following example, the parent element (<EncryptedID>) contains <xenc:EncryptedData> and (referenced) <xenc:EncryptedKey> elements as siblings (note that the key can in fact be anywhere in the same instance, and the key references the <xenc:EncryptedData> element) :

```
<saml:EncryptedID
      xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
      <xenc:EncryptedData
xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
            Id="Encrypted_DATA_ID"
            Type="http://www.w3.org/2001/04/xmlenc#Element">
            <xenc:EncryptionMethod

      Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"/>
            <ds:KeyInfo
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                  <ds:RetrievalMethod URI="#Encrypted_KEY_ID"

      Type="http://www.w3.org/2001/04/xmlenc#EncryptedKey"/>
            </ds:KeyInfo>
            <xenc:CipherData>

      <xenc:CipherValue>Nk4W4mx...</xenc:CipherValue>
            </xenc:CipherData>
      </xenc:EncryptedData>

      <xenc:EncryptedKey
xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
            Id="Encrypted_KEY_ID">
            <xenc:EncryptionMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
            <xenc:CipherData>
<xenc:CipherValue>PzA5X...</xenc:CipherValue>
</xenc:CipherData>
            <xenc:ReferenceList>
                  <xenc:DataReference URI="#Encrypted_DATA_ID"/>
            </xenc:ReferenceList>
      </xenc:EncryptedKey>
</saml:EncryptedID>
```

In the following <EncryptedAttribute> example, the <xenc:EncryptedKey> element is contained within the <xenc:EncryptedData> element, so there is no explicit referencing:

```
<saml:EncryptedAttribute
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
```

```
      <xenc:EncryptedData
xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
            Id="Encrypted_DATA_ID"
            Type="http://www.w3.org/2001/04/xmlenc#Element">
            <xenc:EncryptionMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"/>
            <ds:KeyInfo
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                  <xenc:EncryptedKey Id="Encrypted_KEY_ID">
                        <xenc:EncryptionMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
<xenc:CipherData>
<xenc:CipherValue>SDFSDF... </xenc:CipherValue>
</xenc:CipherData>
                   </xenc:EncryptedKey>
            </ds:KeyInfo>
            <xenc:CipherData>
<xenc:CipherValue>Nk4W4mx...</xenc:CipherValue>
</xenc:CipherData>
      </xenc:EncryptedData>
</saml:EncryptedAttribute>
```

The final example shows an assertion encrypted for multiple recipients, using the `<xenc:CarriedKeyName>` approach:

```
<saml:EncryptedAssertion
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
      <xenc:EncryptedData
xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
            Id="Encrypted_DATA_ID"
            Type="http://www.w3.org/2001/04/xmlenc#Element">
            <xenc:EncryptionMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"/>
            <ds:KeyInfo
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:KeyName>MULTICAST_KEY_NAME</ds:KeyName>
            </ds:KeyInfo>
            <xenc:CipherData>

      <xenc:CipherValue>Nk4W4mx...</xenc:CipherValue>
            </xenc:CipherData>
      </xenc:EncryptedData>

      <xenc:EncryptedKey
xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
            Id="Encrypted_KEY_ID_1" Recipient="https://sp1.org">
            <xenc:EncryptionMethod

      Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
            <ds:KeyInfo
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:KeyName>KEY_NAME_1</ds:KeyName>
            </ds:KeyInfo>
            <xenc:CipherData>
<xenc:CipherValue>xyzABC...</xenc:CipherValue>
</xenc:CipherData>
            <xenc:ReferenceList>
                  <xenc:DataReference URI="#Encrypted_DATA_ID"/>
            </xenc:ReferenceList>


<xenc:CarriedKeyName>MULTICAST_KEY_NAME</xenc:CarriedKeyName>
      </xenc:EncryptedKey>
```

```
<xenc:EncryptedKey xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
Id="Encrypted_KEY_ID_2" Recipient="https://sp2.org">
            <xenc:EncryptionMethod

      Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
            <ds:KeyInfo
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:KeyName>KEY_NAME_2</ds:KeyName>
            </ds:KeyInfo>
            <xenc:CipherData>
<xenc:CipherValue>abcXYZ...</xenc:CipherValue>
</xenc:CipherData>
            <xenc:ReferenceList>
                  <xenc:DataReference URI="#Encrypted_DATA_ID"/>
            </xenc:ReferenceList>


<xenc:CarriedKeyName>MULTICAST_KEY_NAME</xenc:CarriedKeyName>
      </xenc:EncryptedKey>
</saml:EncryptedAssertion>
```

Disposition: During the TC conference call on 5/23/06, the TC approved the changes as stated here.

E45: AuthnContext comparison clarifications

First reported by: Scott Cantor, OSU

Message: http://www.oasis-open.org/archives/security-services/200602/msg00024.html

Document: Core

Description: In section 3.3.2.2.1 contexts are not necessarily a fully ordered set. This should be noted to aid in the interpretation of the comparison types.

Options:

Replace the paragraph at 1815-1819 with:

Either a set of class references or a set of declaration references can be used. If ordering is relevant to the evaluation of the request, then the set of supplied elements MUST be evaluated as an ordered set, where the first element is the most preferred authentication context class or declaration. For example, ordering is significant when using this element in an

<AuthnRequest> message but not in an <AuthnQuery> message.

