SOAP Profile for XACML-SAML

Working Draft 01
30 November 2007

Specification URLs:
urn:mace:switch.ch:doc:xacml-saml:profile:200711

This Version:
URL
Previous Version:
URL
Latest Version:
URL

Editors:
Chad La Joie, SWITCH

Related Work:
This work is related to the SAML 2.0 Profile of XACML, Version 2.0 [XACML-SAML].

Abstract:
This specification defines the use of the SAML SOAP binding [SAMLBind] to carry XACML-SAML request-response messages.

Status:
This document is a working draft produced by SWITCH as a product of its work within the EGEE JRA 1 working group. It is based on the OASIS working draft of the SAML 2.0 Profile of XACML, Version 2.0. This document corrects and clarifies a significant number of items incorrectly specified in previous versions.
# Table of Contents

1 Introduction

1.1 Notation

1.2 Normative References

2 XACML-SAML Query Profile

2.1 Required Information

2.2 Profile Overview

2.3 Profile Description

2.3.1 Query issued by requester

2.3.2 <samlp:Response> issued by responder

2.4 Use of XACML-SAML Query Protocol

2.4.1 <XACMLAuthzDecisionQuery> Usage

2.4.2 <XACMLPolicyQuery> Usage

2.4.3 <samlp:Response> Usage

2.4.4 <saml:Assertion> Usage

2.5 XACML Version Support

2.6 Use of Metadata

3 Security

3.1 Entity Authentication

3.2 Message Integrity

3.3 Message Confidentiality
1 Introduction

The SAML 2.0 Profile of XACML [XACML-SAML] defines extension to SAML V2.0 assertion and request-response protocol messages. This specification defines the use of these messages over the SAML 2 SOAP binding [SAMLBind].

1.1 Notation

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:

<table>
<thead>
<tr>
<th>Prefix</th>
<th>XML Namespace</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>ds:</td>
<td><a href="http://www.w3.org/2000/09/xmldsig#">http://www.w3.org/2000/09/xmldsig#</a></td>
<td>This is the XML Signature namespace [XMLSig].</td>
</tr>
<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] specification.</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] specification.</td>
</tr>
<tr>
<td>xenc:</td>
<td><a href="http://www.w3.org/2001/04/xmlenc#">http://www.w3.org/2001/04/xmlenc#</a></td>
<td>This is the XML encryption namespace defined in the [XMLEnc] specification.</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 is the XML Schema namespace defined in the [Schema1] specification.</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 defined in the [Schema1] specification.</td>
</tr>
</tbody>
</table>

This specification uses the following typographical conventions in text: <XACMLSAMLElement>, <ns:ForeignElement>, Attribute, Datatype, OtherKeyword.

1.2 Normative References


2 XACML-SAML Query Profile

[XACML-SAML] defines a protocol for requesting authorization policies and decisions on the basis of XACML request contexts. This profile describes the use of this protocol with the SAML SOAP binding [SAMLBind].

2.1 Required Information


Contact Information: grid@switch.ch

Updates: None.

2.2 Profile Overview

The messages that govern this profile are defined by Sections 4 and 5 of [XACML-SAML]. Section 3.2 of [SAMLBind] defines the binding of the message exchange to SOAP V1.1. Unless specifically noted here, all requirements defined in those specifications apply.

Figure 1 illustrates the basic template for this profile.

![Figure 1](image)

The following steps describe this profile.

1. XACML-SAML query message issued by requester

   In step 1, XACML-SAML requester initiates the profile by sending a <XACMLAuthzDecisionQuery> or <XACMLPolicyQuery> message to the XACML-SAML responder, a XACML PDP or PAP respectively.

2. <samlp:Response> issued by responder

   In step 2, the XACML-SAML responder (after processing the request) issues a <samlp:Response> message to the requester.

2.3 Profile Description

2.3.1 Query issued by requester

To initiate the profile, a XACML-SAML requester issues either a <XACMLAuthzDecisionQuery> message, if the responder is a XACML PDP, or a <XACMLPolicyQuery> message, if the responder is a XACML PAP. The requester MUST use the SAML SOAP binding [SAMLBind] to send the message directly to the responder. The requester SHOULD authenticate itself to the responder.

