XACML Profile for SAML 2.0

Working Draft 02, 10 March 2004

Document identifier:

wd-xacml-saml-profile-02

Location:

http://www.oasis-open.org/committees/xacml/

Editor:

Anne Anderson, Sun Microsystems (anne.anderson@sun.com)
Hal Lockhart, BEA (hlockhar@bea.com)

Abstract:

This specification defines a profile for the use of the OASIS Security Assertion Markup Language (SAML) Version 2.0 to carry XACML 2.0 policies, policy queries and responses, authorization decisions, and authorization decision queries and responses. It also describes the use of SAML Attribute Assertions with XACML. Using XACML with SAML 2.0, XACML instances can be protected using the SAML guidelines for use of digital signatures and can be transported using SAML bindings to transport mechanisms.

Status:

This version of the specification is a working draft within the OASIS XACML TC. As such, it is expected to change prior to adoption as an OASIS standard.

Committee members should send comments on this specification to the xacml@lists.oasis-open.org list. Others should subscribe to and send comments to the xacml-comment@lists.oasis-open.org list. To subscribe, send an email message to xacml-comment-request@lists.oasis-open.org with the word "subscribe" as the body of the message.

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 XACML TC web page (http://www.oasis-open.org/committees/xacml/).

For any errata page for this specification, please refer to the XACML SAML Profile section of the XACML TC web page (http://www.oasis-open.org/committees/xacml/).

Copyright © OASIS Open 2004. All Rights Reserved.

Table of Contents

Copyright © OASIS Open 2004. All Rights Reserved.

1 Introduction (non-normative)

The OASIS eXtensible Access Control Markup Language [] is a powerful, standard language that specifies schemas for authorization policies and for authorization decision requests and responses. It also specifies how to evaluate policies against requests to compute a response. A brief overview of XACML is available in [].

The non-normative XACML usage model assumes that a *Policy Enforcement Point* (PEP) is responsible for protecting access to one or more resources. When a resource access is attempted, the PEP sends a description of the attempted access to a *Policy Decision Point* (PDP) in the form of an authorization decision request. The PDP evaluates this request against its available policies and attributes and produces an authorization decision that is returned to the PEP. The PEP is responsible for enforcing the decision.

In producing its description of the access request, the PEP may obtain attributes from on-line *Attribute Authorities* (AA) or from *Attribute Repositories* into which AA's have stored attributes. The PDP may augment the PEP's description of the access request with additional attributes obtained from AAs or Attribute Repositories.

The PDP may obtain policies from on-line *Policy Authorities* (PA) or from *Policy Repositories* into which PAs have stored policies.

XACML itself defines the content of some of the messages necessary to implement this model, but deliberately confines its scope to the language elements used directly by the PDP and does not define protocols or transport mechanisms. Full implementation of the usage model depends on use of other standards to specify assertions, protocols, and transport mechanisms. XACML also does not specify how to implement a Policy Enforcement Point, Policy Authority, Attribute Authority, or repository, but XACML can serve as a standard format for exchanging information with these entities when combined with other standards.

One standard suitable for providing the assertion and protocol mechanisms needed by XACML is the OASIS Security Markup Assertion Language [], Version 2.0. SAML defines schemas intended for use in requesting and responding with various types of security assertions. The SAML schemas include information needed to identify and validate the contents of the assertions, such as the identity of the assertion issuer, the validity period of the assertion, and the digital signature of the assertion. The SAML specification document specifies how these elements are to be used. In addition, SAML has associated specifications that define bindings to other standards. These other standards provide transport mechanisms and specify how digital signatures should be created and verified.

This profile defines how to use SAML 2.0 to protect, transport, and request XACML 2.0 schema instances and other information needed by an XACML implementation.

