SAML 2.0 Profile of XACML 2.1

Working Draft 1, 12 April 2006

Document identifier:
xacml-2.1-profile-saml2.0-spec-wd-1

OASIS identifier:
[OASIS document number]

Location:
Persistent: http://docs.oasis-open.org/xacml/2.1/xacml-2.1-profile-saml2.0.zip
This Version:
http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml#CURRENT
Previous Version:
http://www.oasis-open.org/committees/download.php/15447/xacml-2.0-saml-errata-wd.zip

Technical Committee:
OASIS eXtensible Access Control Markup Language (XACML) TC

Chair(s):
Hal Lockhart
Bill Parducci

Editor:
Anne Anderson

Subject / Keywords:
XACML, SAML, access control, security assertions, policy

OASIS Conceptual Model Topic Area:
Security

Related Work:
This specification replaces or supercedes:

- SAML 2.0 profile of XACML 2.0

This specification is related to:

- SAML 2.0 OASIS Standard
- XACML 2.0 OASIS Standard

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. This version defines a more complete extension of SAML for use in XACML systems than in the previous version.

Status:

This document was last revised or approved by the eXtensible Access Control Markup Language (XACML) TC on the above date. The level of approval is also listed above. Check the current location noted above for possible later revisions of this document. This document is updated periodically on no particular schedule.

Technical Committee members should send comments on this specification to the Technical Committee's email list. Others should send comments to the Technical Committee by using the "Send A Comment" button on the Technical Committee's web page at www.oasis-open.org/committees/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 Technical Committee web page (www.oasis-open.org/committees/xacml/ipr.php.

The non-normative errata page for this specification is located at www.oasis-open.org/committees/xacml.

Notices

Table of Contents

1 Introduction....5
1.1 Notation....7
1.2 Terminology....8
1.3 Normative References....9
1.4 Non-normative References....9
2 Attributes....10
2.1 Element <saml:Attribute>....10
2.2 Element <saml:AttributeStatement>....11
2.3 Element <saml:Assertion>....12
2.4 Element <xacml-saml:XACMLAssertion>....13
2.5 Element <samlp:AttributeQuery>....13
2.6 Element <samlp:Response>....13
3 Authorization Decisions....14
3.1 Element <XACMLAuthzDecisionStatement>....14
3.2 Element <XACMLAssertion>....15
3.3 Element <XACMLAuthzDecisionQuery>....16
3.4 Element <XACMLResponse>....18
4 Policies....20
4.1 Element <XACMLPolicyStatement>....20
4.2 Element <XACMLAssertion>....21
4.3 Element <XACMLPolicyQuery>....21
4.4 Element <XACMLResponse>....22
5 Advice....23
5.1 Element <XACMLAdvice>....23
5.2 Element <XACMLAssertion>....23

1 Introduction

[Except for schema fragments, all text is normative unless otherwise indicated.]

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 non-normative 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 artifacts can serve as a standard format for exchanging information between 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, validate, and authenticate 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, store, transport, request, and respond with XACML schema instances and other information needed by an XACML implementation.

This Profile starts by describing how to use SAML Attributes in an XACML system. It describes the use of the following elements:

1. SAML `Attribute` – A standard SAML element that MAY be used in an XACML system for storing and transmitting attribute values. The SAML `Attribute` must be transformed into an XACML `Attribute` before it can be used in an XACML Request Context.

2. SAML `AttributeStatement` – A standard SAML element that SHALL be used to hold SAML `Attribute` instances in an XACML system.

3. SAML `Assertion` – A standard SAML element that MAY be used to hold SAML `AttributeStatement` instances in an XACML system, either in an Attribute Repository or in a

SAML `Response` to a SAML `AttributeQuery`. The SAML `Assertion` contains information that is required in order to transform a SAML `Attribute` into an XACML `Attribute`. A SAML `Attribute` SHALL be contained in either a SAML `Assertion` instance or in an `XACMLAssertion` instance when used in an XACML system.

4. XACMLAssertion – A new SAML extension element that is an alternative to the SAML `Assertion` element and allows inclusion of XACML Statement instances and inclusion of other `XACMLAssertion` instances as advice. A SAML Attribute SHALL be contained in either a SAML `Assertion` instance or in an `XACMLAssertion` instance when used in an XACML system.

5. SAML `AttributeQuery` – A standard SAML protocol element that MAY be used by an XACML PDP or PEP to request SAML `Attribute` instances from an Attribute Authority for use in an XACML Request Context.

6. SAML `Response` – A standard SAML protocol element that SHALL be used to return SAML `Attribute` instances in response to a SAML `AttributeQuery` in an XACML system.

Next, this Profile describes the use of SAML for use in requesting, responding with, storing, and transmitting authorization decisions in an XACML system. The following elements are described:

1. `XACMLAuthzDecisionStatement` – A new SAML extension element defined in this Profile that MAY be used in an XACML system to hold XACML authorization decisions for storage or transmission.

2. `XACMLAssertion` – A new SAML extension element defined in this Profile that MAY be used in an XACML system to hold `XACMLAuthzDecisionStatement` instances for storage or transmission.

3. `XACMLAuthzDecisionQuery` – A new SAML extension protocol element defined in this Profile that MAY be used by a PEP to request an authorization decision from an XACML PDP.

