SAML 2.0 profile of XACML

Committee Draft 02, 11 November 2004

Document identifier:

access_control-xacml-2.0-saml_profile-spec-cd-02

Location:

http://docs.oasis-open.org/xacml/access_control-xacml-2.0-saml_profile-spec-cd-02.pdf

Editors:

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 2.0 Attribute Assertions with XACML.

Status:

This version of the specification is an approved Committee Draft within the OASIS Access Control TC.

Access Control TC members should send comments on this specification to the xacml@lists.oasis-open.org list. Others may use the following link and complete the comment form: http://oasis-open.org/committees/comments/form.php?wg_abbrev=xacml.

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 Access Control TC web page (http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml).

For any errata page for this specification, please refer to the Access Control TC web page (http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml).

Table of Contents

1 Introduction (non-normative)

The OASIS eXtensible Access Control Markup Language [XACML] 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 [XACMLIntro].

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 AAs have stored attributes. The PDP (or, more precisely, its Context Handler component) 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 Administration Points* (PAP) or from *Policy Repositories* into which PAPs 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 Administration Point, Attribute Authority, Context Handler, 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 Assertion Markup Language (SAML), Version 2.0 [SAML]. 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 describes 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 schema instances and other information needed by an XACML implementation.

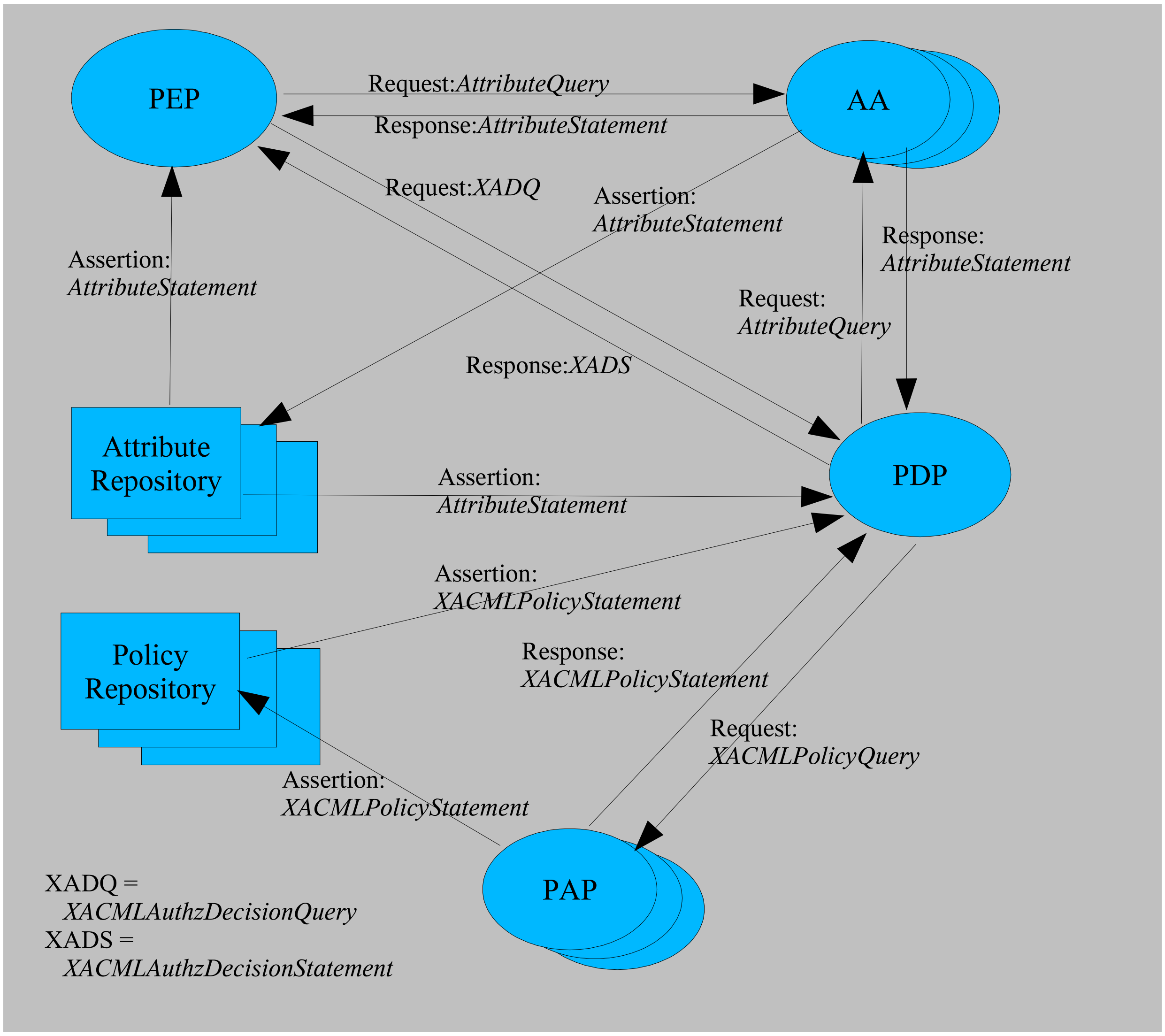
There are 6 types of queries and statements used in this profile:

1. AttributeQuery – A standard SAML Request 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 Request extension, defined in this profile. It is used for requesting one or more policies from a Policy Administration Point.
4. XACMLPolicyStatement – A SAML Statement extension, defined in this profile. It may be used in a SAML Response from a Policy Administration Point, or it may be used in a SAML Assertion as a format for storing policies in a Policy Repository.

5. XACMLAuthzDecisionQuery – A SAML Request extension, defined in this profile. It is used by a PEP to request an authorization decision from an XACML PDP.

6. XACMLAuthzDecisionStatement – 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"
^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:schema:cd-01"
^lt;!ENTITY xml "http://www.w3.org/2001/XMLSchema#"
^lt;!ENTITY subject-id
      "urn:oasis:names:tc:xacml:1.0:subject:subject-id"
^lt;!ENTITY resource "urn:oasis:names:tc:xacml:1.0:resource:"
^lt;!ENTITY resource-id
      "urn:oasis:names:tc:xacml:1.0:resource:resource-id"
^lt;!ENTITY action-id "urn:oasis:names:tc:xacml:1.0:action:action-id"
^lt;!ENTITY environment "urn:oasis:names:tc:xacml:1.0:environment:"
^lt;!ENTITY current-dateTime
      "urn:oasis:names:tc:xacml:1.0:environment:current-dateTime"
```

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

The namespace associated with the XACML schema [XACML-SAML] that extends the SAML Assertion schema is

```
xacml-saml="urn:oasis:names:tc:xacml:2.0:saml:assertion:schema:cd-01"
```

The namespace associated with the XACML schema [XACML-SAMLP] that extends the SAML Protocol schema is