There are 6 types of statements used in this profile:

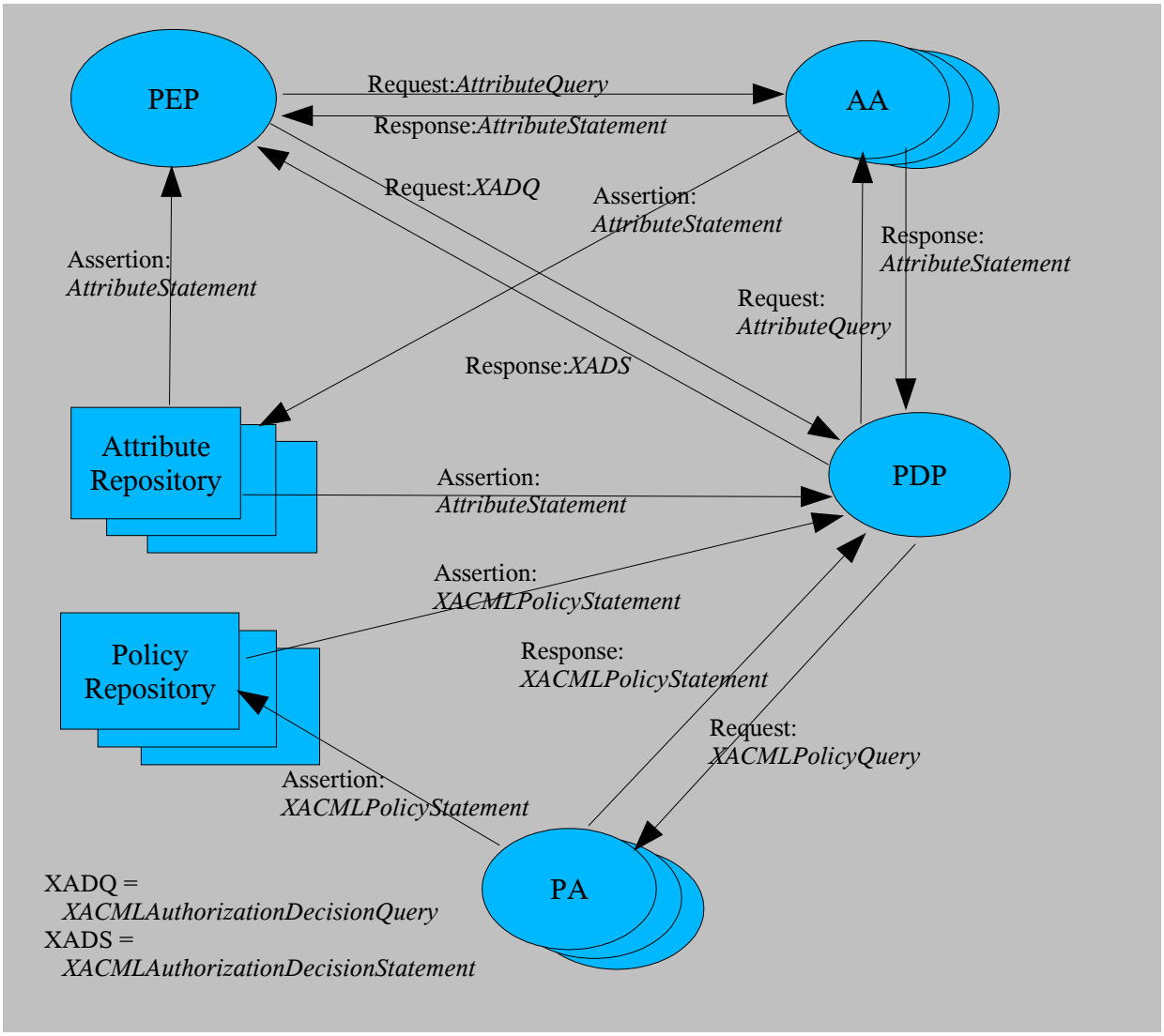
1. AttributeQuery – A standard SAML Query used for requesting one or more attributes from an Attribute Authority.
2. AttributeStatement – A standard SAML Statement that contains one or more attributes. This statement may be used in a SAML Response from an Attribute Authority, or it may be used in a SAML Assertion as a format for storing attributes in an Attribute Repository.
3. XACMLPolicyQuery – A SAML Query extension, defined in this profile. It is used for requesting one or more policies from a Policy Authority.
4. XACMLPolicyStatement – A SAML Statement extension, defined in this profile. It may be used in a SAML Response from a Policy Authority, or it may be used in a SAML Assertion as a format for storing policies in a Policy Repository.
5. XACMLAuthorizationDecisionQuery – A SAML Query extension, defined in this profile. It is used by

Copyright © OASIS Open 2004. All Rights Reserved.

a PEP to request an authorization decision from an XACML PDP.

6. XACMLAuthorizationDecisionStatement – A SAML Statement extension, defined in this profile. It may be used in a SAML Response from an XACML PDP. It might also be used in a SAML Assertion that is used as a credential, but this is not part of the currently defined XACML use model.