4. `XACMLResponse` – A new SAML extension protocol element defined in this Profile that SHALL be used to return authorization decisions from an XACML PDP in response to an `XACMLAuthzDecisionQuery`.

Then, this Profile describes the use of SAML for use in requesting, responding with, storing, and transmitting XACML policies. The following elements are described:

1. `XACMLPolicyStatement` – A new SAML extension element defined in this Profile that MAY be used in an XACML system to hold XACML policies for storage or transmission.

2. `XACMLAssertion` – A new SAML extension element defined in this Profile that MAY be used in an XACML system to hold `XACMLPolicyStatement` instances for storage or transmission.

3. `XACMLPolicyQuery` – A new SAML extension protocol element defined in this Profile that MAY be used by a PDP or other application to request XACML policies from a Policy Administration Point.

4. `XACMLResponse` – A new SAML extension protocol element defined in this Profile that SHALL be used to return policies from a Policy Administration Point in response to an `XACMLPolicyQuery`.

Finally, this Profile describes the use of `XACMLAssertion` instances as advice in other Assertions. The following elements are described:

1. `XACMLAdvice` – A new SAML extension element defined in this Profile that MAY be used for including `XACMLAssertion` instances as advice in another `XACMLAssertion`.

2. `XACMLAssertion` – A new SAML extension element that MAY be used to hold an `XACMLAdvice` instance along with SAML Statement or XACML extension Statement instances.

Figure 1 illustrates the XACML use model and the messages that can be used to communicate between the various components. Statements are carried in SAML or XACML Assertions, and Assertions are carried in SAML or XACML Responses as appropriate. Not all components or messages will be used in every implementation. Not shown, but described in this specification, is the ability to use an XACML Assertion in a SAML Advice instance.