Profile-specific rules for the contents of the various messages are included in Section 2.4.1.
2.3.2 <samlp:Response> issued by responder

The XACML-SAML responder MUST process the query as defined in [XACML]. After processing the message or encountering an error, the XACML-SAML responder MUST return a <samlp:Response> message containing an appropriate status code to the XACML-SAML requester to complete the protocol exchange. If the request is successful the response will also include the appropriate authorization decision statements.

The XACML-SAML responder SHOULD authenticate itself to the requester.

Profile specific rules for the contents of the <samlp:Response> message are included in Section 2.4.3.

2.4 Use of XACML-SAML Query Protocol

2.4.1 <XACMLAuthzDecisionQuery> Usage

The <saml:Issuer> element SHOULD be present. If present the issuer MUST contain the unique identifier of the requester and the Format attribute MUST be omitted or have a value of urn:oasis:names:tc:SAML:2.0:nameid-format:entity. The presence of this element provides an additional mechanism by which a responder may verify the identity of the requester.

2.4.2 <XACMLPolicyQuery> Usage

The <saml:Issuer> element SHOULD be present. If present the issuer MUST contain the unique identifier of the requester and the Format attribute MUST be omitted or have a value of urn:oasis:names:tc:SAML:2.0:nameid-format:entity. The presence of this element provides an additional mechanism by which a responder may verify the identity of the requester.

2.4.3 <samlp:Response> Usage

The <saml:Issuer> element SHOULD be present. If present the issuer MUST contain the unique identifier of the requester and the Format attribute MUST be omitted or have a value of urn:oasis:names:tc:SAML:2.0:nameid-format:entity. The presence of this element provides an additional mechanism by which a responder may verify the identity of the requester.

If the requester does not authenticate itself and no issuer is provided in the request the responder SHOULD return a response with a primary status code of urn:oasis:names:tc:SAML:2.0:status:Requester.

2.4.4 <saml:Assertion> Usage

The <saml:Issuer> present in the <saml:Assertion> returned within the response of an authorization or policy query MUST correspond to signer of the assertion, if the assertion is signed.

2.5 XACML Version Support

[XACML-SAML] supports the usage of XACML 1, 2, and 3. XACML-SAML responder’s SHOULD support XACML 2.0 and MAY support other versions.

2.6 Use of Metadata

[XACML-SAML] Section 8 defines additional SAML metadata role types used to describe the PDP and authorization decisions query endpoints, respectively. Section 1.5 [XACML-SAML] provides the
xacml-saml protocol URIs, used within protocolSupportEnumeration, to indicate which version of XACML is supported by the responder.
3 Security

3.1 Entity Authentication

Entities may authenticate to a peer through the use of a transport specific manner, such as SSL/TLS. Alternatively the <ds:Signature>, specified in [SAML] section 5, contained within the <samlp:Response> MAY be used as a means of authentication. If a <saml:Issuer> is present in a message the responder SHOULD verify that the credentials used by the requester during authentication belong to the identified issuer. A responder MAY use information within the SAML metadata to achieve this or any some other unspecified mechanism.

3.2 Message Integrity

XACML-SAML entities MUST ensure the integrity of the message. If the underlying transport mechanism provides integrity this is sufficient. A digital signature, specified in [SAML] section 5, on the <samlp:Response> MAY also be used. It is RECOMMENDED that the <saml:Assertion> contained within a response also be signed. This ensures that if the assertion is removed from the response, and used or processed elsewhere, its integrity may still be verified.

3.3 Message Confidentiality

XACML-SAML entities MUST ensure the confidentiality of the message as both requests and responses may contain sensitive information about individuals or organizations. If the underlying transport mechanism provides confidentiality this is sufficient. The XACML-SAML requester MUST NOT transport the <saml:Assertion> to a third party if that assertions contains an authorization decisions statement with a XACML request context.

The assertion MAY be encrypted in the case where an appropriate public key for the peer is known or obvious from the environment, such when mutual SSL/TLS authentication is used. If an assertion is encrypted it MUST follow the requirements defined in the [SAML] and any relevant errata.