If none of the specified classes or declarations can be satisfied in accordance with the rules below, then the responder MUST return a <Response> message with a second-level <StatusCode> of urn:oasis:names:tc:SAML:2.0:status:NoAuthnContext."

Change current lines 1825-1827 to:

If Comparison is set to "better", then the resulting authentication context in the authentication statement MUST be stronger (as deemed by the responder) than one of the authentication contexts specified."

Disposition: During the conference call of 3/28/06 TC voted to approve changes as stated here

E46: AudienceRestriction clarifications

First reported by: Connor P. Cahill, Intel

Message: http://www.oasis-open.org/archives/security-services/200603/msg00001.html

Document: Core

Description: On lines 922-925 in the core specification for 2.0, the sentence states:

The effect of this requirement and the preceding definition is that within a given condition, the audiences form a disjunction (an "OR") while multiple conditions form a conjunction (an "AND")

Options: Clarify by modifying these lines to read as follows:

The effect of this requirement and the preceding definition is that within a given <AudienceRestrictions>, the <Audience>s form a disjunction (an "OR") while multiple <AudienceRestrictions> form a conjunction (an "AND").

Disposition: During the conference call of 5/9/06 the TC approved the change as proposed here.

E47: Clarification on SubjectConfirmation

First reported by: Scott Cantor, OSU

Message: http://www.oasis-open.org/archives/security-services/200603/msg00008.html

Document: Core and profiles

Description: The language on Subject Confirmation element and the intent of the embedded secondary identifier requires clarification.

Options:

Insert the following at line 698 of core

If the <SubjectConfirmation> element in an assertion subject contains an identifier the issuer authorizes the attesting entity to wield the assertion on behalf of that subject. A relying party MAY apply additional constraints on the use of such an assertion at its discretion, based upon the identities of both the subject and the attesting entity.

If an assertion is issued for use by an entity other than the subject, then that entity SHOULD be identified in the <SubjectConfirmation> element."

Replace lines 335-337 in Profiles with:

As described in [XMLSig], each <ds:KeyInfo> element holds a key or information that enables an application to obtain a key. The holder of one or more of the specified keys is considered to be an acceptable attesting entity for the assertion by the asserting party.

Insert the following at line 341 of Profiles

"If the keys contained in the <SubjectConfirmationData> element belong to an entity other than the subject, then the asserting party SHOULD identify that entity to the relying party by including a SAML identifier representing it in the enclosing <SubjectConfirmation> element.

Note that a given <SubjectConfirmation> element using the Holder of Key method SHOULD include keys belonging to only a single attesting entity. If multiple attesting entities are to be permitted to use the assertion, then multiple <SubjectConfirmation> elements SHOULD be included.

Replace lines 361-363 in Profiles with:

The bearer of the assertion is considered to be an acceptable attesting entity for the assertion by the asserting party, subject to any optional constraints on confirmation using the attributes that MAY be present in the <SubjectConfirmationData> element, as defined by [SAMLCore].

If the intended bearer is known by the asserting party to be an entity other than the subject, then the asserting party SHOULD identify that entity to the relying party by including a SAML identifier representing it in the enclosing <SubjectConfirmation> element.

If multiple attesting entities are to be permitted to use the assertion based on bearer semantics, then multiple <SubjectConfirmation> elements SHOULD be included."

Disposition: During the conference call of 3/28/06 TC voted to approve changes as stated here

E48: Clarification on encoding for binary values in LDAP profile

First reported by: Greg Whitehead, HP

Message: http://www.oasis-open.org/archives/security-services/200603/msg00034.html

Document: Profiles

Description: In describing the encoding for binary values, the LDAP profile text is ambiguous about whether the ASN.1 OCTET STRING wrapper should be included or not.

Options:
Change line 1762 of Profiles to:
... by base64-encoding [RFC2045] the contents of the ASN.1 OCTET STRING-encoded LDAP attribute value (not including the ASN.1 OCTET STRING wrapper)

Disposition: During the conference call of 5/09/06 TC voted to approve changes as stated here

E49: Clarification on attribute name format

First reported by: Greg Whitehead, HP

Message: http://www.oasis-open.org/archives/security-services/200603/msg00034.html

Document: Core

Description: The relationship between an attribute's `NameFormat` and its syntax is not clear.

Options:

Add the following text after line 1217 of core:
Attributes are identified/named by the combination of the NameFormat and Name XML attributes described above. Neither one in isolation can be assumed to be unique, but taken together, they ought to be unambiguous within a given deployment.
The SAML profiles specification [SAMLProf] includes a number of attribute profiles designed to improve the interoperability of attribute usage in some identified scenarios. Such profiles typically include constraints on attribute naming and value syntax. There is no explicit indicator when an attribute profile is in use, and it is assumed that deployments can establish this out of band, based on the combination of NameFormat and Name.