```
xacml-samlp="urn:oasis:names:tc:xacml:2.0:saml:protocol:schema:cd-01"
```

1.2 Terminology

The key words “MUST”, “MUST NOT”, ”REQUIRED”, ”SHALL”, ”SHALL NOT”, ”SHOULD”, ”SHOULD NOT”, ”RECOMMENDED”, ”MAY”, and ”OPTIONAL” in this specification are to be interpreted as described in IETF RFC 2119 [RFC2119]:

> *“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.

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 the initial letter is 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 XACML 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 a 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 even 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.

PAP – Policy Administration Point. An entity that issues authorization policies. Such policies may be expressed using a SAML Policy Assertion with the Policy Administration Point 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 schema elements used for policies: `<Policy>` and `<PolicySet>`. A `<PolicySet>` is a collection of other `<Policy>` and `<PolicySet>` elements. A `<Policy>` contains actual access control rules.

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 transmit and store SAML Attributes. Systems using XACML MAY use the SAML AttributeQuery protocol to request instances of SAML Attributes. In order to be used in an XACML Request Context, the SAML Attribute SHALL 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.

In order to be used in an XACML Request Context, each SAML Attribute in the SAML Attribute Assertion SHALL comply with *XACML Attribute Profile* (Section 8.5), namespace `urn:oasis:names:tc:SAML:2.0:profiles:attribute:XACML`, in the *Profiles for the OASIS Security Assertion Markup Language* [SAML-PROFILE].

An `<xacml-context:Attribute>` SHALL be constructed from the corresponding `<saml:Attribute>` element in a SAML Attribute Assertion as follows.

- XACML `AttributeId` XML attribute

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

- XACML `DataType` XML attribute

  The fully-qualified value of the `<saml:Attribute> DataType` XML attribute SHALL be used. If the `<saml:Attribute> DataType` XML attribute is missing, the XACML `DataType` XML attribute SHALL be `http://www.w3.org/2001/XMLSchema#string`.

- XACML `Issuer` XML attribute

  The string value of the `<saml:Issuer>` element from the SAML Attribute Assertion SHALL be used.

- <xacml-context:AttributeValue>

  The `<saml:AttributeValue>` value SHALL be used as the value of the `<xacml-context:AttributeValue>` element.

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 value of the `<xacml-context:Attribute>` having an `AttributeId` of `&resource;resource-id`, then `<xacml-context:Attribute>` instances created from `<saml:Attribute>` instances in that SAML Attribute Assertion SHALL 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 attribute SHALL also be consistent with the entity that is the Subject of the

<saml:Assertion>.

The entity performing the mapping SHALL 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 SHALL 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 NotOnOrAfter XML attributes in the <saml:Assertion> SHALL be valid with respect to the <xacml:Request> in which the SAML-derived <xacml:Attribute> is used. This means that the NotBefore and NotOnOrAfter XML attribute values SHALL be consistent with the &environment;current-time, &environment;current-date, and &environment:current-dateTime <xacml:Attribute> values associated with the <xacml:Request>.
- The entity doing the mapping SHALL 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 SHALL ensure that the signature is valid and that the SAML <Issuer> element is consistent with any <ds:X509IssuerName> value in the signature. The guidelines regarding digital signatures in Section 5: *SAML and XML Signature Syntax and Processing* of the SAML core specification [SAML] SHALL be adhered to.

3 Authorization Decisions (normative)

SAML 2.0 defines a rudimentary AuthzDecisionQuery in the SAML Protocol Schema and a rudimentary AuthzDecisionStatement in the SAML Assertion Schema. A SAML AuthzDecisionQuery is unable to convey all the information that an XACML PDP is capable of accepting as part of its Request Context. Likewise, the SAML AuthzDecisionStatement is unable to convey all the information contained in an XACML Response Context.

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

- `<xacml-samlp:XACMLAuthzDecisionQuery>` is a SAML Query that extends the SAML Protocol Schema. It allows a PEP to submit an XACML Request Context in a SAML Request, along with other information.
- `<xacml-saml:XACMLAuthzDecisionStatement>` 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 `<XACMLAuthzDecisionStatement>`, 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. The extensions are contained in [XACML-SAML] and [XACML-SAMLP].

3.1 Element `<XACMLAuthzDecisionQuery>`

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

```
<xs:element name=”XACMLAuthzDecisionQuery”
            type=”XACMLAuthzDecisionQueryType”/>
<xs:complexType name=”XACMLAuthzDecisionQueryType”>
    <xs:complexContent>
        <xs:extension base=”samlp:RequestAbstractType”>
            <xs:sequence>
                <xs:element ref=”xacml-context:Request”/>
            </xs:sequence>
            <xs:attribute name="InputContextOnly"
                          type="boolean"
                          use="optional"
                          default="false"/>
            <xs:attribute name=”ReturnContext”
                          type=”boolean"
                          use=”optional”
                          default="false"/>
        </xs:extension>
    </xs:complexContent>
</xs:complexType>
```

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

The `<XACMLAuthzDecisionQuery>` element contains the following XML attributes and elements:

`InputContextOnly` [Default “false”]

This XML attribute governs the sources of information that the PDP is allowed to use in making its authorization decision. If this XML attribute is “true”, then the authorization decision SHALL be made solely on the basis of information contained in the <XACMLAuthzDecisionQuery>; no external attributes MAY be used. If this XML attribute is “false”, then the authorization decision MAY be made on the basis of external attributes not contained in the <XACMLAuthzDecisionQuery>.

ReturnContext [Default “false”]

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

If this XML attribute is “true”, then the PDP SHALL include the <xacml-context:Request> element in the <XACMLAuthzDecisionStatement> element in the <XACMLResponse>. This <xacml-context:Request> element SHALL include all those attributes supplied by the PEP in the <XACMLAuthzDecisionQuery> that were used in making the authorization decision. The PDP MAY include additional 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 <XACMLAuthzDecisionQuery> requests.

If this XML attribute is “false”, then the PDP SHALL NOT include the <xacml-context:Request> element in the <XACMLAuthzDecisionStatement> element of the <XACMLResponse> .

<xacml-context:Request> [Required]

An XACML Request Context.

3.2 Element <XACMLAuthzDecisionStatement>

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

