SAML Protocol Extension for Third-Party Requests

Committee Draft 01, 14 March 2006

Document identifier:

sstc-saml-protocol-ext-thirdparty-cd-01

Location:

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

Editors:

Scott Cantor (cantor.2@osu.edu), 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 14 March 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 3
1.1 Notation 3
2 Third-Party Request SAML Protocol Extension 4
2.1 Element <thrpty:RespondTo> 4
2.2 Processing Rules 4
2.3 Unsolicited Responses 5
2.4 Metadata Considerations 5
2.4.1 Metadata Example 5
3 References 6
3.1 Normative References 6

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 [SAML2Core].
samlp:	urn:oasis:names:tc:SAML:2.0:protocol	This is the SAML V2.0 protocol namespace [SAML2Core].
md:	urn:oasis:names:tc:SAML:2.0:metadata	This is the SAML V2.0 metadata namespace [SAML2Meta].
thrpty:	urn:oasis:names:tc:SAML:protocol:ext:third-party	This is the SAML V2.0 protocol extension 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

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.

2.1 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]).

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

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

2.2 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 extension to [SAML2Meta] in Section 2.4 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. A requester MUST NOT include more than one `<samlpext: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.

2.3 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.

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.

2.4 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 by adding a boolean-typed XML attribute to an element of or 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"/>
```

2.4.1 Metadata Example

The example below shows a fragmentary `<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 SSTC, March 2005. Document ID saml-core-2.0-os. http://www.oasis-open.org/committees/security/.

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

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

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

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

[ThrPtyExt-xsd] S. Cantor. SAML third-party protocol extension schema. OASIS SSTC, March 2006. Document ID sstc-saml-protocol-ext-thirdparty.xsd. See http://www.oasis-open.org/committees/security/.