The following diagram illustrates the XACML use model and the messages that are used to communicate between the various components. Not all components will be used in every implementation.



This specification describes all these query and statement schema elements, and describes how to use them. It also describes some other aspects of using SAML with XACML. This specification requires no changes or extensions to XACML, but does define extensions to SAML.

1.1 Notation

In order to improve readability, the examples in this profile assume use of the following XML Internal Entity declarations:

```
^lt;!ENTITY saml "urn:oasis:names:tc:SAML:2.0:assertion"
```


Copyright © OASIS Open 2004. All Rights Reserved.

```
^lt;!ENTITY samlp "urn:oasis:names:tc:SAML:2.0:protocol"
^lt;!ENTITY xacml "urn:oasis:names:tc:xacml:2.0:">
^lt;!ENTITY xacml-context "urn:oasis:names:tc:xacml:2.0:context">
^lt;!ENTITY xml "http://www.w3.org/2001/XMLSchema#">
^lt;!ENTITY subject-category
            "urn:oasis:names:tc:xacml:1.0:subject-category:">
^lt;!ENTITY subject "urn:oasis:names:tc:xacml:1.0:subject:">
^lt;!ENTITY resource "urn:oasis:names:tc:xacml:1.0:resource:">
^lt;!ENTITY action "urn:oasis:names:tc:xacml:1.0:action:">
^lt;!ENTITY environment "urn:oasis:names:tc:xacml:1.0:environment:">
```

For example, `&xml;#string` is equivalent to `http://www.w3.org/2001/XMLSchema#string`.

1.2 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].

AA – Attribute Authority. An entity that binds attributes to identities. Such a binding may be expressed using a SAML Attribute Assertion with the Attribute Authority as the issuer.

Attribute - In this Profile, the term “Attribute”, when capitalized, may refer to either an XACML Attribute or to a SAML Attribute. The term will always be preceded with the type of Attribute intended.

- An XACML Attribute is a typed name/value pair, with other optional information, specified using an XACML Request Context `<xacml-context:Attribute>` element. An XACML Attribute is associated with an identity by the Attribute's position within the XACML Request; for example, an XACML Attribute contained within the `<xacml-context:Resource>` element is an attribute of that resource.
- A SAML Attribute is also a typed name/value pair, with other optional information, specified using a SAML Assertion `<saml:Attribute>` element. A SAML Attribute is associated with a particular subject by its inclusion in a `<saml:SubjectStatement>` element. The SAML subject may correspond to an XACML subject, resource, action, or environment.

attribute – In this profile, the term “attribute”, when not capitalized, refers to a generic attribute or characteristic unless it is preceded by the term “XML”. An “XML attribute” is a syntactic component in XML that occurs inside the opening tag of an XML element.

PA – Policy Authority. An entity that issues authorization policies. Such policies may be expressed using a SAML Policy Assertion with the Policy Authority as the issuer.

PDP - Policy Decision Point. An entity that evaluates an access request against one or more policies to produce an access decision.

PEP – Policy Enforcement Point. An entity that enforces access control for one or more resources. When a resource access is attempted, a PEP sends an access request describing the attempted access to a PDP. The PDP returns an access decision that the PEP then enforces.

policy – A set of rules indicating which subjects are permitted to access which resources using which actions under which conditions. XACML has two different schemas for policies: `<Policy>` and `<PolicySet>`. A `<PolicySet>` is a collection of other `<Policy>` and `<PolicySet>` elements. A `<Policy>` contains actual access control rules.

Copyright © OASIS Open 2004. All Rights Reserved.

2 Attributes (normative)

The SAML assertion schema defines an Attribute Assertion. The SAML protocol schema defines an AttributeQuery used for requesting instances of Attribute Assertions, and a Response that contains the requested instances. Systems using XACML MAY use instances of these SAML elements to request, transmit, and store SAML Attributes. In order to be used in an XACML Request Context, the SAML Attribute MUST be mapped to an XACML Attribute. This Section describes that mapping.

2.1 Mapping a SAML Attribute Assertion to XACML Attributes

A SAML Attribute Assertion is a <saml:Assertion> instance that contains one or more <saml:AttributeStatement> instances, each of which may contain one or more <saml:Attribute> instances. If an <xacml-context:Attribute> is created from a <saml:Attribute>, the <xacml-context:Attribute> MUST be populated from the contents of the <saml:Attribute> and its SAML Attribute Assertion as follows.