```
<xs:element name=”XACMLAuthzDecisionStatement”
            type=”xacml-saml:XACMLAuthzDecisionStatementType”/>
<xs:complexType name=”XACMLAuthzDecisionStatementType”>
    <xs:complexContent>
        <xs:extension base=”saml:StatementAbstractType”>
          <xs:sequence>
            <xs:element ref=”xacml-context:Response”/>
            <xs:element ref=”xacml-context:Request”
                        MinOccurs=”0”/>
          </xs:sequence>
        </xs:extension>
    </xs:complexContent>
</xs:complexType>
```

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

The <XACMLAuthzDecisionStatement> element contains the following elements:

<xacml-context:Response> [Required]

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

<xacml-context:Request> [Optional]

An `<xacml-context:Request>` containing XACML Attributes returned by the XACML PDP in response to the `<XACMLAuthzDecisionQuery>`. This element SHALL be included if the `ReturnResponse` XML attribute in the `<XACMLAuthzDecisionQuery>` is “true”. This element SHALL NOT be included if the `ReturnResponse` XML attribute in the `<XACMLAuthzDecisionQuery>` is “false”.

See the description of the `ReturnContext` XML attribute in Section 3.1: *Element* *`<XACMLAuthzDecisionQuery>`* for a description of the XACML `<Attribute>` values that SHALL be returned in this element.

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 <XACMLPolicyQuery> and <XACMLPolicyStatement> elements. Instances of these new elements can be used to request, transmit, and store XACML <Policy> and <PolicySet> instances. The new extensions are contained in [XACML-SAML] and [XACML-SAMLP].

4.1 Element <XACMLPolicyQuery>

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

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

The <XACMLPolicyQuery> element is of XACMLPolicyQueryType complex type.

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

<xacml-context:Request> [Any Number]

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

<xacml:Target> [Any Number]

Supplies an XACML <Target> element. All XACML Policy and PolicySet instances applicable to this <Target> SHALL be returned.

<xacml:PolicySetIdReference> [Any Number]

Identifies an XACML <PolicySet> to be returned.

<xacml:PolicyIdReference> [Any Number]

Identifies an XACML <Policy> to be returned.

4.2 Element <XACMLPolicyStatement>

The <XACMLPolicyStatement> is used by a Policy Administration Point 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.

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

The <XACMLPolicyStatement> element is of XACMLPolicyStatementType complex type.

The <XACMLPolicyStatement> element contains the following elements. If the <XACMLPolicyStatement> is issued in response to an <XACMLPolicyQuery>, and there are no <xacml:Policy> or <xacml:PolicySet> instances that meet the specifications of the associated <XACMLPolicyQuery>, then there SHALL be no elements in the <XACMLPolicyStatement>.

<xacml:Policy> [Any Number]

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

<xacml:PolicySet> [Any Number]

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

5 Element <saml:Assertion> (normative)

An <XACMLAuthzDecisionStatement>, <XACMLPolicyStatement>, or SAML standard <saml:AttributeStatement> SHALL be encapsulated in a <saml:Assertion>, which MAY be signed.

Most components of a <saml:Assertion> are fully specified in the SAML 2.0 specification [SAML]. The following elements and XML attributes are further specified here for use with the SAML statement types defined and used in this Profile.

Except as specified here, this Profile imposes no requirements or restrictions on information in the <saml:Assertion> element.

5.1 Element <saml:Issuer>

The <saml:Issuer> element is a required element for holding information about “the SAML authority that is making the claim(s) in the assertion” [SAML].

In order to support 3rd party digital signatures, this Profile does NOT require that the identity provided in the <saml:Issuer> element be consistent with the identity of the signer. It is up to the relying party to have an appropriate trust relationship with the authority that signs the <saml:Assertion>.