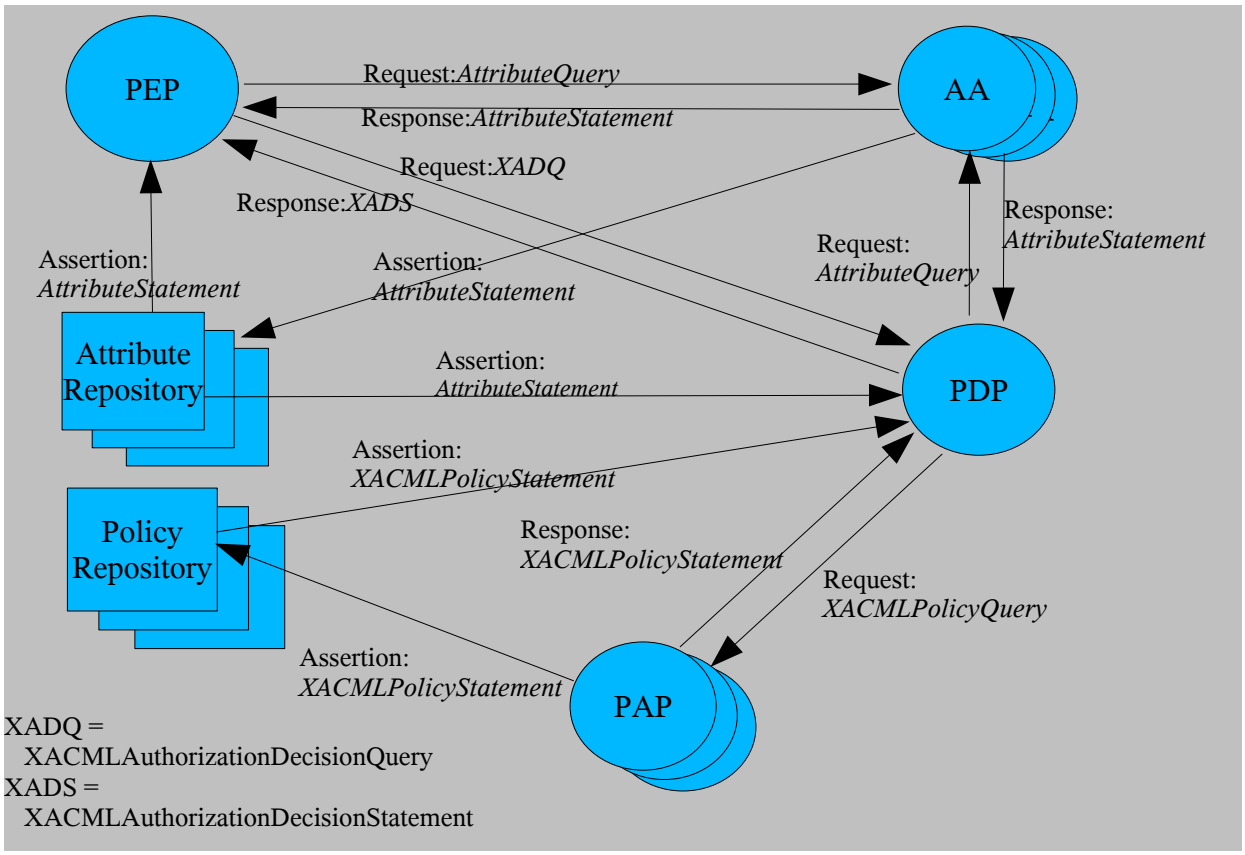

Figure 1: Components and messages in an integration of SAML with an XACML system

This specification describes all these message 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:

```
<!ENTITY saml          "urn:oasis:names:tc:SAML:2.0:assertion">
<!ENTITY samlp         "urn:oasis:names:tc:SAML:2.0:protocol">
<!ENTITY xacml         "urn:oasis:names:tc:xacml:2.0:">
<!ENTITY xacml-context "urn:oasis:names:tc:xacml:2.0:context:schema:os">
```

```
<!ENTITY xs              "http://www.w3.org/2001/XMLSchema#">
<!ENTITY subject-id      "urn:oasis:names:tc:xacml:1.0:subject:subject-id">
<!ENTITY resource        "urn:oasis:names:tc:xacml:1.0:resource:">
<!ENTITY resource-id     "urn:oasis:names:tc:xacml:1.0:resource:resource-id">
<!ENTITY action-id       "urn:oasis:names:tc:xacml:1.0:action:action-id">
<!ENTITY environment     "urn:oasis:names:tc:xacml:1.0:environment:">
<!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:2.1:profile:saml2.0:schema:assertion"
```

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

```
xacml-samlp="urn:oasis:names:tc:xacml:2.1:profile:saml2.0:schema:protocol"
```

1.2 Terminology

The keywords "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 [RFC 2119]

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 a subject, resource, action, or environment identity by the XACML Attribute's position within the XACML Request; for example, an XACML Attribute contained within a `<xacml-context:Resource>` instance 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>` instance. A SAML Attribute is associated with a particular subject by its inclusion in a `<saml:Assertion>` or an `<xacml-saml:XACMLAssertion>` instance that contains a `<saml:Subject>` instance. 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 that are used by a Policy Decision Point (PDP).

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

1.3 Normative References

[RFC 2119] 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,* 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*, http://www.oasis-open.org/committees/documents.php?wg_abbrev=security.

[XACML] T. Moses, ed., *OASIS eXtensible Access Control Markup Language (XACML) Version 2.0,* OASIS Standard, 1 February 2005, http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf.

[XACML-SAML] A. Anderson, ed., *xacml-2.1-profile-saml2.0-schema-assertion.xsd*, http://docs.oasis-open.org/xacml/2.1/xacml-2.1-profile-saml2.0-schema-assertion.xsd

[XACML-SAMLP] A. Anderson, ed., *xacml-2.1-profile-saml2.0-schema-protocol.xsd*, http://docs.oasis-open.org/xacml/2.1/xacml-2.1-profile-saml2.0-schema-protocol.xsd.

1.4 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.

2 Attributes

In an XACML system, PEPs and PDP Context Handlers often need to retrieve attributes from on-line Attribute Authorities or from Attribute Repositories. SAML provides assertion and protocol elements that MAY be used for retrieval of attributes for use in an XACML Request Context. These elements include a `<saml:Attribute>` element for expressing a named attribute value, a `<saml:AttributeStatement>` for holding a collection of `<saml:Attribute>` elements, and a `<saml:Assertion>` element that can hold various kinds of statements, including a `<saml:AttributeStatement>`. A `<saml:Assertion>` includes the name of the attribute issuer, an optional digital signature for authenticating the attribute, an optional subject identity to which the attribute is bound, and optional conditions for use of the assertion that include an optional validity period for use of the attribute. Such an assertion is suitable for storing attributes in a Repository and for transmitting attributes between an Attribute Authority and an Attribute Repository, and between an Attribute Repository and a PEP or Context Handler. The `<xacml-saml:XACMLAssertion>` element defined in this Profile is an alternative to the `<saml:Assertion>` element that MAY be used to hold `<saml:Attribute>` instances. In the remainder of this Section, “Attribute Assertion” SHALL refer to either a `<saml:Assertion>` or an `<xacml-saml:XACMLAssertion>` that contains one or more `<saml:Attribute>` instances. For querying an on-line Attribute Authority for attributes, and for holding the response to that query, SAML defines `<samlp:AttributeQuery>` and `<samlp:Response>` elements. This Section describes the use of these SAML elements in an XACML system.

Since the format of a `<saml:Attribute>` differs from that of an `<xacml-context:Attribute>`, a mapping operation is required. This Section describes how to transform information contained in an Attribute Assertion into one or more `<xacml-context:Attribute>` instances.

2.1 Element `<saml:Attribute>`

The standard SAML `<saml:Attribute>` element MAY be used in an XACML system for storing and transmitting attribute values.

In order to be used in an XACML Request Context, each SAML Attribute SHALL comply with the XACML Attribute Profile (Section 8.5), associated with 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>` instance SHALL be constructed from the corresponding `<saml:Attribute>` instance contained in an 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>` instance from the Attribute Assertion SHALL be used.

- `<xacml-context:AttributeValue>`

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

Each <saml:Attribute> instance SHALL be mapped to no more than one <xacml-context:Attribute> instance. Not all <saml:Attribute> instances in an Attribute Assertion need to be mapped; a subset of SAML Attribute instances MAY be selected by a mechanism not specified here. The Issuer of the Attribute Assertion SHALL be used as the Issuer for each <xacml-context:Attribute> instance that is created from <saml:Attribute> instances in that Attribute Assertion.