Disposition: During the TC conference call on 7/18 the TC approved the changes as stated here

E50: Clarification SSL Ciphersuites

First reported by: Eric Tiffany, Liberty Alliance

Message: http://www.oasis-open.org/archives/security-services/200604/msg00030.html

Document: Conformance

Description: The text needs to be clarified based on ciphersuites that were explicitly called out in the text. This is required to make it clear that:

1. these are not the only ones that are supported, and
2. this is not a minimal set that needs to be supported.

Options:

Change the following in the Conformance document:

1. In the intro of section 4 (XML Digital Signature and XML Encryption) after line 235, add:
   - The algorithms listed below as being required for SAML 2.0 conformance are based on the mandated algorithms in the W3C recommendations for XML Signature and for XML Encryption, but modified by the SSTC to ensure interoperability of conformant SAML implementations. While the SAML-defined

set of algorithms is a minimal set for conformance, additional algorithms supported by XML Signature and XML Encryption MAY be used. Note, however, that the use of non-mandated algorithms may introduce interoperability issues if those algorithms are not widely implemented. As additional algorithms become mandated for use in XML Signature and XML Encryption, the set required for SAML conformance may be extended. [RSP: not sure about including the last sentence… opinions?]

1. In the intro of section 5 (Use of SSL 3.0 and TLS 1.0) after line 257, add:
   - The set up algorithms required for SAML 2.0 conformance is equivalent to that defined in SAML 1.0 and SAML 1.1. These mandated algorithms were chosen by the SSTC because of their wide implementation support in the industry. While the algorithms defined below are the minimal set for SAML conformance, additional algorithms supported by SSL 3.0 and TLS 1.0 MAY be used.

Disposition: During the conference call of 5/23/06 TC voted to approve changes as stated here

E51: Schema type of contents of <AttributeValue>

First reported by: Prateek Mishra, Oracle

Message: http://lists.oasis-open.org/archives/security-services/200605/msg00001.html

Document: Profiles

Description: Section 8.1 of SAML 2 Profiles state:

The Basic attribute profile specifies simplified, but non-unique, naming of SAML attributes together with attribute values based on the built-in XML Schema data types, eliminating the need for extension schemas to validate syntax.

Further in the document, lines (1699-70) it states:
The schema type of the contents of the <AttributeValue> element MUST be drawn from one of the types defined in Section 3.3 of [Schema2].

This appears to be in error. Section 3 of [Schema2] defines the "Built-in Datatypes" and Section 3.3 is one specific sub-section within it (defines "Derived Datatypes"). With the current language both "Date" and "anyURI" are excluded; I somehow do not believe this was the original intent.

Options: Replace lines 1699-70 with:

The schema type of the contents of the <AttributeValue> element MUST be drawn from one of the types defined in Section 3 of [Schema 2].

Disposition: During the TC conference call on 5/9 the TC approved the changes as proposed here

E52: Clarification on <NotOnOrAfter> attribute

First reported by: Rob Philpott, RSA Security

Message: http://lists.oasis-open.org/archives/security-services/200605/msg00007.html

Document: Profiles

Description: Line 556-7: "a `NotOnOrAfter` attribute that limits the window during which the assertion can be delivered."

The NotOnOrAfter in a ConfirmationData element isn't about a window when the assertion can be delivered. Core defines it as being the time after which the subject cannot be confirmed. That's independent of assertion delivery

Options:

Changes Profiles lines 556-7 from:

"a `NotOnOrAfter` attribute that limits the window during which the assertion can be delivered"

to:

"a `NotOnOrAfter` attribute that limits the window during which the recipient can perform a confirmation of the assertion <Subject>".

Disposition: During the TC conference call on 15 Aug 2006 the TC modified the wording to read "...during which the assertion can be confirmed by the relying party" and approved the change.

E53: Correction to LDAP/X.500 profile attribute

First reported by: Scott Cantor, OSU

Message: http://lists.oasis-open.org/archives/security-services/200605/msg00004.html

Document: Profiles

Description: The X.500/LDAP attribute profile is schema-invalid right now because we tell people to specify xsi:type="xsd:string" but then add our own X500:Encoding attribute into the AttributeValue element. That's illegal. Any fix would be a normative change to the profile, so either it has to be fixed or create a new profile and deprecate the original.

Options:

1. Remove the xsi:type requirement.
   Forces implementations to recognize string vs base64 encoding based on Attribute Name.

2. Remove the x500:Encoding attribute.
   Forces implementations to trigger profile behavior based on Attribute Namespace and Name, encoding rules are implied.
3. Move the x500:Encoding attribute to the Attribute element.
   Suggests that future encoding rules will be uniform across all values of an attribute, but otherwise fully consistent with intent of profile.

4. Define an extended schema type that extends string and base64Binary with the x500:Encoding attribute and change the mandated xsi:type values to the extended types.
   Least change to existing profile behavior, but requires publishing and approving an additional schema document.
5. Deprecate the existing profile and define a new one incorporation whatever input can be gleaned from implementers.
6. A variation on 2 and 3, which is to:
   a. remove the x500:Encoding attribute and document that the LDAP encoding uses xsi:type string and base64Binary
   b. document that other encodings should define new types

Disposition: During the TC conference call on 6/20 the TC approved option 3 (which subsumes option 5) but subsequently decided that this would be a substantive change, such that the profile would have to be deprecated once a replacement profile could be specified. At the 16 January 2007 TC telecon we agreed it's now safe to mention the (still-draft) new profile and do the deprecation.

