



XACML Profile of SAML V2.0 Attributes

Working Draft 03, 25 May 2004

Document identifier:

sstc-xacml-saml-attr-profile-2.0-draft-03

Location:

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

Editors:

Hal Lockhart, BEA (hlockhar@bea.com)

Anne Anderson, Sun Microsystems (anne.anderson@sun.com)

Contributors:

Frank Siebenlist, Argonne National Laboratory

Daniel Engovatov, BEA

Tim Moses, Entrust

Michiharu Kudo, IBM

Michael McIntosh, IBM

Anthony Nadalin, IBM

Steve Anderson, Open Network

Simon Godik, OverXeer

Bill Parducci, OverXeer

Seth Proctor, Sun Microsystems

Polar Humenn, Syracuse University

Abstract:

This document provides a profile for creating SAML Attribute Assertions that can be mapped automatically to XACML Attributes.

Status:

Committee members should send comments on this specification to the security-services@lists.oasis-open.org list. Others should use the comment form 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 section of the XXXX TC web page (<http://www.oasis-open.org/committees/security/ipr.php>).

34 **Table of Contents**

35 1 Introduction.....3

36 1.1 Terminology.....3

37 2 Data Type.....4

38 3 Attribute Identifiers.....5

39 4 References.....6

40

1 Introduction

{Non-normative}

SAML Attribute Assertions may be used as input to authorization decisions made according to the OASIS eXtensible Access Control Markup Language (XACML) standard specification [XACML]. Since the SAML **Attribute** format differs from the XACML **Attribute** format, there is a mapping that must be performed. The OASIS XACML TC has defined a Profile for doing this mapping [XACML-Profile], but that Profile imposes constraints on the meta-data provided with the SAML **Attribute**. This Profile describes those meta-data constraints. SAML Attribute Assertions generated in conformance with this Profile can be mapped automatically to XACML **Attributes** and used as input to XACML authorization decisions.

1.1 Terminology

{Non-normative}

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 IETF RFC 2119 [RFC2119].

The following additional terms are used with particular semantics in this Profile. When used in this way, the terms are specified in **bold, italicized font**.

Attribute – when capitalized, the term **Attribute** refers to an instance of the SAML schema **Attribute** element or to an instance of the XACML schema **Attribute** element.

attribute – when not capitalized, the term **attribute** refers to an XML element **attribute**.

Context Handler – an entity in the XACML operational model that uses an authorization decision request and possibly other information to create the context for an XACML **PDP** policy evaluation. The **Context Handler** is responsible for converting **Attributes** to the XACML **Attribute** format if necessary.

Policy Decision Point or **PDP** – an entity in the XACML operational model that evaluates an authorization decision request against an authorization policy and returns an authorization decision.

Policy Enforcement Point or **PEP** – an entity in the XACML operational model that protects access to a resource. When access to a resource is attempted, the **PEP** sends an authorization decision request to a **Policy Decision Point** and carries out the authorization decision returned by the **PDP**.

XACML processor – in this Profile, the term **XACML processor** is used for any entity that is constrained to use XACML **Attributes**. Typically, such an entity will be an XACML **Context Handler** or a **Policy Enforcement Point** that will be sending authorization decision requests to an XACML **Policy Decision Point**.

73 2 Data Type

74 {Normative}

75 XACML requires each **Attribute** to have an explicit data type. To supply this data type value, a SAML
76 **Attribute** to be used as input to an **XACML processor** SHALL have the following metadata provided.

```
77 <xs:attribute name="DataType" type="xs:anyURI" use="optional"  
78             default="http://www.w3.org/2001/XMLSchema#string"/>
```

79 The standard values for the `DataType` **attribute** are specified in Appendix A of the XACML 2.0
80 Specification [XACML].

81 If non-standard values are used for the `DataType` **attribute**, each XACML PDP that will be consuming
82 **Attributes** with these new `DataType` values must be extended to support the new data types.

83 3 Attribute Identifiers

84 {Normative}

85 XACML requires each **Attribute** to have a single identifier that is sufficient to distinguish instances of the
86 **Attribute** from instances of other **Attributes** that have different semantics. In SAML 2.0, two standard
87 identifiers – `Name` and `NameFormat` - are required to distinguish two **Attributes** that may have different
88 semantics. SAML 2.0 also allows the use of arbitrary additional identifiers. In order to map a SAML
89 **Attribute** to an XACML **Attribute**, there must be a canonical way to generate a single XACML **Attribute**
90 identifier from the set of SAML **attributes** that are sufficient to distinguish instances of the SAML
91 **Attribute** that have different semantics.

92 In order to satisfy this requirement, a SAML **Attribute** that is to be used as input to an **XACML**
93 **processor** SHALL have a `NameFormat` value of “urn:oasis:names:tc:SAML:2.0:attrname-
94 format:uri”. The value of the SAML **Attribute's** `Name` **attribute** SHALL be a URI or URI reference
95 that is sufficient to distinguish instances of this **Attribute** from instances of other SAML or XACML
96 **Attributes** that have different semantics. Additional **attributes** not necessary for distinguishing the
97 SAML **Attribute** semantics MAY be used in the SAML metadata, but will not be used in the
98 corresponding XACML **Attribute**.

99

4 References

100 {Normative}

101

102 **[XACML]** T. Moses, ed., *OASIS eXtensible Access Control Markup Language (XACML)*
103 *Versions 1.0, 1.1, and 2.0*. Available on the OASIS XACML TC web page at
104 http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml.

105 **[XACML-Profile]** A. Anderson and H. Lockhart, eds., *XACML Profile for SAML 2.0*. Available on
106 the OASIS XACML TC web page at [http://www.oasis-](http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml)
107 [open.org/committees/tc_home.php?wg_abbrev=xacml](http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml).

108 **[RFC2119]** S. Bradner, *Key words for use in RFCs to Indicate Requirement Levels*, IETF
109 RFC 2119, March 1997, <http://www.ietf.org/rfc/rfc2119.txt>.

110

A. Revision History

Rev	Date	By Whom	What
01	13 May 2004	Anne Anderson	Initial draft.
02	14 May 2004	Anne Anderson	Require NameFormat to be ...:uri and Name to be a semantically distinguishing URI.
03	25 May 2004	Anne Anderson	Clarify value and format of Attribute Name

111

112

B. Notices

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

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

124 **Copyright © OASIS Open 2004. All Rights Reserved.**

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

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

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