The <xacml-context:Attribute> created from the Attribute Assertion SHALL be placed into the <xacml-context:Resource>, <xacml-context:Subject>, <xacml-context:Action>, or <xacml-context:Environment> instance that corresponds to the entity that is represented by the <saml:Subject> in the Attribute Assertion. For example, if the Attribute Assertion Subject contains a <saml:NameIdentifier> instance, 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 Attribute Assertion SHALL be placed into the <xacml-context:Resource> instance. If a mapped <saml:Attribute> is placed into an <xacml-context:Subject> instance, then the XACML SubjectCategory XML attribute SHALL also be consistent with the entity that is the Subject of the Attribute Assertion that contained the <saml:Attribute>.

The entity performing the mapping SHALL ensure that the semantics defined by SAML for the elements in an Attribute 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 an Attribute 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 Attribute 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> instance occurs in the Attribute Assertion, then the entity performing the mapping SHALL ensure that the signature is valid and that the SAML <Issuer> instance 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.

2.2 Element <saml:AttributeStatement>

When a <saml:Attribute> instance is stored or transmitted in an XACML system, the instance SHALL be enclosed in a standard SAML <saml:AttributeStatement>. The definition and use of the <saml:AttributeStatement> element SHALL be as described in the SAML 2.0 standard [SAML].

2.3 Element <saml:Assertion>

When a <saml:AttributeStatement> instance is stored or transmitted in an XACML system, the instance SHALL be enclosed in either a <saml:Assertion> or <xacml-saml:XACMLAssertion>. The definition and use of the <saml:Assertion> element SHALL be as specified in the SAML 2.0 standard, augmented with the following requirements. Except as specified here, this Profile imposes no requirements or restrictions on the <saml:Assertion> element and its contents beyond those specified in SAML 2.0.

<saml:Issuer> [Required]

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:Assertion> containing a <saml:Attribute> is used to construct an XACML Attribute, the string value of the <saml:Issuer> instance will be used as the value of the XACML Issuer XML attribute, so the SAML value SHOULD be specified with this in mind.

<ds:Signature> [Optional]

The <ds:Signature> element is an optional element for holding "An XML Signature that authenticates the assertion, as described in Section 5 [of the SAML specification]."

A <ds:Signature> instance MAY be used in a <saml:Assertion>. In order to support 3rd party digital signatures, this Profile does NOT require that the identity provided in the <saml:Issuer> instance 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.

<saml:Subject> [Optional]

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

In a <saml:Assertion> containing a <saml:Attribute> that is to be mapped to an XACML Attribute, the <saml:Subject> instance SHALL contain the identity of the entity to which the attribute and its value are bound. For a mapped Attribute to be placed in the XACML <xacml-context:Subject> instance, this identity SHOULD be consistent with the value of any XACML Attribute having an AttributeId of &subject-id; that occurs in the same <xacml-context:Subject> instance. For a mapped Attribute to be placed in the XACML <xacml-context:Resource> instance, this identity SHOULD be consistent with the value of any XACML Attribute having an AttributeId of &resource-id; that occurs in the same <xacml-context:Resource> instance. For a mapped Attribute to be placed in the XACML <xacml-context:Action> instance, this identity SHOULD be consistent with the value of any XACML Attribute having an AttributeId of &action-id; that occurs in the same <xacml-context:Action> instance. For a mapped Attribute to be placed in the XACML <xacml-context:Environment> instance, this identity SHOULD be consistent with the value of any XACML Attribute that occurs in the same <xacml-context:Environment> instance and provides an environment identity. See Section 2.1 for more information.

<saml:Conditions> [Optional]

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> instance 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 an <xacml-context:Attribute> derived from the Assertion is used by a PDP for evaluating policies only when the value of the XACML Attribute in the <xacml-context:Environment> instance having an AttributeId of &current-dateTime; is contained within the Assertion's specified validity period.

2.4 Element <xacml-saml:XACMLAssertion>

The <xacml-saml:XACMLAssertion> element is an extension to the <saml:Assertion> element that MAY be used to hold <saml:AttributeStatement> instances and <saml:Attribute> instances in an XACML system. When used in an XACML system, <saml:Attribute> instances SHALL be contained in either a <saml:Assertion> or <xacml-saml:Assertion> instance.

The <xacml-saml:XACMLAssertion> element allows the inclusion of other XACML extension elements. All the requirements for use of a <saml:Assertion> described in Section 2.3 apply also to an <xacml-saml:XACMLAssertion> when used as an Attribute Assertion. See Section 3.2 for a description of the syntax of an <xacml-saml:XACMLAssertion>.

2.5 Element <samlp:AttributeQuery>

The standard SAML <samlp:AttributeQuery> element MAY be used in an XACML system by a PEP or Context Handler to request SAML Attributes from an on-line Attribute Authority for use in an XACML Request Context. The definition and use of the <samlp:AttributeQuery> element SHALL be as described in the SAML 2.0 standard [SAML].

2.6 Element <samlp:Response>

The response to a <samlp:AttributeQuery> SHALL be either a <samlp:Response> instance or an <xacml-samlp:XACMLResponse> instance containing an Attribute Assertion that holds any <saml:AttributeStatement> instances that match the query. The definition and use of the <samlp:Response> element SHALL be as described in the SAML 2.0 standard, augmented with the following requirements. Except as specified here, this Profile imposes no requirements or restrictions on the <samlp:Response> element and its contents beyond those specified in SAML 2.0.

<samlp:Issuer> [Required]

This element SHALL be handled as specified in Section 2.3 for the <saml:Issuer> element in a <saml:Assertion>.

