SAML V2.0 Asynchronous Single Logout Profile Extension Version 1.0

Committee Specification 01

22 November 2012

Specification URIs

This version:

http://docs.oasis-open.org/security/saml/Post2.0/saml-async-slo/v1.0/cs01/saml-async-slo-v1.0-cs01.odt (Authoritative)
http://docs.oasis-open.org/security/saml/Post2.0/saml-async-slo/v1.0/cs01/saml-async-slo-v1.0-cs01.html
http://docs.oasis-open.org/security/saml/Post2.0/saml-async-slo/v1.0/cs01/saml-async-slo-v1.0-cs01.pdf

Previous version:

N/A

Latest version:

http://docs.oasis-open.org/security/saml/Post2.0/saml-async-slo/v1.0/saml-async-slo-v1.0.odt (Authoritative)
http://docs.oasis-open.org/security/saml/Post2.0/saml-async-slo/v1.0/saml-async-slo-v1.0.html
http://docs.oasis-open.org/security/saml/Post2.0/saml-async-slo/v1.0/saml-async-slo-v1.0.pdf

Technical Committee:

OASIS Security Services (SAML) TC

Chairs:

Thomas Hardjono (hardjono@mit.edu), M.I.T.
Nate Klingenstein (ndk@internet2.edu), Internet2

Editors:

Chad La Joie (lajoie@itumi.biz), Internet2
Scott Cantor (cantor.2@osu.edu), Internet2

Additional artifacts:

This prose specification is one component of a Work Product which also includes:

- XML schema: http://docs.oasis-open.org/security/saml/Post2.0/saml-async-slo/v1.0/cs01/xsd/

Related work:

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 SAML 2.0 Single Logout Protocol that allows the initiator to indicate that it does not expect to receive a response from the session authority. This improves user interface interoperability in deployments that want the identity provider to control the user experience during logout.

Status:

This document was last revised or approved by the OASIS Security Services (SAML) TC on the above date. The level of approval is also listed above.

Technical Committee members should send comments on this Work Product 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 Work Product, 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).

Citation format:

When referencing this Work Product the following citation format should be used:

[SAML-Async-SLO]

SAML V2.0 Asynchronous Single Logout Profile Extension Version 1.0. 22 November 2012. OASIS Committee Specification 01. http://docs.oasis-open.org/security/saml/Post2.0/saml-async-slo/v1.0/cs01/saml-async-slo-v1.0-cs01.html.

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 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/policies-guidelines/trademark for above guidance.

Table of Contents

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:

Prefix	XML Namespace	Comments
`samlp:`	urn:oasis:names:tc:SAML:2.0:protocol	This is the SAML V2.0 protocol namespace defined in the SAML V2.0 core specification [SAMLCore]
`aslo:`	urn:oasis:names:tc:SAML:2.0:protocol:ext:async-slo	The namespace defined by this document.
`xsd:`	http://www.w3.org/2001/XMLSchema	This namespace is defined in the W3C XML Schema specification [Schema1]. In schema listings, this is the default namespace and no prefix is shown.
`xsi:`	http://www.w3.org/2001/XMLSchema-instance	This is the XML Schema namespace for schema-related markup that appears in XML instances [Schema1].

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

[RFC 2119] S. Bradner. *Key words for use in RFCs to Indicate Requirement Levels*. IETF RFC 2119, March 1997. http://www.ietf.org/rfc/rfc2119.txt

[SAMLCore] OASIS Approved Standard, *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0*, March 2005. http://docs.oasis-open.org/security/saml/v2.0/saml-2.0-os.zip

[SAML2Errata] OASIS Approved Errata, *SAML V2.0 Errata*, May 2012. http://docs.oasis-open.org/security/saml/v2.0/errata05/os/saml-v2.0-errata05-os.pdf

[SAMLMeta] OASIS Approved Standard, *Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0*, March 2005. http://docs.oasis-open.org/security/saml/v2.0/saml-2.0-os.zip

[Schema1] H. S. Thompson et al. XML Schema Part 1: Structures. World Wide Web Consortium Recommendation, May 2001. See http://www.w3.org/TR/2001/REC- xmlschema-1-20010502/

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

Revision	Date	Editor	Changes Made
WD01	July 6, 2012	Chad La Joie	Initial version
WD02	Sep 4, 2012	Scott Cantor	Added metadata portion, and a bit of cleanup.