E54: Correction to ECP URN

First reported by: Thomas Wisniewski, Entrust

Message: http://lists.oasis-open.org/archives/security-services/200606/msg00019.html

Document: Profiles

Description:

Line 757: The reference to the ecp urn should be in double quotes.

Lines 763 - 764: In the example, the reference to the ecp urn and the PAOS version should be in double quotes instead of single quotes.

Both of these seem incorrect based on the PAOS specification lines 95 - 100.

Disposition: During the TC conference call on 6/20 the TC approved to make the changes as stated here.

E55: Various Language Cleanups

First reported by: Scott Cantor, OSU

Message: http://lists.oasis-open.org/archives/security-services/200606/msg00026.html

Document: Core and Profiles

Description: This erratum attempts to capture all language cleanup in light of repeated questions. The goal here is to clarify these fundmantal issues:

- NameIDMgmt applies to most of the formats
- NameIDMgmt affects only a given identifier for a principal, not every possible identifier that might exist for a principal (this is intended as a simplification)

Profiles, line 1319, change "some form of persistent identifier" to "some form of long-term identifier (including but not limited to identifiers with the Format urn....persistent)"

Profiles, line 1323, change "about the principal" to "using that identifier".

Core, lines 3337-3339, I'm inclined to say that text should be struck.

Core, line 2477, change "it will no longer issue assertions to the SP about the principal" to "it will no longer issue assertions to the SP using that identifier". This does step on an errata, but is a separate change from it.

Core, line 2483, change "regarding this principal" to "using the primary identifier".

Core, line 2487-8, change "regarding this principal" to "in any case where the identifier being changed would have been used".

Disposition: During the TC conference call on 8/15 the TC approved the changes as proposed here

E56: Typo in Profiles

First reported by: Eric Tiffany, Liberty Alliance

Message: http://lists.oasis-open.org/archives/security-services/200606/msg00021.html

Document: Profiles

Description: Line 326 of profiles states:

"It is anticipated that profiles will define and use several different values for <ConfirmationMethod>"

The last atom should be "Method" as there is not any<ConfirmationMethod> element in the SAML schema.

Disposition: During the conference call on 7/18 the TC approved to making the changes as stated here.

E57: SAMLMime Reference

First reported by: Jeff Hodges, Nustar

Message: http://lists.oasis-open.org/archives/security-services/200606/msg00036.html

Document: Bindings

Description: The [SAMLmime] reference in saml-bindings-2.0-os lines 1468-1469 reads as:

[SAMLmime] application/saml+xml Media Type Registration, IETF Internet-Draft, http://www.ietf.org/internet-drafts/draft-hodges-saml-mediatype-01.txt.

The document draft-hodges-saml-mediatype-01 expired (and thus was deleted from the I-D repository), since we ended up using the new "fast track" MIME Media Type registration process rather than publishing an RFC.

Options: The reference should be replaced with a reference similar to

[SAMLmime] OASIS Security Services Technical Committee (SSTC), "application/samlassertion+xml MIME Media Type Registration", IANA MIME Media Types Registry application/samlassertion+xml, December 2004. http://www.iana.org/assignments/media-types/application/samlassertion+xml

Disposition: During the TC conference call on 7/18 the TC approved the changes as stated here

E58: Typos in Profiles

First reported by: Tom Scavo, NCSA/University of Illinois

Message: http://www.oasis-open.org/archives/security-services/200607/msg00049.html

Document: Profiles

Description: There are two minor errors in the profiles document on lines 626 and 627.

Options:

On line 626 change “sign” to “signing”

On line 627 change “encrypt” to “encryption”

Disposition: During the TC conference call on 8/15 the TC approved the changes as proposed here

E59: SSO Response when using HTTP-Artifact

First reported by: Rob Phillpot, RSA Security

Message: http://www.oasis-open.org/archives/security-services/200509/msg00019.html

Document: Bindings

Description: The specification mandates support for the HTTP Artifact binding for a Web SSO <Response> in full and Lite versions of IDP's and SP's. However, the spec does not indicate what mechanisms (HTTP Redirect or HTTP POST) are mandated for delivery of the artifact.

Options:

Insert a clarifying paragraph after line 1173 of Bindings:

"Finally, note that the use of the Destination attribute in the root SAML element of the protocol message is unspecified by this binding, because of the message indirection involved."

Disposition: During the TC conference call on 8/15 the TC approved the changes as proposed here

E60: Incorrect URI

First reported by: Tom Scavo, NCSA/University of Illinois

Message: http://lists.oasis-open.org/archives/security-services/200608/msg00069.html

Document: Core

Description: Line 460 references the URI

```
urn:oasis:names:tc:SAML:1.0:nameid-format:unspecified.
```

This is incorrect and should be replaced with

```
urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
```

Options:

Disposition: During the TC conference call on 8/29, the TC approved the changes as proposed here.

E61 Reference to non-existent element

First reported by: Tom Scavo, NCSA/University of Illinois

Message: http://lists.oasis-open.org/archives/security-services/200608/msg00075.html

Document: Core

Description: Line 3160 of core refers to the <Request> element. This is a non-existent element.