<ds:Signature> [Required]

This element SHALL be handled as specified in Section 2.3 for the <ds:Signature> in a <saml:Assertion>.

3 Authorization Decisions

XACML defines <xacml-context:Request> and <xacml-context:Response> elements for describing an authorization decision request and the corresponding response from a PDP. In many environments, these instances of these elements need to be signed or associated with a validity period in order to be used in an actual protocol between entities. SAML 2.0 defines a rudimentary <saml:AuthzDecisionQuery> in the SAML Protocol Schema and a rudimentary <saml:AuthzDecisionStatement> in the SAML Assertion Schema, but these elements are not able to convey all the information that an XACML PDP is capable of accepting as part of its Request Context. Likewise, the SAML <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 protocol with full support for the XACML Request Context and XACML Response Context syntax, this specification defines four SAML extension elements:

- <xacml-saml:XACMLAuthzDecisionStatement> allows a PDP Context Handler to include an XACML <xacml-context:Response>, along with other optional information, in a SAML Statement.
- <xacml-saml:XACMLAssertion> allows a PDP Context Handler to include an <xacml-saml:XACMLAuthzDecisionStatement> in a SAML Assertion.
- <xacml-samlp:XACMLAuthzDecisionQuery> allows a PEP to submit an XACML Request Context, along with other optional information, as a SAML protocol query.
- <xacml-samlp:XACMLResponse> allows a PDP to include <xacml-saml:XACMLAuthzDecisionStatement> instances in a SAML protocol response.

This Section defines these elements. All these elements are contained in the [XACML-SAML] and [XACML-SAMLP] schema documents.

3.1 Element <XACMLAuthzDecisionStatement>

The <xacml-saml:XACMLAuthzDecisionStatement> element MAY be used by an XACML PDP to hold an authorization decision that provides full support for XACML functionality. It allows a SAML Statement to contain an XACML Response Context along with related information. This element is an alternative to the SAML-defined <samlp:AuthzDecisionStatement>. This element SHALL be used as part of a response to an <xacml-samlp:XACMLAuthzDecisionQuery>. It MAY also be used in an <xacml-saml:XACMLAssertion> as a format for storage of an authorization decision in a Repository.

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

The <xacml-saml:XACMLAuthzDecisionStatement> element is of <xacml-saml:XACMLAuthzDecisionStatementType> complexType, which is an extension to the SAML-defined <saml:StatementAbstractType>.

The <xacml-saml:XACMLAuthzDecisionStatement> element contains the following elements:

<xacml-context:Response> [Required]

An XACML Response Context created by an XACML PDP. This Response MAY be the result of evaluating an XACML Request Context from <xacml-samlp:XACMLAuthzDecisionQuery>.

<xacml-context:Request> [Optional]

An <xacml-context:Request> element containing XACML Attributes that were used by the XACML PDP in evaluating policies to obtain the Response.

If the statement represents a response to an <xacml-samlp:XACMLAuthzDecisionQuery>, and if the ReturnContext XML attribute in the query is "true", then this element SHALL be included; if the ReturnContext XML attribute in the query is "false", then this element SHALL NOT be included. See the description of the ReturnContext XML attribute in Section 3.3 for a specification of the XACML Attribute values that SHALL be returned in this element when it is part of a response to an <xacml-samlp:XACMLAuthzDecisionQuery>.

If this statement does not represent the response to an <xacml-samlp:XACMLAuthzDecisionQuery>, then this element MAY be included. In this case, the PDP SHALL determine which XACML Attributes are included.

3.2 Element <XACMLAssertion>

The <xacml-saml:XACMLAssertion> element allows XACML or SAML Statements to be carried in a SAML Assertion, which MAY be signed. The <xacml-saml:XACMLAssertion> element MAY be used by a PDP, Policy Administration Authority, or Attribute Authority to hold <xacml-saml:XACMLAuthzDecisionStatement>, <xacml-saml:XACMLPolicyStatement>, or any of the standard SAML Statement instances, including <saml:AttributeStatement> instances.

```
<element name="XACMLAssertion"
    xsi:type="xacml-saml:XACMLAssertionType>
<complexType name="XACMLAssertionType">
    <complexContent>
        <extension base="saml:AssertionType">
            <choice minOccurs="0" maxOccurs=unbounded">
               <element
                   ref="xacml-saml:XACMLAdvice" maxOccurs="1" />
               <element
                   ref="xacml-saml:XACMLAuthzDecisionStatement"/>
               <element
                   ref="xacml-saml:XACMLPolicyStatement"/>
            </choice>
        </extension>
    </complexContent>
</complexType>
```

The <xacml-saml:XACMLAssertion> element is of <xacml-saml:XACMLAssertionType> complexType, which is an extension of the SAML-defined <saml:AssertionType>.

The specification of the components of a <saml:Assertion> in SAML 2.0 SHALL apply to an <xacml-saml:XACMLAssertion>. The additional requirements and restrictions on a <saml:Assertion> specified in Section 2.3 SHALL also apply to an <xacml-saml:XACMLAssertion>.

The following elements are defined or further specified here for use with the extended SAML statement types defined and used in this Profile. These elements are in addition to the elements and attributes defined for the <saml:AssertionType>:

<xacml-saml:XACMLAdvice> [Optional]

> "Additional information related to the assertion that assists processing in certain situations but which MAY be ignored by applications that do not understand the advice or do not wish to make use of it." [SAML] The <xacml-saml:XACMLAdvice> element allows the use of <xacml-saml:XACMLAssertion> instances as advice in assertions. See Section 5.1 for the definition of the <xacml-saml:XACMLAdvice> element.

