Abstract:
This specification defines an extension to the SAML V2.0 protocol specification [SAML2Core] that facilitates requests made by parties other than the intended response recipient. Protocol extensions enable extension-aware SAML requesters and responders to modify protocol behavior in a generic, layered fashion. Readers should be familiar with [SAML2Core] before reading this document.

Status
This document was last revised or approved by the SSTC on the above date. The level of approval is also listed above.
Technical Committee members should send comments on this specification to the Technical Committee’s email list. 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/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 (http://www.oasis-open.org/committees/security/ipr.php).
# Table of Contents

1 Introduction.................................................................................................................................4
  1.1 Notation.................................................................................................................................4
2 Third-Party Request SAML Protocol Extension........................................................................5
  2.1 Required Information.............................................................................................................5
  2.2 Profile Overview....................................................................................................................5
  2.3 Element <thrpty:RespondTo>...............................................................................................5
  2.4 Processing Rules....................................................................................................................5
  2.5 Unsolicited Responses............................................................................................................6
  2.6 Metadata Considerations.......................................................................................................6
    2.6.1 Metadata Example............................................................................................................6
3 References....................................................................................................................................7
  3.1 Normative References............................................................................................................7
Appendix A. Acknowledgements.................................................................................................8
Appendix B. Notices.....................................................................................................................9
1 Introduction

Protocol extensions consist of elements defined for inclusion in the `<samlp:Extensions>` element that modify the behavior of SAML requesters and responders when processing extended protocol messages. This specification defines an extension to the SAML V2.0 protocol specification that overrides the implicit relationship between the issuer of a request and the intended response recipient. Normally these are the same entity. The use of this extension allows a third party to make a request on behalf of another entity to whom the response should be delivered.

1.1 Notation

This specification uses normative text. The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this specification are to be interpreted as described in [RFC 2119]:

...they MUST only be used where it is actually required for interoperability or to limit behavior which has potential for causing harm (e.g., limiting retransmissions)...

These keywords are thus capitalized when used to unambiguously specify requirements over protocol and application features and behavior that affect the interoperability and security of implementations. When these words are not capitalized, they are meant in their natural-language sense.

Listings of XML schemas appear like this.

Example code listings appear like this.

Conventional XML namespace prefixes are used throughout the listings in this specification to stand for their respective namespaces as follows, whether or not a namespace declaration is present in the example:

<table>
<thead>
<tr>
<th>Prefix</th>
<th>XML Namespace</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>saml:</td>
<td>urn:oasis:names:tc:SAML:2.0:assertion</td>
<td>This is the SAML V2.0 assertion namespace defined in the SAML V2.0 core specification [SAML2Core].</td>
</tr>
<tr>
<td>samlp:</td>
<td>urn:oasis:names:tc:SAML:2.0:protocol</td>
<td>This is the SAML V2.0 protocol namespace defined in the SAML V2.0 core specification [SAML2Core].</td>
</tr>
<tr>
<td>md:</td>
<td>urn:oasis:names:tc:SAML:2.0:metadata</td>
<td>This is the SAML V2.0 metadata namespace defined in the SAML V2.0 metadata specification [SAML2Meta].</td>
</tr>
<tr>
<td>thrpty:</td>
<td>urn:oasis:names:tc:SAML:protocol:ext:third-party</td>
<td>This is the namespace defined by this document and its accompanying schema [ThrPtyExt-xsd].</td>
</tr>
<tr>
<td>xsd:</td>
<td><a href="http://www.w3.org/2001/XMLSchema">http://www.w3.org/2001/XMLSchema</a></td>
<td>This namespace is defined in the W3C XML Schema specification [Schema1]. In schema listings, this is the default namespace and no prefix is shown.</td>
</tr>
<tr>
<td>xsi:</td>
<td><a href="http://www.w3.org/2001/XMLSchema-instance">http://www.w3.org/2001/XMLSchema-instance</a></td>
<td>This is the XML Schema namespace for schema-related markup that appears in XML instances [Schema1].</td>
</tr>
</tbody>
</table>

This specification uses the following typographical conventions in text: `<SAMLElement>`, `<ns:ForeignElement>`, Attribute, Datatype, OtherCode.

Copyright © OASIS Open 2007. All Rights Reserved.
2 Third-Party Request SAML Protocol Extension

2.1 Required Information


Contact information: security-services-comment@lists.oasis-open.org

Description: Given below.

Updates: None

2.2 Profile Overview

This extension defines a mechanism for signaling in a request that the intended recipient of the protocol response is not the request's issuer (that is, the requester is a third party to an exchange between the responder and the eventual recipient). Practically, this has the effect of terminating the initial protocol exchange and producing an unsolicited response to the recipient identified by the extension. It is typically used when message integrity requires that a request be signed, making it impossible for the third party to simply impersonate the intended recipient.

Unless specifically noted, nothing in this document should be taken to conflict with the SAML V2.0 protocol specification [SAML2Core]. Readers are advised to familiarize themselves with that specification first.

2.3 Element <thrpty:RespondTo>

The <thrpty:RespondTo> element, with complex type saml:NameIDType, specifies the intended recipient of the SAML protocol exchange initiated by the containing request. The element requires the use of a string to carry the intended recipient's name, but permits various pieces of descriptive data (see section 2.2.2 of [SAML2Core]).

Overriding the usual rule for this element's type, if no Format attribute is provided with this element, then the value urn:oasis:names:tc:SAML:2.0:nameid-format:entity is in effect (see section 8.3.6 of [SAML2Core]). Note that in such a case, the NameQualifier, SPNameQualifier, and SPProvidedID attributes MUST be omitted, in accordance with that format's definition.