- XACML AttributeId XML attribute

  The value of the <saml:Attribute> Name XML attribute SHALL be used.

- XACML DataType XML attribute

  The value of the <saml:Attribute> AttributeFormat XML attribute SHALL be used.

- XACML Issuer XML attribute

  The value of the <saml:Issuer> element SHALL be used.

- <xacml-context:AttributeValue>

  The <xacml-context:AttributeValue> value SHALL be used.

Each <saml:Attribute> instance is mapped to a single <xacml-context:Attribute> element. Not all <saml:Attribute> instances in a SAML Attribute Assertion need to be mapped; the SAML Attribute instances to be mapped may be selected by a mechanism not specified here. The Issuer of the <saml:Assertion> element is used as the Issuer for each <xacml-context:Attribute> element that is created.

The <xacml-context:Attribute> created from the <saml:Assertion> SHALL be placed into the <xacml-context:Resource>, <xacml-context:Subject>, <xacml-context:Action>, or <xacml-context:Environment> element that corresponds to the entity that is the <saml:Subject> in the SAML Attribute Assertion. For example, if the SAML Attribute Assertion Subject contains a <saml:NameIdentifier> element, and the value of that NameIdentifier matches the &resource;resource-id <xacml-context:Attribute> value, then <xacml-context:Attribute> instances created from <saml:Attribute> instances in that SAML Attribute Assertion MUST be placed into the <xacml-context:Resource> element. If the <xacml-context:Attribute> is placed into an <xacml-context:Subject> element, then the XACML SubjectCategory XML element MUST also be consistent with the entity that is the Subject of the <saml:Assertion>.

The entity performing the mapping MUST ensure that the semantics defined by SAML for the elements in the <saml:Assertion> have been adhered to. The mapping entity need not perform these semantic checks itself, but it MUST ensure that the checks have been done before any <xacml:Attribute> created from the <saml:Assertion> is used by an XACML PDP. These semantic checks include, but are not limited to, the following.

- Any NotBefore and NotAfter XML attributes in the <saml:Assertion> MUST be valid with respect to the <xacml:Request> in which the SAML-derived <xacml:Attribute> will be used. This means that the NotBefore and NotAfter XML attribute values must be consistent with the &environment;current-time, &environment;current-date, and &environment:current-dateTime <xacml:Attribute> values associated with the <xacml:Request>.

Copyright © OASIS Open 2004. All Rights Reserved.

- The entity doing the mapping MUST ensure that the semantics defined by SAML for any `<saml:AudienceRestrictionCondition>` or `<saml:DoNotCacheCondition>` elements have been adhered to.
- If a `<ds:Signature>` element occurs in the `<saml:Assertion>`, then the entity performing the mapping MUST ensure that the signature is valid and that the SAML `Issuer` XML attribute is consistent with any `<ds:X509IssuerName>` value in the signature. The guidelines regarding digital signatures in Section 5 of the SAML core specification [] MUST be adhered to.

*[**Issue:** do we want to provide a non-normative XSLT for mapping the SAML Attribute Assertion to one or more XACML Attributes?]*

*[**Issue:** do we want to define the following mappings:*

- *SAML 2.0 Attribute to XACML 1.0/1.1 Attribute*
- *SAML 1.0/1.1 Attribute to XACML 2.0 Attribute*
- *SAML 2.0 Attribute to XACML 1.0/1.1 Attribute*

If so, do we want to provide non-normative XSLT for the mappings?]

Copyright © OASIS Open 2004. All Rights Reserved.

3 Authorization Decisions (normative)

SAML defines a very rudimentary AuthorizationDecisionQuery in the SAML Protocol Schema and a very rudimentary AuthorizationDecision Assertion containing a `<saml:AuthorizationDecisionStatement>` in the SAML Assertion Schema. A SAML AuthorizationDecisionQuery is unable to convey all the information that an XACML PDP is capable of acceptiing as part of its Request Context. Likewise, the SAML AuthorizationDecision Assertion is unable to convey all the information contained in an XACML Response Context.