<saml:Subject> [Optional]

> The <saml:Subject> element SHALL NOT be included in an assertion that contains an <xacml-saml:XACMLAuthzDecisionStatement>. Instead, the Subject of an <xacml-saml:XACMLAuthzDecision> is specified in the XACML Request Context of the corresponding authorization decision request. This corresponding XACML Request Context MAY be included in the <xacml-samlp:XACMLAuthzDecisionStatement> as described in Section 3.1.
>
> The <saml:Subject> element MAY be included in an assertion that contains an <xacml-saml:XACMLPolicyStatement> instance. There is usually not a unique Subject for an <xacml-saml:XACMLPolicyStatement>, as typically an XACML policy applies to multiple Subjects.

3.3 Element <XACMLAuthzDecisionQuery>

The <xacml-samlp:XACMLAuthzDecisionQuery> protocol element MAY be used by a PEP to request an authorization decision from an XACML PDP. This element is an alternative to the SAML-defined <samlp:AuthzDecisionQuery> and allows the PEP to use the full capabilities of an XACML

PDP. It allows the SAML query protocol to convey an XACML Request Context along with related information.

```
<element name="XACMLAuthzDecisionQuery"
    xsi:type="xacml-samlp:XACMLAuthzDecisionQueryType" />
<complexType name="XACMLAuthzDecisionQueryType">
    <complexContent>
        <extension base="samlp:RequestAbstractType">
            <sequence>
                <element ref="xacml-context:Request"/>
                <element ref="xacml:Policy
                    minOccurs="0" maxOccurs="unbounded" />
                <element ref="xacml:PolicySet
                    minOccurs="0" maxOccurs="unbounded" />
            </sequence>
            <attribute name="InputContextOnly"
                          type="boolean"
                          use="optional"
                       default="false"/>
             <attribute name="ReturnContext"
                          type="boolean"
                          use="optional"
                       default="false"/>
        </extension>
    </complexContent>
</complexType>
```

The <xacml-samlp:XACMLAuthzDecisionQuery> element is of <xacml-samlp:XACMLAuthzDecisionQueryType> complexType, which is an extension to the SAML-defined <samlp:RequestAbstractType>.

The <xacml-samlp:XACMLAuthzDecisionQuery> element contains the following XML attributes and elements in addition to those defined for the <saml:RequestAbstractType>:

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 <xacml-samlp: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 <xacml-samlp:XACMLAuthzDecisionQuery>.

ReturnContext [Default "false"]

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

If this XML attribute is "true", then the PDP SHALL include an <xacml-context:Request> instance in the <xacml-saml:XACMLAuthzDecisionStatement> in the <xacml-samlp:XACMLResponse> used in the response to the query. This <xacml-context:Request> instance SHALL include all those attributes supplied by the PEP in the <xacml-samlp:XACMLAuthzDecisionQuery> that were used in making the authorization decision. The PDP MAY include additional attributes in this <xacml-context:Request> instance, 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 authorization decision queries.

If this XML attribute is "`false`", then the PDP SHALL NOT include an `<xacml-context:Request>` instance in the `<xacml-saml:XACMLAuthzDecisionStatement>` contained in the `<xacml-samlp:XACMLResponse>` that is used in the query response.

`<xacml-context:Request>` [Required]

An XACML Request Context.

`<xacml:Policy>` [0 to Many]

Optional XACML Policy instances that MAY be used in evaluating this authorization decision request only. The PDP MAY choose to use such Policy instances. If used, the PDP SHALL determine the combining algorithm.

`<xacml:PolicySet>` [Any Number]

Optional XACML PolicySet instances that MAY be used in evaluating this authorization decision request only. The PDP MAY choose to use such PolicySet instances . If used, the PDP SHALL determine the combining algorithm.

3.4 Element <XACMLResponse>

The `<xacml-samlp:XACMLResponse>` element allows XACML Statements to be carried in a SAML response, which MAY be signed. An `<xacml-samlp:XACMLResponse>` instance SHALL be used when `<xacml-saml:XACMLAssertion>` instances are included in SAML protocol responses. The `<xacml-samlp:XACMLResponse>` element MAY be used to carry other SAML `<saml:Assertion>` instances, including those containing `<saml:AttributeStatement>` instances to be mapped to XACML Attributes.

```
<element name="XACMLResponse"
    xsi:type="xacml-samlp:XACMLResponseType>
<complexType name="XACMLResponseType">
    <complexContent>
        <extension base="samlp:ResponseType">
            <choice minOccurs="0" maxOccurs=unbounded">
               <element
                   ref="xacml-saml:XACMLAssertion"/>
           </choice>
        </extension>
    </complexContent>
</complexType>
```

The `<xacml-samlp:XACMLResponse>` element is of `<xacml-samlp:XACMLResponseType>` complexType, which is an extension of the SAML-defined `<samlp:ResponseType>`.

The specification of the components of a `<samlp:Response>` in SAML 2.0 SHALL apply to an `<xacml-samlp:XACMLResponse>`.

The following additional elements and requirements are specified here for use in responses to an `<xacml-samlp:XACMLAuthzDecisionQuery>`.