When a <saml:AttributeAssertion> is used to construct an XACML Attribute, the string value of the <saml:Issuer> element will be used as the value of the XACML Issuer XML attribute, so the SAML value SHOULD be specified with this in mind. See *Section 2.1: Mapping a SAML Attribute Assertion to XACML Attributes* for more information.

5.2 Element <ds:Signature>

The <ds:Signature> element is an optional element for holding “An XML Signature that authenticates the assertion, as described in Section 5.”

A <ds:Signature> element MAY be used in an assertion used with an XACML Statement. In order to support 3rd party digital signatures, this Profile does NOT require that the identity provided in the <saml:Issuer> element be consistent with the identity of the signer. It is up to the relying party to have an appropriate trust relationship with the authority that signs the <saml:Assertion>.

A relying party SHOULD verify any signature included in the assertion and SHOULD NOT use information derived from the assertion unless the signature is verified successfully.

5.3 Element <saml:Subject>

The <saml:Subject> element is an optional element used for holding “The subject of the statement(s) in the assertion” [SAML].

The <saml:Subject> element SHALL NOT be included in an assertion that contains an <XACMLAuthzDecision> or <XACMLPolicy>.

In a <saml:AttributeAssertion> that is to be mapped to an XACML Attribute, the <saml:Subject> element SHALL contain the identity of the entity to which the attribute and its value are bound. For an XACML <Subject> Attribute, this identity SHOULD be consistent with the value of any XACML &subject-id; Attribute that occurs in the same <Subject> element. For an XACML <Resource> Attribute, this identity SHOULD be consistent with the value of any XACML &resource-id; Attribute that occurs in the same <Resource> element. For an XACML <Action> Attribute, this identity SHOULD be consistent with the value of any XACML &action-id; Attribute that occurs in the same <Action> element. For an XACML <Environment> Attribute, this identity SHOULD be consistent with the value of any XACML

Attribute that occurs in the same <Environment> element and provides an environment identity.

5.4 Element <saml:Conditions>

The <saml:Conditions> element is an optional element that is used for “conditions that MUST be taken into account in assessing the validity of and/or using the assertion” [SAML].

The <saml:Conditions> element SHOULD contain NotBefore and NotOnOrAfter XML attributes to specify the limits on the validity of the assertion. If these XML attributes are present, the relying party SHOULD ensure that information derived from the assertion is used by a PDP for evaluating policies only when the value of the request context &current-dateTime; resource attribute is contained within the assertion's specified validity period.

6 Element <samlp:RequestAbstractType> (normative)

An `<XACMLAuthzDecisionQuery>` or `<XACMLPolicyQuery> SHALL be` encapsulated in a `<samlp:RequestAbstractType>` element, which MAY be signed.

Most components of a `<samlp:RequestAbstractType>` are fully specified in the SAML 2.0 specification [SAML]. The following elements and XML attributes are further specified here for use with the SAML query types defined and used in this Profile. Except as specified here, this Profile imposes no requirements or restrictions on information in the `<samlp:RequestAbstractType>` element.

6.1 Element <saml:Issuer>

See *Section 5.1: Element <saml:Issuer>*.

6.2 Element <ds:Signature>

See *Section 5.2: Element <ds:Signature>*.

7 Element <samlp:Response> (normative)

An <XACMLAuthzDecisionStatement> or <XACMLPolicyStatement> SHALL be encapsulated in a <samlp:Response> element, which MAY be signed.

Most components of a <samlp:Response> are fully specified in the SAML 2.0 specification [SAML]. The following elements and XML attributes are further specified here for use with the SAML statement types defined and used in this Profile. Except as specified here, this Profile imposes no requirements or restrictions on information in the <samlp:Response> element.

