SAML V2.0 Protocol Extension for Third-Party Requests

Committee Draft 02, 1 September 2006

Document identifier:

sstc-saml-protocol-ext-thirdparty-cd-02

Location:

http://www.oasis-open.org/committees/documents.php?wg_abbrev=security

Editors:

Scott Cantor, Internet2

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 is a **Committee Draft** approved by the Security Services Technical Committee on 28 August 2006.

Committee members should submit comments and potential errata to the security-services@lists.oasis-open.org list. Others should submit them by filling out the web form located at http://www.oasis-open.org/committees/comments/form.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 web page for the Security Services TC (http://www.oasis-open.org/committees/security/ipr.php).

Table of Contents

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 interoperation 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:

Prefix	XML Namespace	Comments
`saml:`	urn:oasis:names:tc:SAML:2.0:assertion	This is the SAML V2.0 assertion namespace defined in the SAML V2.0 core specification [SAML2Core].
`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 [SAML2Core].
`md:`	urn:oasis:names:tc:SAML:2.0:metadata	This is the SAML V2.0 metadata namespace defined in the SAML V2.0 metadata specification [SAML2Meta].
`thrpty:`	urn:oasis:names:tc:SAML:protocol:ext:third-party	This is the namespace defined by this document and its accompanying schema [ThrPtyExt-xsd].
`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: `<SAMLElement>`, `<ns:ForeignElement>`, `Attribute`, **Datatype**, `OtherCode`.

2 Third-Party Request SAML Protocol Extension

2.1 Required Information

Identification: urn:oasis:names:tc:SAML:protocol:ext:third-party

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 **samlp: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 requester 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:

```
<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.

```
<md:SingleSignOnService
  xmlns:thrpty="urn:oasis:names:tc:SAML:protocol:ext:third-party"
  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 RFC 2119, March 1997. http://www.ietf.org/rfc/rfc2119.txt.

[SAML2Core] S. Cantor et al. Assertions *and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS Standard, March 2005. Document ID saml-core-2.0-os. See http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf.

[SAML2Bind] S. Cantor et al. *Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS Standard, March 2005. Document ID saml-bindings-2.0-os. See http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf.

[SAML2Meta] S. Cantor et al. *Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS Standard, March 2005. Document ID saml-metadata-2.0-os. See http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf.

[SAML2Prof] S. Cantor et al. *Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS Standard, March 2005. Document ID saml-profiles-2.0-os. See http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf.

[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/.

[ThrPtyExt-xsd] S. Cantor. SAML 2.0 Protocol Extension Schema for Third-Party Requests. OASIS SSTC, July 2006. Document ID sstc-saml-protocol-ext-thirdparty.xsd. See 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
- Thomas Wisniewski, Entrust
- Ashish Patel, France Telecom
- Greg Whitehead, Hewlett-Packard
- Heather Hinton, IBM
- Anthony Nadalin, IBM
- Eric Tiffany, IEEE Industry Standards and Technology Org (IEEE-ISTO)
- Scott Cantor, Internet2
- Bob Morgan, Internet2
- Tom Scavo, National Center for Supercomputing Applications (NCSA)
- Peter Davis, Neustar, Inc.
- Jeff Hodges, Neustar, Inc.
- Frederick Hirsch, Nokia Corporation
- Abbie Barbir, Nortel Networks Limited
- Paul Madsen, NTT Corporation
- Ari Kermaier, Oracle Corporation
- Prateek Mishra, Oracle Corporation
- John Hughes, PA Consulting
- Brian Campbell, Ping Identity Corporation
- Rob Philpott, RSA Security
- Jahan Moreh, Sigaba Corp.
- Bhavna Bhatnagar, Sun Microsystems
- Eve Maler, Sun Microsystems
- Emily Xu, Sun Microsystems
- David Staggs, Veterans Health Administration

Appendix B. Notices

OASIS takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on OASIS's procedures with respect to rights in OASIS specifications can be found at the OASIS website. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification, can be obtained from the OASIS Executive Director.

OASIS invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to implement this specification. Please address the information to the OASIS Executive Director.

Copyright © OASIS Open 2006. *All Rights Reserved.*

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to OASIS, except as needed for the purpose of developing OASIS specifications, in which case the procedures for copyrights defined in the OASIS Intellectual Property Rights document must be followed, or as required to translate it into languages other than English.

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

This document and the information contained herein is provided on an “AS IS” basis and OASIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.