`<samlp:Issuer>` [Required]

This element SHALL be handled as specified in Section 2.3 for the <saml:Issuer> element in a <saml:Assertion>.

<ds:Signature> [Required]

This element SHALL be handled as specified in Section 2.3 for the <ds:Signature> in a <saml:Assertion>.

<xacml-saml:XACMLAssertion> [Any Number]

<xacml-saml:XACMLAssertion> instances containing SAML Statement or XACML extended Statement instances that represent the response to the associated query.

<samlp:StatusCode> [Required]

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

In the response to an <xacml-samlp:XACMLAuthzDecisionQuery>, the <samlp:StatusCode> Value XML attribute SHALL depend on the value of the <xacml-context:StatusCode> instance of the XACML Response Context <xacml-context:Status> instance 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-context: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-context:StatusCode> value is urn:oasis:names:tc:xacml:1.0:status:missing-attribute or the when the <xacml-context:StatusCode> value is urn:oasis:names:tc:xacml:1.0:status:syntax-error due to a syntax error in the <xacml-context: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-context: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 schema used in the query.

4 Policies

XACML defines two policy elements: <xacml:Policy> and <xacml:PolicySet>. These may need to be transmitted between entities in an XACML system, but SAML does not define any Protocol or Assertion elements for policies. In order to query for and make assertions about policies, this specification defines four SAML extension elements:

- <xacml-saml:XACMLPolicyStatement> allows one or more XACML policies to be included in a SAML statement.
- <xacml-saml:XACMLAssertion> allows an <xacml-saml:XACMLPolicyStatement> to be included in a SAML assertion.
- <xacml-samlp:XACMLPolicyQuery> allows a PDP or application to request XACML policies as a SAML protocol query.
- <xacml-samlp:XACMLResponse> allows an <xacml-saml:XACMLAssertion>, which may contain an <xacml-saml:XACMLPolicyStatement>, to be included in a SAML protocol response.

This Section defines these elements for use with XACML policies. All these elements are contained in the [XACML-SAML] and [XACML-SAMLP] schema documents.

4.1 Element <XACMLPolicyStatement>

The <xacml-saml:XACMLPolicyStatement> element MAY be used by a Policy Administration Point to hold one or more XACML policies. This element MAY be used as part of a response to an <xacml-samlp:XACMLPolicyQuery>. This element may also be used in a SAML Assertion as a format for storing an XACML policy in a Repository.

```
<element name="XACMLPolicyStatement"
    xsi:type="xacml-saml: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 <xacml-saml:XACMLPolicyStatement> element is of <xacml-saml:XACMLPolicyStatementType> complexType, which is an extension to the SAML-defined <saml:StatementAbstractType>.

An <xacml-saml:XACMLPolicyStatement> element contains the following elements.

<xacml:Policy> [Any Number]

If the statement represents a response to an <xacml-samlp:XACMLPolicyQuery>, then this element SHALL contain all <xacml:Policy> instances that meet the specifications of the associated <xacml-samlp:XACMLPolicyQuery>. Otherwise, this element MAY contain arbitrary <xacml:Policy> instances.

<xacml:PolicySet> [Any Number]

If the statement represents a response to an <xacml-samlp:XACMLPolicyQuery>, then this element SHALL contain all <xacml:PolicySet> instances that meet the specifications of the associated <xacml-samlp:XACMLPolicyQuery>. Otherwise, this element MAY contain arbitrary <xacml:PolicySet> instances.

If the <xacml-saml:XACMLPolicyStatement> is issued in response to an <xacml-samlp:XACMLPolicyQuery>, and there are no <xacml:Policy> or <xacml:PolicySet> instances that meet the specifications of the associated <xacml-samlp:XACMLPolicyQuery>, then there SHALL be exactly one empty <xacml-saml:XACMLPolicyStatement> included in the response.

4.2 Element <XACMLAssertion>

When an <xacml-saml:XACMLPolicyStatement> instance is stored or transmitted in an XACML system, the instance SHALL be enclosed in an <xacml-saml:XACMLAssertion> instance. When an <xacml-saml:XACMLAssertion> is part of a response to an <xacml-samlp:XACMLPolicyQuery>, then the <xacml-saml:XACMLAssertion> SHALL contain exactly one <xacml-saml:XACMLPolicyStatement>. The definition and use of the <xacml-saml:XACMLAssertion> element is described in Section 3.2.

4.3 Element <XACMLPolicyQuery>

The <xacml-samlp:XACMLPolicyQuery> element MAY be used by a PDP or application to request XACML <xacml:Policy> or <xacml:PolicySet> instances from an on-line Policy Administration Point.

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

The <xacml-samlp:XACMLPolicyQuery> element is of <xacml-samlp:XACMLPolicyQueryType> complexType, which is an extension to the SAML-defined <samlp:RequestAbstractType>.

The <xacml-samlp:XACMLPolicyQuery> element contains zero or more of the following elements in addition to those defined for the <samlp:RequestAbstractType>:

<xacml-context:Request> [Any Number]

Supplies an XACML Request Context. All XACML <xacml:Policy> and <xacml: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 <xacml:Target> instance. All XACML <xacml:Policy> and <xacml:PolicySet> instances applicable to this <Target> SHALL be returned.

<xacml:PolicySetIdReference> [Any Number]

Identifies an XACML <xacml:PolicySet> instance to be returned.

<xacml:PolicyIdReference> [Any Number]

Identifies an XACML <xacml:Policy> instance to be returned.

If the <xacml-samlp:XACMLPolicyQuery> contains no element instances, then the Policy Administration Point SHOULD return all policies that are authorized and appropriate for use by the requester.

4.4 Element <XACMLResponse>

The response to an <xacml-samlp:XACMLPolicyQuery> SHALL be an <xacml-samlp:Response> instance containing exactly one <xacml-saml:XACMLAssertion> instance that contains exactly one <xacml-saml:XACMLPolicyStatement> instance.

The specification of the components of a <saml:Response> in SAML 2.0 SHALL apply to an <xacml-samlp:XACMLResponse>. The following additional elements and requirements are specified here for use in responses to an <xacml-samlp:XACMLPolicyQuery>.

<samlp:Issuer> [Required]

This element SHALL be handled as specified in Section 2.3 for the <saml:Issuer> element in a <saml:Assertion>.

<ds:Signature> [Required]

This element SHALL be handled as specified in Section 2.3 for the <ds:Signature> in a <saml:Assertion>.

<xacml-saml:XACMLAssertion> [Any Number]

This element SHALL contain exactly one <xacml-saml:XACMLPolicyStatement> that represents the response to the associated query. It MAY contain other SAML or XACML Assertions.

5 Advice

This Section describes how to include <xacml-saml:XACMLAssertion> instances as advice to accompany any SAML Statement or XACML extended Statement.

5.1 Element <XACMLAdvice>

A SAML Assertion includes an optional <saml:Advice> element containing "Additional information related to the assertion that assists processing in certain situations but which MAY be ignored [without affecting either the semantics or the validity of the assertion] by applications that do not understand the advice or do not wish to make use of it." [SAML] The <xacml-saml:XACMLAdvice> element extends <saml:Advice> to allow the inclusion of <xacml-saml:XACMLAssertion> instances containing <xacml-saml:XACMLAuthzDecisionStatement> or <xacml-saml:XACMLPolicyStatement> instances.