In order to allow a PEP to use the SAML Query and Response syntax with full support for the XACML Request and Response Context syntax, this specification defines two SAML extensions:

- `<XACMLAuthorizationDecisionQuery>` is a SAML Query that extends the SAML Protocol Schema. It allows a PEP to submit an XACML Request Context in a SAML Query, along with other information.
- `<XACMLAuthorizationDecisionStatement>` is a SAML Statement that extends the SAML Assertion schema. It allows an XACML PDP to return an XACML Response Context in the Response to an `<XACMLAuthorizationDecisionStatement>`, along with other information. It also allows an XACML Response Context to be stored or transmitted in the form of a SAML Assertion.

This Section defines these extensions.

*[**Issue:** Should we describe and provide non-normative XSLT for mapping native SAML AuthorizationDecisionQuery and AuthorizationDecisionStatement to and from XACML Request and Response? Michiharu did an early version of this [].]*

*[**Issue:** Should we describe mappings between pre-2.0 SAML AuthorizationDecisionQuery and/or pre-2.0 XACML Request formats? Likewise for responses? If so, should we provide non-normative XSLT transforms for those mappings?]*

*[**Issue:** Currently, SAML QueryAbstractType is extensible, but there is no way to specify an extension to this type as the payload of a SAML Request. Similarly for SAML Statement and the inclusion of extensions to that in a SAML Assertion or SAML Response. SAML 2.0 is addressing this issue. Until the SAML 2.0 extensibility mechanism is settled, we do not know whether we must define an XACMLRequest, XACMLAssertion, and XACMLResponse.]*

3.1 Element `<XACMLAuthorizationDecisionQuery>`

The `<XACMLAuthorizationQuery>` element is used by a PEP to request an authorization decision from an XACML PDP. It allows a SAML Query to convey an XACML Request Context instance.

```
<element name="XACMLAuthorizationDecisionQuery"
         type="XACMLAuthorizationDecisionQueryType"/>
<complexType name="XACMLAuthorizationDecisionQueryType">
    <complexContent>
        <extension base="samlp:QueryAbstractType">
            <sequence>
                <element ref="xacml-context:Request>/>
            </sequence>
            <attribute name="InputContextOnly"
                       type="boolean"
                       use="required"/>
            <attribute name="ReturnContext"
                       type="boolean"
                       use="required"/>
        </extension>
    </complexContent>
</complexType>
```

The `<XACMLAuthorizationDecisionQuery>` element is of XACMLAuthorizationDecisionQueryType

Copyright © OASIS Open 2004. All Rights Reserved.

complex type. This element is an alternative to the SAML-defined <samlp:AuthorizationDecisionQuery> that allows a PEP to use the full capabilities of an XACML PDP.

The <XACMLAuthorizationDecisionQuery> element contains the following attributes and elements:

InputContextOnly [Required]

This attribute governs the sources of information that the PDP is allowed to use in making its authorization decision. If this attribute is "True", then the authorization decision MUST be made solely on the basis of information contained in the <XACMLAuthorizationDecisionQuery>; no external attributes MAY be used. If this attribute is "False", then the authorization decision MAY be made on the basis of external attributes not contained in the <XACMLAuthorizationDecisionQuery>.

ReturnContext [Required]

This attribute allows the PEP to request that an <xacml-context:Request> element be included in the <XACMLAuthorizationDecisionStatement> resulting from the request. It also governs the contents of that <xacml-context:Request> element.

If this attribute is "True", then the PDP MUST include the <xacml-context:Request> element in the <XACMLAuthorizationDecisionStatement> element in the <XACMLResponse>. This <xacml-context:Request> element MUST include all those XACML Attributes supplied by the PEP in the <XACMLAuthorizationDecisionQuery> that were used in making the authorization decision. The PDP MAY include additional XACML Attributes in this <xacml-context:Request> element, such as external attributes obtained by the PDP and used in making the authorization decision or other attributes known by the PDP that may be useful to the PEP in making subsequent <XACMLAuthorizationDecisionQuery> requests.

If this element is "False", then the PDP MUST NOT include the <xacml-context:Request> element in the <XACMLAuthorizationDecisionStatement> element of the <XACMLResponse> .

<xacml-context:Request> [Required]

An XACML Request Context.

3.2 Element <XACMLAuthorizationDecisionStatement>

The <XACMLAuthorizationDecisionStatement> is used by an XACML PDP to return a SAML Response containing an XACML Response Context to a PEP in response to an <XACMLAuthorizationDecisionQuery>. It may also be used in a SAML Assertion as a format for storage of a authorization decision in a repository..