Options: Delete line 3160

Disposition: During the TC conference call on 8/29 the TC approved the changes as proposed here. (Additional edits proposed, in order to make sense of the text that remains. Scheduled to be brought up in 13 Feb 2007 telecon again for final approval.)

E62: TLS Keys in KeyDescriptor

First reported by: Scott Cantor on security-services list

Message: http://lists.oasis-open.org/archives/security-services/200612/msg00034.html

Document: Metadata

Description: The Metadata specification is underspecified with regard to how to interpret the KeyDescriptor element's "use" attribute and how TLS keys are expressed.

Options: Scott proposes one solution: Insert text after line 624 of Metadata:

> A use value of "signing" means that the contained key information is applicable to both signing and TLS/SSL operations performed by the entity when acting in the enclosing role.
>
> A use value of "encryption" means that the contained key information is suitable for use in wrapping encryption keys for use by the entity when acting in the enclosing role.
>
> If the use attribute is omitted, then the contained key information is applicable to both of the above uses.

He further comments: “If "wrapping encryption keys" isn't a precise enough term, please find some crypto experts to clarify it... It's worth noting to the TC that this doesn't even scratch the surface of the problems with KeyInfo interop, and spec and product users are starting to notice...”

Disposition: During the TC conference call on 16 January 2007 the TC approved the changes as proposed here.

E63: IdP Discovery Cookie Interpretation

First reported by: Scott Cantor on security-services list

Message: http://lists.oasis-open.org/archives/security-services/200612/msg00035.html

Document: Profiles

Description: There is confusion over how the contents of an IdP Discovery cookie are meant to be interpreted because of the allowance for specifying either persistent or session lifetime.

Options: Scott proposes one solution: In Profiles Section 4.3, insert the following paragraph after line 1105:

> Note that while a session-only cookie can be used, the intent of this profile is not to provide a means of determining whether a user actually has an active session with one or more of the identity providers stored in the cookie. The cookie merely identifies identity providers known to have been used in the past. Service providers MAY instead rely on the IsPassive attribute in their samlp:AuthnRequest message to probe for active sessions.

Disposition: During the TC conference call on 16 January 2007 the TC approved the changes as proposed here.

E64: Liberty Moniker Used Inappropriately

First reported by: Jeff Hodges on security-services list

Message: http://lists.oasis-open.org/archives/security-services/200702/msg00047.html

Document: SecConsider

Description: Section 7.1.1.9, Impersonation without Reauthentication, contains the following text:

> Cookies posted by identity providers MAY be used to support this validation process, though **Liberty** does not mandate a cookie-based approach.

Options: The reference to Liberty should be changed to a reference to SAML V2.0, as follows:

> Cookies posted by identity providers MAY be used to support this validation process, though **SAML V2.0** does not mandate a cookie-based approach.

Disposition: During the TC conference call on 27 Feb 2007, the TC approved the changes as proposed here.

E65: Second-level StatusCode

First reported by: Philpott**,** Robert, EMC

Message: http://lists.oasis-open.org/archives/security-services/200708/msg00053.html

Document:**:** SAML Core

Description: There are several places in SAML Core that are currently mandating the return of second-level `<StatusCode>` elements, which for security reasons are assumed to be optional.

Options: Reword the relevant sections to indicate that use of a second-level code is optional, but if present, the value is constrained.

Change section 3.3.2.2.1 Element `<RequestedAuthnContext>`, lines 1817-1819, to:

> If none of the specified classes or declarations can be satisfied in accordance with the rules below, then the responder MUST return a `<Response>` message with a top-level `<StatusCode>` value of `urn:oasis:names:tc:SAML:2.0:status:Responder` and MAY return a second-level `<StatusCode>` value of `urn:oasis:names:tc:SAML:2.0:status:NoAuthnContext`.

Change section 3.4.1.2, lines 2172-2173, to:

> In profiles specifying an active intermediary, the intermediary MAY examine the list and return a `<Response>` message with an error `<Status>` and optionally a second-level `<StatusCode>` of

Change section 3.4.1.5.1 Proxy Processing Rules, lines 2282-2285, to:

> Unless the identity provider can directly authenticate the presenter, it MUST return a `<Response>` message with a top-level `<StatusCode>` value of `urn:oasis:names:tc:SAML:2.0:status:Responder` and MAY return a second-level `<StatusCode>` value of `urn:oasis:names:tc:SAML:2.0:status:ProxyCountExceeded`.

Change section 3.8.3, lines 2729-2731:

> If the responder does not recognize the principal identified in the request, it MAY respond with an error `<Status>`, optionally containing a second-level `<StatusCode>` of `urn:oasis:names:tc:SAML:2.0:status:UnknownPrincipal`.

Disposition: During the TC conference call on 11 March 2008 the TC approved the changes as proposed here.

E66: Metadata and DNSSEC

First reported by: Peter Davis, Neustar

Message: http://lists.oasis-open.org/archives/security-services/200709/msg00014.html

Document: SAML Metadata

Description: The metadata specification references RFC 2535, which has been obsoleted by RFC 4035.