```
<element name="XACMLAdvice"
    xsi:type="xacml-saml:XACMLAdviceType>
<complexType name="XACMLAdviceType">
    <complexContent>
        <extension base="saml:AdviceType">
            <choice minOccurs="0" maxOccurs=unbounded">
               <element
                   ref="xacml-saml:XACMLAssertion"/>
           </choice>
        </extension>
    </complexContent>
</complexType>
```

The <xacml-saml:XACMLAdvice> element is of <xacml-saml:XACMLAdviceType> complexType, which is an extension to the SAML-defined <saml:AdviceType>.

The <xacml-saml:XACMLAdvice> element contains the following elements in addition to those defined in the <saml:AdviceType>:

<xacml-saml:XACMLAssertion> [Any Number]

An assertion representing advice for the use of the outer assertion. It MAY contain any number of <xacml-saml:XACMLAuthzDecisionStatement> or <xacml-saml:XACMLPolicyStatement> instances.

5.2 Element <XACMLAssertion>

The <xacml-saml:XACMLAssertion> element includes an optional <xacml-saml:XACMLAdvice> element. Since the <xacml-saml:XACMLAssertion> extends the standard <saml:Assertion>, this means that not only <xacml-saml:XACMLAuthzDecisionStatement> and <xacml-saml:XACMLPolicyStatement> instances, but any instance of a SAML Statement, may be used in an <xacml-saml:XACMLAssertion>, and may be associated there with an <xacml-saml:XACMLAdvice> instance that includes an <xacml-saml:XACMLAssertion> to be used as advice for the outer <xacml-saml:XACMLAssertion>.

Appendix A. Acknowledgments

The following individuals have participated in the creation of this specification and are gratefully acknowledged

Participants:

- Anne Anderson, Sun Microsystems
- Anthony Nadalin, IBM
- Bill Parducci,
- Carlisle Adams, University of Ottawa
- Daniel Engovatov, BEA
- Don Flinn,
- Ed Coyne
- Ernesto Damiani
- Frank Siebenlist
- Gerald Brose
- Hal Lockhart
- Haruyuki Kawabe
- James MacLean
- John Merrells
- Ken Yagen
- Konstantin Beznosov
- Michiharu Kudo
- Michael McIntosh
- Pierangela Samarati
- Pirasenna Velandai Thiyagarajan
- Polar Humenn
- Rebekah Metz
- Ron Jacobson
- Satoshi Hada
- Sekhar Vajjhala
- Seth Proctor
- Simon Godik
- Steve Anderson
- Steve Crocker
- Suresh Damodaran
- Tim Moses
- Von Welch
- Frederic Deleon
- Argyn Kuketayev

Appendix B. Revision History

Rev	Date	By whom	What
WD 1	12 April 2006	Anne Anderson	Create from SAML Profile errata document. <XACMLAuthzDecisionStatementType>: replace “ReturnResponse” with “ReturnContext” in description. Authorization Decisions: replaced “in the Response to an <XACMLAuthzDecisionStatement>” with “...<XACMLAuthzDecisionQuery>”. Create new types for SAML elements that will need to include XACML extensions. Create new elements for each extended type. Allow an XACMLAuthzDecisionQuery to include XACML policies for use in evaluating that query. Allow an XACMLAssertion to contain an XACMLAdvice element that in turn can contain an XACMLAssertion.