

---

## 2 **SOAP Profile for XACML-SAML**

### 3 **Working Draft 01** 4 **30 November 2007**

5 **Specification URIs:**

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

7 **This Version:**

8 URL

9 **Previous Version:**

10 URL

11 **Latest Version:**

12 URL

13 **Editors:**

14 Chad La Joie, SWITCH

15 **Related Work:**

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

17 **Abstract:**

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

20 **Status:**

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

## 25 Table of Contents

26	1 Introduction.....	3
27	1.1 Notation.....	3
28	1.2 Normative References.....	3
29	2 XACML-SAML Query Profile.....	5
30	2.1 Required Information.....	5
31	2.2 Profile Overview.....	5
32	2.3 Profile Description.....	5
33	2.3.1 Query issued by requester.....	5
34	2.3.2 <samlp:Response> issued by responder.....	6
35	2.4 Use of XACML-SAML Query Protocol.....	6
36	2.4.1 <XACMLAuthzDecisionQuery> Usage.....	6
37	2.4.2 <XACMLPolicyQuery> Usage.....	6
38	2.4.3 <samlp:Response> Usage.....	6
39	2.4.4 <saml:Assertion> Usage.....	6
40	2.5 XACML Version Support.....	6
41	2.6 Use of Metadata.....	6
42	3 Security.....	8
43	3.1 Entity Authentication.....	8
44	3.2 Message Integrity.....	8
45	3.3 Message Confidentiality.....	8
46		

# 47 1 Introduction

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

## 51 1.1 Notation

52 The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD",  
53 "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this specification are to be  
54 interpreted as described in [RFC 2119]:

55 ...they MUST only be used where it is actually required for interoperation or to  
56 limit behavior which has potential for causing harm (e.g., limiting  
57 retransmissions)...

58 These keywords are thus capitalized when used to unambiguously specify requirements over protocol  
59 and application features and behavior that affect the interoperability and security of implementations.  
60 When these words are not capitalized, they are meant in their natural-language sense.

61 Listings of XML schemas appear like this.

62 Example code listings appear like this.

63 Conventional XML namespace prefixes are used throughout the listings in this specification to stand  
64 for their respective namespaces as follows, whether or not a namespace declaration is present in the  
65 example:

Prefix	XML Namespace	Comments
ds :	http://www.w3.org/2000/09/xmldsig#	This is the XML Signature namespace [XMLSig].
saml :	urn:oasis:names:tc:SAML:2.0:assertion	This is the SAML V2.0 assertion namespace defined in the [SAML] specification.
samlp :	urn:oasis:names:tc:SAML:2.0:protocol	This is the SAML V2.0 protocol namespace defined in the [SAML] specification.
xacml-saml :	urn:oasis:names:tc:xacml:2.0:saml:assertion:schema:os	This is the XACML-SAML assertion namespace defined in the [XACML-SAML] specification.
xacml-samlp :	urn:oasis:names:tc:xacml:2.0:saml:protocol:schema:os	This is the XACML-SAML protocol namespace defined in the [XACML-SAML] specification.
xenc :	http://www.w3.org/2001/04/xmlenc#	This is the XML encryption namespace defined in the [XMLEnc] specification.
xsd :	http://www.w3.org/2001/XMLSchema	This is the XML Schema namespace defined in the [Schema1] specification.
xsi :	http://www.w3.org/2001/XMLSchema-instance	This is the XML Schema instance namespace defined in the [Schema1] specification.

67

68 This specification uses the following typographical conventions in text: <XACMLSAMElement>,  
69 <ns:ForeignElement>, Attribute, **Datatype**, OtherKeyword.