Copyright © OASIS Open 2004. All Rights Reserved.

```
<element name="XACMLAuthorizationDecisionStatement"
         type="XACMLAuthorizationDecisionStatementType"/>
<complexType name="XACMLAuthorizationDecisionStatementType">
    <complexContent>
        <extension base="saml:StatementAbstractType">
          <sequence>
            <element ref="xacml-context:Response"/>
            <element ref="xacml-context:Request"
                     MinOccurs="0"/>
          </sequence>
        </extension>
    </complexContent>
</complexType>
```

The <XACMLAuthorizationDecisionStatement> element is of **XACMLAuthorizationDecisionStatementType** complex type. This element is an alternative to the SAML-defined <samlp:AuthorizationDecisionStatement> that allows a SAML Assertion to contain the full content of the response from an XACML PDP.

The <XACMLAuthorizationDecisionStatement> element contains the following elements:

<xacml-context:Response> [Required]

The XACML Response Context created by the XACML PDP in response to the <XACMLAuthorizationDecisionQuery>.

<xacml-context:Request> [Optional]

An <xacml-context:Request> containing XACML Attributes returned by the XACML PDP in response to the <XACMLAuthorizationDecisionQuery>. This element MUST be included if the ReturnResponse XML attribute in the <XACMLAuthorizationDecisionQuery> is "True". This element MUST NOT be included if the ReturnResponse XML attribute in the <XACMLAuthorizationDecisionQuery> is "False".

See Section [] for a description of the XACML <Attribute> values that MUST be returned in this element.

Copyright © OASIS Open 2004. All Rights Reserved.

4 Policies (normative)

XACML defines two policy schema elements: Policy and PolicySet. SAML does not define any Protocol or Assertion schemas for policies. This Section defines new SAML extensions for PolicyQuery and Policy Assertion schemas. Instances of these new extensions can be used to request, transmit, and store XACML Policy and PolicySet instances.

4.1 Element <XACMLPolicyQuery>

*[**Issue**: define abstract SAML PolicyQuery as part of SAML 2.0, of which XACMLPolicyQuery is an XACML TC-defined extension, or define just a specific XACMLPolicyQuery?]*

The <XACMLPolicyQuery> element is used by an PDP to request one or more XACML Policy or PolicySet instances from an on-line Policy Authority as part of a SAML Request.

```
<element name="XACMLPolicyQuery"
         type="XACMLPolicyQueryType"/>
<complexType name="XACMLPolicyQueryType">
    <complexContent>
        <extension base="samlp:QueryAbstractType">
            <choice minOccurs="0" maxOccurs="unbounded">
                <element ref="xacml-context:Request"/>
                <element ref="xacml:PolicySetIdReference"/>
                <element ref="xacml:PolicyIdReference"/>
            </choice>
        </extension>
    </complexContent>
</complexType>
```

The <XACMLPolicyQuery> element is of XACMLPolicyQueryType complex type.

The <XACMLPolicyQuery> element contains one of the following elements:

<xacml-context:Request> [Any Number]

Supplies an XACML Request Context. All XACML Policy and PolicySet instances applicable to this Request are to be returned. The concept of "applicability" in the XACML context is defined in the XACML 2.0 Specification [].

<xacml:PolicySetIdReference> [Any Number]

Identifies an XACML <PolicySet> to be returned.

<xacml:PolicyIdReference> [Any Number]

Identifies an XACML <Policy> to be returned.

*[**Issue**: Should we allow a single XACMLPolicyQuery be limited to one Request, PolicySetIdRef, or PolicyIdRef ("selector"), or should we allow a single XACMLPolicyQuery to contain multiple selectors, as in the schema above?]*

*[**Issue**: If a single Query can include multiple selectors, do we need to link each returned element by the selector that it matches? What if it matches more than one selector?]*

4.2 Element <XACMLPolicyStatement>

[This is XACML 2.0 Work Item #40] Need to define a SAML Assertion whose payload is an XACML Policy or PolicySet. May want to include other information from the PolicyQuery. Should be able to return multiple Policy and PolicySet instances.]

*[**Issue:** define abstract SAML Policy Assertion as part of SAML 2.0, of which XACMLPolicyAssertion is an extension, or just specific XACMLPolicyAssertion. In either case, XACMLPolicyAssertion will be*

Copyright © OASIS Open 2004. All Rights Reserved.

defined as a SAML extension by the XACML TC in the XACML namespace.]

