SAML V2.0 Asynchronous Single Logout Protocol Extension Version 1.0

Working Draft 02

4 September 2012

Technical Committee:
OASIS Security Services (SAML) TC

Chairs:
Thomas Hardjono, M.I.T.
Nate Klingenstein, Internet2

Editor:
Chad La Joie, Internet2
Scott Cantor, Internet2

Additional artifacts:
This prose specification is one component of a Work Product which also includes:
• XML schemas (saml-async-slo-v1.0.xsd)

Related work:
This specification replaces or supersedes:
• None
This specification is related to:
• Security Assertion Markup Language (SAML) v2.0. OASIS Standard.
http://docs.oasis-open.org/security/saml/v2.0/saml-2.0-os.zip

Declared XML namespace:
• urn:oasis:names:tc:SAML:2.0:protocol:ext:async-slo

Abstract:
This document defines an extension to the Single Logout Protocol that allows the initiator to indicate that it does not expect to receive a response from the session authority.

Status:
This Working Draft (WD) has been produced by one or more TC Members; it has not yet been voted on by the TC or approved as a Committee Draft (Committee Specification Draft or a Committee Note Draft). The OASIS document Approval Process begins officially with a TC vote to approve a WD as a Committee Draft. A TC may approve a Working Draft, revise it, and re-approve it any number of times as a Committee Draft.

Copyright © OASIS Open 2012. 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.
# Table of Contents

1 Introduction.............................................................................................................................................. 4  
  1.1 Terminology...................................................................................................................................... 4  
  1.2 Normative References...................................................................................................................... 4

2 Single Logout Protocol Extension for Asynchronous Requests ............................................................ 6  
  2.1 Element `<aslo:Asynchronous>` ........................................................................................................ 6  
  2.2 Asynchronous Logout Request Processing ........................................................................................ 6  
  2.3 Metadata Considerations.................................................................................................................... 6

3 Conformance ........................................................................................................................................... 7

Appendix A Acknowledgments .................................................................................................................. 8

Appendix B Revision History .................................................................................................................... 9
1 Introduction

This document defines an extension to the Single Logout Protocol that allows the initiator to indicate that it does not expect to receive a response from the session authority.

The SAML 2 Single Logout Protocol, defined in section 3.7 of [SAMLCore], provides for request delivery over front- and back-channel mechanisms. When logout is begun with an SP-initiated front-channel request, either the session authority or service provider may present a user interface to the user but neither entity knows, or can indicate, that it will perform this task. If both present such a UI, this would likely lead to user confusion. This extension allows the SP to signal to the session authority that the session authority is expected to present the UI.

In addition, an entity may wish to directly initiate a logout (e.g., an administrator destroying a user’s session). If such behavior is triggered by the delivery of a SAML 2 logout request (instead of via a proprietary mechanism), this extension informs the sessions authority that a response is not necessary.

1.1 Terminology

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “should not”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in [RFC 2119].

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>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 [SAMLCore]</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: <ns:Element>, Attribute, Datatype, OtherCode.

This specification uses the following typographical conventions in XML listings:

Listings of XML schemas appear like this.

Listings of XML examples appear like this. These listings are non-normative.

1.2 Normative References


[saml-async-slo-v1.0-wd02] Working Draft 02 Standards Track Draft Copyright © OASIS Open 2012. All Rights Reserved. 4 September 2012 Page 4 of 9

2 Single Logout Protocol Extension for Asynchronous Requests

2.1 Element <aslo:Asynchronous>

The <aslo:Asynchronous> element indicates that the containing <samlp:LogoutRequest> is an asynchronous request and should be processed as described in the following section.

The <aslo:Asynchronous> element MUST appear within the <samlp:Extensions> element of a <samlp:LogoutRequest> element. The use of the <aslo:Asynchronous> element outside of that context is not defined by this specification.

```
<element name="Asynchronous" type="aslo:AsynchronousType" />
<complexType name="AsynchronousType" />
```

2.2 Asynchronous Logout Request Processing

When a session authority receives a <samlp:LogoutRequest> containing the asynchronous request extension, the session authority SHALL process the request as described in section 3.7.3.2 of [SAMLCore] except that the session authority MUST NOT send a <samlp:LogoutResponse> to the request initiator.

Note, because no <samlp:LogoutResponse> is sent back to the request initiator, the session authority MUST provide all relevant feedback. For example, in the case of front-channel bindings, the session authority would display a web page indicating the success or failure of the logout process.

2.3 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 [SAMLMeta] 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 aslo:supportsAsynchronous attribute:

```
<attribute name="supportsAsynchronous" type="boolean"/>
```
3 Conformance

A logout request initiator conforms to this specification if it supports the inclusion of the `<aslo:Asynchronous>` element as defined in section 2.1 of this specification.

A session authority conforms to this specification if it can processes a logout request as defined primarily by [SAMLCore], as supplemented by section 2.2 of this specification.
Appendix A  Acknowledgments

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

- Scott Cantor, Internet2
- Chad LaJoie, Internet2,
- Nate Klingenstein, Internet2,
- Thomas Hardjono, M.I.T.
- Frederick Hirsch, Nokia Corporation
- Hal Lockhart, Oracle
- Anil Saldhana, Red Hat
- Duane DeCouteau, Veteran's Health Administration
## Appendix B  Revision History

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Editor</th>
<th>Changes Made</th>
</tr>
</thead>
<tbody>
<tr>
<td>WD01</td>
<td>July 6, 2012</td>
<td>Chad La Joie</td>
<td>Initial version</td>
</tr>
<tr>
<td>WD02</td>
<td>Sep 4, 2012</td>
<td>Scott Cantor</td>
<td>Added metadata portion, and a bit of cleanup.</td>
</tr>
</tbody>
</table>