## 70 1.2 Normative References

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

73	[SAML]	S. Cantor, <i>Assertions and Protocols for the OASIS Security Assertion Markup Language V2.0</i> . OASIS, 15 March 2005. See <a href="http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf">http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf</a> .
76	[SAMLBind]	S. Cantor et al. <i>Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0</i> . OASIS, 15 March 2005. See <a href="http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf">http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf</a> .
79	[Schema1]	H. S. Thompson et al. <i>XML Schema Part 1: Structures</i> . World Wide Web Consortium Recommendation, May 2001. See <a href="http://www.w3.org/TR/2001/REC-xmlschema-1-20010502/">http://www.w3.org/TR/2001/REC-xmlschema-1-20010502/</a> .
82	[XACML]	T. Moses. <i>eXtensible Access Control Markup Language (XACML) Version 2.0</i> . OASIS, 1 February 2005. See <a href="http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-rbac-profile1-spec-os.pdf">http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-rbac-profile1-spec-os.pdf</a> .
85	[XACML-SAML]	A. Anderson et al. <i>SAML 2.0 profile of XACML, Version 2.0</i> . OASIS, 19 July 2007. See <a href="http://www.oasis-open.org/committees/download.php/24681/xacml-profile-saml2.0-v2-spec-wd-5-en.pdf">http://www.oasis-open.org/committees/download.php/24681/xacml-profile-saml2.0-v2-spec-wd-5-en.pdf</a> .
89	[XMLEnc]	D. Eastlake et al. <i>XML Encryption Syntax and Processing</i> . Word Wide Web Consortium, 10 December 2002. See <a href="http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/">http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/</a> .
92	[XMLSig]	D. Eastlake et al. <i>XML-Signature Syntax and Processing</i> . Word Wide Web Consortium, February 2002. See <a href="http://www.w3.org/TR/xmlsig-core/">http://www.w3.org/TR/xmlsig-core/</a> .

## 94 2 XACML-SAML Query Profile

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

### 98 2.1 Required Information

99 **Identification:** urn:mace:switch.ch:doc:xacml-saml:profile:200711:SOAP

100 **Contact Information:** grid@switch.ch

101 **Updates:** None.

### 102 2.2 Profile Overview

103 The messages that govern this profile are defined by Sections 4 and 5 of [XACML-SAML]. Section  
104 3.2 of [SAMLBind] defines the binding of the message exchange to SOAP V1.1. Unless specifically  
105 noted here, all requirements defined in those specifications apply.

106 Figure 1 illustrates the basic template for this profile.

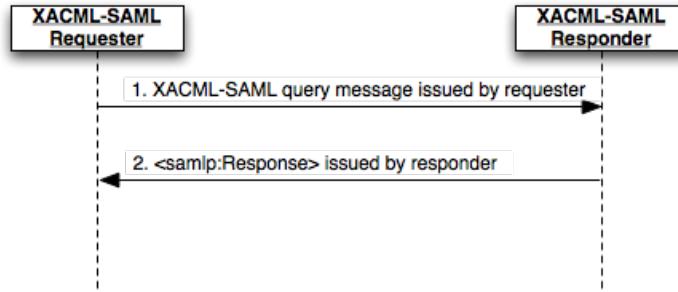


Figure 1

107 The following steps describe this profile.

#### 108 1. XACML-SAML query message issued by requester

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

#### 112 2. <samlp:Response> issued by responder

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

### 115 2.3 Profile Description

#### 116 2.3.1 Query issued by requester

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

121 Profile-specific rules for the contents of the various messages are included in Section 2.4.1.

122 **2.3.2 <samlp:Response> issued by responder**

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

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

129 Profile specific rules for the contents of the <samlp:Response> message are included in Section  
130 2.4.3.

131 **2.4 Use of XACML-SAML Query Protocol**

132 **2.4.1 <ACMIAuthzDecisionQuery> Usage**

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

137 **2.4.2 <ACMLPolicyQuery> Usage**

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

142 **2.4.3 <samlp:Response> Usage**

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

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

150 **2.4.4 <saml:Assertion> Usage**

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

153 **2.5 XACML Version Support**

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

156 **2.6 Use of Metadata**

157 [XACML-SAML] Section 8 defines additional SAML metadata role types used to describe the PDP  
158 and authorization decisions query endpoints, respectively. Section 1.5 [XACML-SAML] provides the

159 xacml-saml protocol URIs, used within `protocolSupportEnumeration`, to indicate which version  
160 of XACML is supported by the responder.

161 **3 Security**

162 **3.1 Entity Authentication**

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

169 **3.2 Message Integrity**

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

175 **3.3 Message Confidentiality**

176 XACML-SAML entities MUST ensure the confidentiality of the message as both requests and  
177 responses may contain sensitive information about individuals or organizations. If the underlying  
178 transport mechanism provides confidentiality this is sufficient. The XACML-SAML requester MUST  
179 NOT transport the <saml:Assertion> to a third party if that assertions contains an authorization  
180 decisions statement with a XACML request context.  
  
181 The assertion MAY be encrypted in the case where an appropriate public key for the peer is known or  
182 obvious from the environment, such when mutual SSL/TLS authentication is used. If an assertion is  
183 encrypted it MUST follow the requirements defined in the [SAML] and any relevant errata.