Options: Make the following changes:

Change line 1253 to the following:

> It is RECOMMENDED that entities publish their resource records in signed zone files using [RFC4035]

Substitute the following for lines 1447-1448:

> [RFC4035] R. Arends et al. Protocol Modifications for the DNS Security Extensions. IETF RFC 4035, March 2005. See http://www.ietf.org/rfc/rfc4035.txt.

Disposition: During the TC conference call on 11 March 2008 the TC approved the changes as proposed here.

E68: Use of Multiple <KeyDescriptor> Elements

First reported by: Scott Cantor, Internet2

Message: http://lists.oasis-open.org/archives/security-services/200802/msg00066.html

Document: SAML Metadata

Description: The metadata specification is silent about the meaning of multiple <KeyDescriptor> elements with the same use attribute.

Options: Insert text before line 625:

> The inclusion of multiple <KeyDescriptor> elements with the same use attribute (or no such attribute) indicates that any of the included keys may be used by the containing role or affiliation. A relying party SHOULD allow for the use of any of the included keys. When possible the signing or encrypting party SHOULD indicate as specifically as possible which key it used to enable more efficient processing.

Disposition: During the TC conference call on 11 March 2008 the TC approved the changes as proposed here.

E69: Semantics of <ds:KeyInfo> in <KeyDescriptor>

First reported by: Scott Cantor, Internet2

Message: http://lists.oasis-open.org/archives/security-services/200802/msg00066.html

Document: SAML Metadata

Description: The metadata specification is silent about the semantic interpretation of the <ds:KeyInfo> element as it pertains to communicating keys that may be wielded by an entity.

Options: Insert text before line 625:

> The <ds:KeyInfo> element is a highly generic and extensible means of communicating key material. This specification takes no position on the allowable or suggested content of this element, nor on its meaning to a relying party. As a concrete example, no implications of including an X.509 certificate by value or reference are to be assumed. Its validity period, extensions, revocation status, and other relevant content may or may not be enforced, at the discretion of the relying party. The details of such processing, and their security implications, are out of scope; they may, however, be addressed by other SAML profiles.

Disposition: During the TC conference call on 11 March 2008 the TC approved the changes as proposed here.

E70: Obsolete reference to UUID URN namespace

First reported by: Tom Scavo, NCSA

Message: http://lists.oasis-open.org/archives/security-services/200801/msg00001.html

Document: SAML Profiles

Description: The normative reference to an I-D at lines 2111-2112 of the profiles specification is obsolete and was replaced by an actual RFC.

Options: Replace the reference at lines 2111-212 with a reference to:

> P. Leach et al. *A Universally Unique IDentifier (UUID) URN Namespace*. IETF RFC 4122, July 2005. See http://www.ietf.org/rfc/rfc4122.txt.
>
> Also adjust the references to same at lines 1836 and 1885, which currently include the entire URL rather than a shorthand ref name.

Disposition: During the TC conference call on 25 March 2008 the TC approved the changes as proposed here.

E71: Missing namespace definition in Profiles

First reported by: Tom Scavo, NCSA

Message: http://lists.oasis-open.org/archives/security-services/200802/msg00000.html

Document: SAML Profiles

Description: The namespace prefix xs:, used repeatedly in section 8 of [SAML2Prof], is not defined in section 1 of the same document.

Options: Add the namespace definition to the table in section 1.

Disposition: During the TC conference call on 25 March 2008 the TC approved the changes as proposed here.

3 Proposed Errata

These proposed errata, given a "PE*nn*" number designation, have either been determined by the SSTC not to be resolvable with a "non-substantive" change or, in the case of PEs with "[OPEN]" in the title, have not been considered by the SSTC yet.

PE3: Supported URL Encoding

First reported by: Scott Cantor, OSU

Message: http://lists.oasis-open.org/archives/security-services/200501/msg00058.html

Document: Metadata

Description: Specify the URL encoding supported by an HTTP Redirect binding endpoint.

Options: This isn't actually an erratum, it's a missing piece that doesn't currently break anything but could in the future if alternate URL encodings for the Redirect binding emerge (for example a binary XML representation). We need an extension attribute to indicate non-default encoding support, it can just be added to our new "2.0 metadata extension schema". This should be moved to the issues list.

Disposition: During the conference call of April 12 the TC agreed to move this to the issues list.

PE15: NameID Policy (Reopened)

First reported by: Thomas Wisniewski, Entrust

Message: http://lists.oasis-open.org/archives/security-services/200506/maillist.html - 00030

Document: Core

Description: The returned assertion subject's NameID format and/or SPNameQualifier may be different from the ones suggested in the authentication request's NameIDPolicy. I.e., the spec does not explicitly forbid these from being different (which it should).

Options: Insert the following text between lines 2139 and 2140 in core

When a `Format` defined in Section 8.3.7 is used other than `urn:oasis:names:TC:SAML:1.1:nameid-format:unspecified` or `urn:oasis:names:TC:SAML:2.0:nameid-format:encrypted`, then if the identity provider returns any assertions:

- the `Format` value of the `<NameID>` within the `<Subject>` of any `<Assertion>` MUST be identical to the `Format` value supplied in the `<NameIDPolicy>`, and
- if `SPNameQualifier` is not omitted in `<NameIDPolicy>`, the `SPNameQualifier` value of the `<NameID>` within the `<Subject>` of any `<Assertion>` **MUST** be identical to the `SPNameQualifier` value supplied in the `<NameIDPolicy>`."

