XACML Profile of SAML V2.0 Attributes

Working Draft 01, 13 May 2004

Document identifier:

sstc-xacml-saml-attr-profile-2.0-draft-01

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
Ganiel 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).

Table of Contents

1 Introduction

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

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.***

2 Data Type

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

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

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

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

3 Attribute Identifiers

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

In order to satisfy this requirement, a SAML ***Attribute*** that is to be used as input to an ***XACML processor*** SHALL contain no ***attributes*** other than `Name` and `NameFormat` that are needed to distinguish distinguish the SAML ***Attribute*** from other ***Attributes*** with different semantics. The XACML identifier for a SAML ***Attribute*** SHALL be the concatenation of `NameFormat` and `Name` using a ":" character as a separator. This concatenation SHALL be a valid URI and SHALL be sufficient to distinguish instances of the given SAML ***Attribute*** from instances of other SAML or XACML ***Attributes*** that have different semantics. Additional ***attributes*** not necessary for distinguishing the SAML ***Attribute*** semantics MAY be used in the SAML metadata, but will not be used in the corresponding XACML ***Attribute***.

4 References

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

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

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

A. Revision History

Rev	Date	By Whom	What
01	13 May 2004	Anne Anderson	Initial draft.

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.

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 does 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.