The <XACMLPolicyStatement> is used by a Policy Authority to return one or more XACML Policy or PolicySet instances in a SAML Response to an <XACMLPolicyQuery> SAML Request. The <XACMLPolicyStatement> may also be used in a SAML Assertion as a format for storing the <XACMLPolicyStatement> in a repository.

```
<element name="XACMLPolicyStatement"
         type="XACMLPolicyStatementType"/>
<complexType name="XACMLPolicyStatementType">
    <complexContent>
        <extension base="saml:StatementAbstractType">
          <choice minOccurs="0" maxOccurs=unbounded">
            <element ref="xacml:Policy"/>
            <element ref="xacmlPolicySet"/>
          </choice>
        </extension>
    </complexContent>
</complexType>
```

The <XACMLPolicyStatement> element is of XACMLPolicyStatementType complex type.

The <XACMLPolicyStatement> element contains the following elements. If there are no <xacml:Policy> or <xacml:PolicySet> instances that meet the specifications of the associated <XACMLPolicyQuery>, then there MUST be no elements in the <XACMLPolicyStatement>.

<xacml:Policy> [Any Number]

An <xacml:Policy> instance that meets the specifications of the associated <XACMLPolicyQuery>.

<xacml:PolicySet> [Any Number]

An <xacml:PolicySet> instance that meets the specifications of the associated <XACMLPolicyQuery>.

Copyright © OASIS Open 2004. All Rights Reserved.

5 References

5.1 Normative References

[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

[XACML] T. Moses, ed., *OASIS eXtensible Access Control Markup Language (XACML) Version 1.1*,http://www.oasis-open.org/committees/xacml/repository/cs-xacml-specification-1.1.pdf, Committee Specification, 24 July 2003.

5.2 Non-normative References

[XACMLIntro] A Brief Introduction to XACML, http://www.oasis-open.org/committees/download.php/2713/Brief_Introduction_to_XACML.html, 14 March 2003.

Agreement between SSTC and XACML recorded in http://lists.oasis-open.org/archives/xacml/200309/msg00039.html. Since then it was decided that the extensions would be defined by the XACML TC as specific XACMLAuthorizationDecisionQuery and XACMLAuthorizationDecisionStatement extensions to SAML, rather than as a new SAML AuthorizationDecisionQuery/Statement format.

XSLT to map saml:AuthorizationDecisionQuery to XACML Request and XACML Response to saml:Response
http://lists.oasis-open.org/archives/xacml/200207/msg00008.html This was written against a pre-1.0 version of XACML, so is somewhat out of date. By Michiharu Kudo.

Copyright © OASIS Open 2004. All Rights Reserved.

A. Acknowledgments

The editor would like to acknowledge the contributions of the OASIS XACML Technical Committee, whose voting members at the time of publication were:

- *Frank Siebenlist, Argonne National Laboratory*
- *Daniel Engovatov, BEA Systems, Inc.*
- *Hal Lockhart, BEA Systems, Inc.*
- *Tim Moses, Entrust*
- *Maryann Hondo, IBM*
- *Michiharu Kudo, IBM*
- *Michael McIntosh, IBM*
- *Anthony Nadalin, IBM*
- *Rebekah Lepro, NASA*
- *Steve Anderson, OpenNetwork*
- *Simon Godik, Overxeer*
- *Bill Parducci, Overxeer*
- *Anne Anderson, Sun Microsystems*
- *Seth Proctor, Sun Microsystems*
- *Polar Humenn, Syracuse University*

In addition, the following people made contributions to this specification:

- *Ravi Sandhu, George Mason Univ.*
- *John Barkley, NIST*
- *Ramaswamy Chandramouli, NIST*
- *David Ferraiolo, NIST*
- *Rick Kuhn, NIST*
- *Serban Gavrila, VDG Inc.*

Copyright © OASIS Open 2004. All Rights Reserved.

B. Revision History

Rev	Date	By Whom	What
01	25 Feb 2004	Anne Anderson	Initial Working Draft.
02	03/10/04	Anne Anderson	Added proposed extension schemas and normative text. Makes use of sstc-maler-w28a-attribute-draft-02, which has not been approved by SSTC. Based on SAML 2.0 Draft 07 core and schemas.

Copyright © OASIS Open 2004. All Rights Reserved.

C. 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.

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

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.