Disposition: Open

PE23: Metadata for <ArtifactResolutionService>

First reported by: Nick Ragouzis, Enosis Group

Message: http://lists.oasis-open.org/archives/security-services/200507/msg00036.html

Document: Profiles

Description: The text is not as clear as it should be. In Section 4.1.6 (Web Browser SSO Profile), at Line 639 change "MUST" to "SHOULD". Also, add the following text:

If the request or response message is delivered using the HTTP Artifact binding, the artifact issuer SHOULD provide at least one <md:ArtifactResolutionService> endpoint element in its metadata.

Options: Accept changes as suggested here.

Disposition: During the call on 2/28 the TC moved to close with no resolution

---

PE67: Absence of elements in metadata (Open)

First reported by: Scott Cantor, Internet2

Message: http://lists.oasis-open.org/archives/security-services/200802/msg00066.html

Document: SAML Metadata

Description: The metadata specification is ambiguous about the meaning of omission of the <NameIDFormat> element and many other elements such as <AttributeProfile>, <KeyDescriptor>, and generally anything that's optional.

Options: Supplement the note at lines 165-172 with a new paragraph:

> In the absence of other sources of information, implementations SHOULD generally view the absence of particular elements as implying that any values supported by the consuming implementation are acceptable, with the obvious exception of metadata elements representing roles, endpoints, keys, etc. (elements that cannot be "defaulted" or that would be security-sensitive if assumed). Alternatively, the presence of particular elements SHOULD generally constrain the choices made by the consuming implementation.
>
> Of course, if other sources of information are available, implementations are free to combine it with, or override, the information found in metadata, as appropriate to that implementation and deployment.

Disposition: Open. Scott to supply reworked text.

Appendix A.Revision History

Rev	Date	By Whom	What
Draft-00	2005-01-31	Jahan Moreh	Initial version based on emails to the list
Draft-01	2005-02-14	Jahan Moreh	Removed E5 as it is related to the Technical Overview document, which is work in progress. Relabeled all items as Potential Errata (PE). Added PE4 and PE5. Added E1.
Draft-02	2005-03-27	Jahan Moreh	Moved E1 to PE section. Added E2,E3 and E4. Added PE7
Draft-03	2005-03-29	Jahan Moreh	Rearranged E and PE items. The E items now are those which have been resolved and have proposed text, where required. PE items will be moved to E as they meet these requirements.
Draft-04	2005-04-11	Jahan Moreh	Incorporated proposes text all Pes based on emails to the list:
Draft-05	2005-04-12	Jahan Moreh	Minor corrections to PE5 and PE8. Accepted disposition of all items except PE5, PE7 and PE10. Decided to keep disposed Pes in the PE section (and not move them to the E section)
Draft-06	2005-04-25	Jahan Moreh	Added PE11, PE12 and PE13
Draft-07	2005-05-27	Jahan Moreh	Added PE14
Draft-08	2005-06-03	Jahan Moreh	Added PE15
Draft-09	2005-06-20	Jahan Moreh	Added PE16. Disposed PE11, PE12, PE13, and PE16 and PE17.
Draft 10	2005-07-04	Jahan Moreh	Added PE18
Draft 11	2005-07-18	Jahan Moreh	Disposed PE17, added PE19 and PE20
Draft 12	2005-08-01	Jahan Moreh	Disposed PE18, PE19 and PE20. Added PE21-PE25.
Draft 13	2005-08-15	Jahan Moreh	Closed PE19, PE22, PE24. Added PE26.
Draft 14	2005-08-29	Jahan Moreh	Updated PE26

Rev	Date	By Whom	What
Draft 15	2005-09-12	Jahan Moreh	Closed PE26, added PE27-34
Draft 16	2005-09-26	Jahan Moreh	Added PE35. Closed PE30, PE33 and PE34
Draft 17	2005-10-10	Jahan Moreh	Closed PE7, PE25, PE27-29, PE31, PE35.
Draft 18	2005-10-24	Jahan Moreh	Added PE36
Draft 19	2005-11-07	Jahan Moreh	Closed PE36
Draft 20	2005-11-21	Jahan Moreh	Added PE37 and PE38
Draft 21	2005-12-05	Jahan Moreh	Closed PE37 and PE38. Added text for PE32.
Draft 22	2006-01-30	Jahan Moreh	Added PE39, PE40, PE41, PE42 and 43
Draft 23	2006-02-13	Jahan Moreh	Closed PE39, PE41. Added PE44.
Draft 24	2006-02-27	Jahan Moreh	Closed PE10 and added PE45. Modified description and option for correcting PE 35.
Draft 24	2006-02-27	Jahan Moreh	Closed PE10 and added PE45. Modified description and option for correcting PE 35.
Draft 25	2006-03-27	Jahan Moreh	Closed PE23, PE35, PE40. Added PE46 and PE47.
Draft 26	2006-04-10	Jahan Moreh	Closed PE44, PE45 and PE47. Added PE48.
Draft 27	2006-04-24	Jahan Moreh	Split PE48 into two PEs (48 and 49).
Draft 28	2006-05-05	Jahan Moreh	Added PE50 and PE51
Draft 29	2006-05-22	Jahan Moreh	Closed PE46, PE48 and PE51. Added PE52 and PE53
Draft 30	2006-06-05	Jahan Moreh	Closed PE43 and PE50. Updated PE53
Draft 31	2006-06-19	Jahan Moreh	Added PE54
Draft 32	2006-07-17	Jahan Moreh	Added PE55, PE56, PE57 and PE58. Updated PE49
Draft 33	2006-07-31	Jahan Moreh	Replaced PE58. Closed PE49, PE56, PE57. Added PE59.
Draft 34	2006-08-28	Eve Maler and Jahan	Reformatting and clean up.