The following schema fragment defines the <thrpty:RespondTo> element:

```
<element name="RespondTo" type="saml:NameIDType"/>
```

2.4 Processing Rules

This extension is included in a protocol request message by placing it in the optional <samlp:Extensions> element. Due to existing processing requirements, all extensions are explicitly deemed optional. Therefore, requesters SHOULD only include this extension when they can be reasonably confident that the extension will be understood by the recipient. The SAML V2.0 metadata extension defined in section 2.6 MAY be used for this purpose.

This extension element MUST NOT be used in conjunction with any protocol message element whose complex type is not derived from the sampl:RequestAbstractType complex type. Moreover, a requester MUST NOT include more than one <thrpty:RespondTo> element in a given request.

If a request message's <samlp:Extensions> element contains a <thrpty:RespondTo> element, then a responder that understands the extension MUST fulfill the request (if it does so at all) by issuing an
unsolicited response message to the entity identified by the extension, or else it SHOULD respond to the request with an error response.

In the event that it successfully processes the request, the responder MUST interpret the non-generic content of the protocol request as though the request was issued by the entity identified by the extension. That is, while generic content such as the `<samlp:Issuer>` element is interpreted in the usual manner, protocol-specific content that affects the response is instead interpreted in the context of the eventual recipient. An example of such content is the `AssertionConsumerServiceIndex` attribute in the `<samlp:AuthnRequest>` element.

If the request is delivered using a SAML protocol binding [SAML2Bind] that supports the notion of "relay state" (data to be communicated unmodified to the protocol recipient), then any state data accompanying the request MUST be passed along to the recipient in accordance with the encoding rules specified by the protocol binding used for the response.

Note that in the event of a successful response, the original requester is not involved in any subsequent interactions within the scope of the SAML protocol exchange.

Specific profiles MAY define additional requirements or processing rules related to this extension, if the desired profile behavior cannot be derived through a self-evident composition of the two.

### 2.5 Unsolicited Responses

As noted earlier, the effect of this extension is to produce an unsolicited response message to the entity identified in the extension.

Many SAML protocols and profiles do not support the notion of an unsolicited response (in fact, in SAML V2.0, only the Browser and Enhanced Client SSO profiles do [SAML2Prof]). The use of this extension in a request used with a protocol or profile that does not provide any processing rules for an unsolicited response is undefined. The use of this extension in conjunction with the SAML SOAP Binding [SAML2Bind] is also undefined.

Note that the processing rule regarding “relay state” defined in the previous section takes precedence over the usual handling of unsolicited responses, which normally permit the responder to attach its own state information with the response.

### 2.6 Metadata Considerations

SAML metadata MAY be used to indicate support for this protocol extension at particular protocol endpoints, using the extension capabilities of the metadata schema.

Support for this extension is expressed in SAML V2.0 metadata [SAML2Meta] by adding a boolean-typed XML attribute to an element derived from the `md:EndpointType` complex type, indicating that SAML request messages sent to that endpoint MAY include this extension.

The following schema fragment defines the `thrpty:supportsRespondTo` attribute:

```xml
<attribute name="supportsRespondTo" type="boolean"/>
```

### 2.6.1 Metadata Example

The example below shows a fragment of an `<md:SingleSignOnService>` element that advertises support for this extension. The namespace declaration must be in scope, but the prefix is of course arbitrary.

```xml
    thrpty:supportsRespondTo="true" .../>
```
3 References

The following works are referenced in the body of this specification.

3.1 Normative References

[RFC 2119] S. Bradner. Key words for use in RFCs to Indicate Requirement Levels. IETF

saml-core-2.0-os. See http://docs.oasis-open.org/security/saml/v2.0/saml-
core-2.0-os.pdf.


[SAML2Prof] S. Cantor et al. Profiles for the OASIS Security Assertion Markup Language

Consortium Recommendation, May 2001. See http://www.w3.org/TR/2001/REC-
xmleschema-1-20010502/.

http://www.oasis-open.org/committees/security/.
Appendix A. Acknowledgements

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

- Hal Lockhart, BEA Systems, Inc.
- Steve Anderson, BMC Software
- Rob Philpott, EMC Corporation
- Carolina Canales-Valenzuela, Ericsson
- Dana Kaufman, Forum Systems
- Ashish Patel, France Telecom
- Greg Whitehead, Hewlett-Packard Company
- Heather Hinton, IBM
- Anthony Nadalin, IBM
- Conor P. Cahill, Intel
- Scott Cantor, Internet2
- Bob Morgan, Internet2
- Tom Scavo, National Center for Supercomputing Applications
- Peter Davis, NeuStar
- Jeff Hodges, NeuStar
- Frederick Hirsch, Nokia
- Abbie Barbir, Nortel
- Paul Madsen, NTT Corporation
- Ari Kermaier, Oracle
- Prateek Mishra, Oracle
- Brian Campbell, Ping Identity
- Bhavna Bhatnagar, Sun Microsystems
- Eve Maler, Sun Microsystems
- Emily Xu, Sun Microsystems
- David Staggs, Veteran's Health Administration
Appendix B. Notices

Copyright © OASIS Open 2007. All Rights Reserved.

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 translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published, and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this section are included on all such copies and derivative works. However, this document itself may not be modified in any way, including by removing the copyright notice or references to OASIS, except as needed for the purpose of developing any document or deliverable produced by an OASIS Technical Committee (in which case the rules applicable to copyrights, as set forth in the OASIS IPR Policy, must be followed) or as required to translate it into languages other than English.

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

This document and the information contained herein is provided on an "AS IS" basis and OASIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY 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.