7.1 Element <samlp:Issuer>

See *Section 5.1: Element <saml:Issuer>*.

7.2 Element <ds:Signature>

See *Section 5.2: Element <ds:Signature>*.

7.3 Element <samlp:StatusCode>

The <samlp:StatusCode> element is a component of the <samlp:Status> element in the <samlp:Response>.

7.3.1 Response to <XACMLAuthzDecisionQuery>

In the response to an <XACMLAuthzDecisionQuery> request, the <samlp:StatusCode> Value XML attribute SHALL depend on the <xacml:StatusCode> element of the authorization decision <xacml:Status> element as follows:

urn:oasis:names:tc:SAML:2.0:status:Success

> This value for the <samlp:StatusCode> Value XML attribute SHALL be used if and only if the <xacml:StatusCode> value is urn:oasis:names:tc:xacml:1.0:status:ok.

urn:oasis:names:tc:SAML:2.0:status:Requester

> This value for the <samlp:StatusCode> Value XML attribute SHALL be used when the <xacml:StatusCode> value is urn:oasis:names:tc:xacml:1.0:status:missing-attribute or the when the <xacml:StatusCode> value is urn:oasis:names:tc:xacml:1.0:status:syntax-error due to a syntax error in the <xacml:Request>.

urn:oasis:names:tc:SAML:2.0:status:Responder

> This value for the <samlp:StatusCode> Value XML attribute SHALL be used when the <xacml:StatusCode> value is urn:oasis:names:tc:xacml:1.0:status:syntax-error due to a syntax error in an <xacml:Policy> or <xacml:PolicySet>. Note that not all syntax errors in policies will be detected in conjunction with the processing of a particular query, so not all policy syntax errors will be reported this way.

urn:oasis:names:tc:SAML:2.0:status:VersionMismatch

> This value for the <samlp:StatusCode> Value XML attribute SHALL be used only when the SAML interface at the PDP does not support the version of the SAML request message used in the query.

7.3.2 Response to <XACMLPolicyQuery>

In the response to an <XACMLPolicyQuery> request, the <samlp:StatusCode> Value XML attribute SHALL be as specified in the SAML specification.

8 References

8.1 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.

[SAML] S. Cantor, et al., eds., *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0*, Committee Draft 01c, 18 September 2004*,* http://www.oasis-open.org/committees/documents.php?wg_abbrev=security.

[SAML-PROFILE] J. Hughes, et al., eds., *Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0*, Committee Draft 01b, 14 September 2004, http://www.oasis-open.org/committees/documents.php?wg_abbrev=security**.**

[XACML] S. Godik, T. Moses, eds., *OASIS eXtensible Access Control Markup Language (XACML) Version 2.0*, Committee Draft 01, 16 September 2004, http://docs.oasis-open.org/xacml/access_control-xacml-2.0-core-spec-cd-01.pdf.

[XACML-SAML] A. Anderson, ed., *access_control-xacml-2.0-saml-assertion-schema-cd-01.xsd*, http://docs.oasis-open.org/xacml/access_control-xacml-2.0-saml-assertion-schema-cd-01.xsd.

[XACML-SAMLP] A. Anderson, ed., *access_control-xacml-2.0-saml-protocol-schema-cd-01.xsd*, http://docs.oasis-open.org/xacml/access_control-xacml-2.0-saml-protocol-schema-cd-01.xsd.

8.2 Non-normative References

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

A. Acknowledgments

The editors would like to acknowledge the contributions of the OASIS XXX 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.
- Rebekah Metz, Booz Allen Hamilton
- Ronald Jacobson, Computer Associates
- Tim Moses, Entrust
- Simon Godik, GlueCode Software
- Bill Parducci, GlueCode Software
- Michiharu Kudo, IBM
- Michael McIntosh, IBM
- Anthony Nadalin, IBM
- Steve Anderson, OpenNetwork
- Anne Anderson, Sun Microsystems
- Seth Proctor, Sun Microsystems
- Polar Humenn, Syracuse University
- Edward Coyne, Veterans Health Administration

B. Revision History

Rev	Date	By Whom	What
CD-01	16 Sept 2004	XACML committee	Committee Draft
CD-02	11 Nov 2004	XACML committee	-Section 5.1: changed “the string value of the <saml:Issuer> element SHALL be used” to “the string value of the <saml:Issuer> element will be used” -Replaced <samlp:Request> with <samlp:RequestAbstractType>

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.

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.