Rev	Date	By Whom	What
		Moreh	
Draft 35	2006-09-11	Jahan Moreh	Closed PE52, PE55, PE58, and PE59. Added and closed PE60 and PE61.
Draft 36	2006-09-21	Jahan Moreh	Renamed all approved PEs as Es keeping the original numbers. Renamed E1 to E0. Changed Summary of Disposition table to reflect new E #'s.
Draft 37	2006-12-19	Eve Maler	Added PE62 and PE63.
Draft 38	2007-01-14	Eve Maler	Cleanup in accordance with final decisions made by TC (verified by review of the errata composite documents and the creation of the standards-track errata document) and to prepare for eventual final publication of the whole set of documents.
Draft 39	2007-02-12	Eve Maler	Closed PE62 (->E62) and PE63 (->E63). Did a litle more editorial distinction around this document vs. the other errata-related documents.
Draft 40	2007-03-04	Eve Maler	Opened (and immediately closed) E64.
Draft 41	2007-10-12	Abbie Barbir	Added PE64 and PE65
Draft 42	2008-02-29	Scott Cantor	Cleaned up PE65 and PE66. Removed any PE that was disposed of as part of an approved errata item but left in the document. Added (Open) to title of undisposed PE items. Added PE67, PE68, PE69.
Draft 43	2008-03-24	Scott Cantor	Closed PE65, PE66, PE68, P69. Added PE70, PE71, PE72. Reworded PE67.
Draft 44	2008-05-06	Scott Cantor	Closed PE70, PE71. Reopened E15 in place of PE72.

1613

Appendix B.Summary of Disposition

Erratum #	*Status*	*Document*
E0	Closed	Core
E1	Closed	Bindings
E2	Closed	Bindings
PE3	Closed	Metadata
E4	Closed	Binding
PE5	Closed	Binding/Profiles
E6	Closed	Core
E7	Closed	Metadata
E8	Closed	Core
PE9	Closed – combined with PE7	Metadata
E10	Closed	Core
E11	Closed	Conformance
E12	Closed	Core/Profiles
E13	Closed	Core
E14	Closed	Core/Profiles
E15	Closed	Core
PE16	Closed	Conformance
E17	Closed	Profiles
E18	Closed	Profiles
E19	Closed	Bindings
E20	Closed	Profiles
E21	Closed	Bindings
E22	Closed	Profiles
PE23	Closed	Profiles
E24	Closed	Bindings

Erratum #	*Status*	*Document*
E25	Closed	Conformance
E26	Closed	Profiles
E27	Closed	Profiles
E28	Closed	Conformance
E29	Closed	Conformance
E30	Closed	Core
E31	Closed	Bindings
E32	Closed	Profiles
E33	Closed	Metadata
E34	Closed	Metadata
E35	Closed	Profiles
E36	Closed	Core
E37	Closed	Metadata
E38	Closed	Core/Profiles
E39	Closed	Profiles
E40	Closed	Profiles
E41	Closed	Metadata
E42	Closed	Conformance
E43	Closed	Core
PE44	Closed – combined with PE47	Placeholder for Constrained Delegation
E45	Closed	Core
E46	Closed	Core
E47	Closed	Core/Profiles
E48	Closed	Profiles
E49	Closed	Core
E50	Closed	Conformance
E51	Closed	Profiles
E52	Closed	Profiles

Erratum #	*Status*	*Document*
E53	Closed	Profiles
E54	Closed	Profiles
E55	Closed	Core/Profiles
E56	Closed	Profiles
E57	Closed	Bindings
E58	Closed	Profiles
E59	Closed	Bindings
E60	Closed	Core
E61	Closed	Core
E62	Closed	Metadata
E63	Closed	Profiles
E64	Closed, not incorporated in the Errata	SecConsider
E65	Closed	Core
E66	Closed	Metadata
PE67	Open	Metadata
E68	Closed	Metadata
E69	Closed	Metadata
E70	Closed	Profiles
E71	Closed	Profiles
PE72	Closed, reopened as change to PE15.	Core

Appendix C. Acknowledgments

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

- TBS

The editors also would like to gratefully acknowledge Jahan Moreh of Sigaba, who during his tenure on the SSTC was the primary editor of this errata document and who made major substantive contributions to all of the errata materials.