Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML)

OASIS Standard, 5 November 2002

Document identifier:
oasis-sstc-saml-core-1.0 (PDF, Word)

Location:
http://www.oasis-open.org/committees/security/docs/

Editors:
Phillip Hallam-Baker, VeriSign (pbaker@verisign.com)
Eve Maler, Sun Microsystems (eve.maler@sun.com)

Contributors:
Stephen Farrell, Baltimore Technologies
Irving Reid, Baltimore Technologies
David Orchard, BEA Systems
Krishna Sankar, Cisco Systems
Simon Godik, Crosslogix
Hal Lockhart, Entegrity
Carlisle Adams, Entrust
Tim Moses, Entrust
Nigel Edwards, Hewlett-Packard
Joe Pato, Hewlett-Packard
Marc Chanliau, Netegrity
Chris McLaren, Netegrity
Prateek Mishra, Netegrity
Charles Knouse, Oblix
Scott Cantor, Ohio State University
Darren Platt, formerly with RSA Security
Jeff Hodges, Sun Microsystems
Bob Blakley Tivoli
Marlena Erdos, Tivoli
RL “Bob” Morgan, University of Washington

Abstract:
This specification defines the syntax and semantics for XML-encoded assertions about authentication, attributes and authorization, and for the protocol that conveys this information.

Status:

This is an OASIS Standard document that was approved by the OASIS membership on 5 November 2002.

If you are on the security-services@lists.oasis-open.org list for committee members, send comments there. If you are not on that list, subscribe to the security-services-comment@lists.oasis-open.org list and send comments there. To subscribe, send an email message to security-services-comment-request@lists.oasis-open.org with the word "subscribe" as the body of the message.

This document has not changed substantively since its Committee Specification stage. Changes from cs-sstc-core-00 are noted in the errata document, draft-sstc-cs-errata-04.

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 Security Services TC web page (http://www.oasis-open.org/committees/security/).

Table of Contents

152

1 Introduction

This specification defines the syntax and semantics for XML-encoded SAML assertions, protocol requests, and protocol responses. These constructs are typically embedded in other structures for transport, such as HTTP form POSTs and XML-encoded SOAP messages. The SAML specification for bindings and profiles **[SAMLBind]** provides frameworks for this embedding and transport. Files containing just the SAML assertion schema **[SAML-XSD]** and protocol schema **[SAMLP-XSD]** are available.

The following sections describe how to understand the rest of this specification.

1.1 Notation

This specification uses schema documents conforming to W3C XML Schema **[Schema1]** and normative text to describe the syntax and semantics of XML-encoded SAML assertions and protocol messages.

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 **[RFC 2119]**:

> *"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.

```
Listings of SAML schemas appear like this.
```

```
Example code listings appear like this.
```

In cases of disagreement between the SAML schema files **[SAML-XSD] [SAMLP-XSD]** and this specification, the schema files take precedence.

Conventional XML namespace prefixes are used throughout the listings in this specification to stand for their respective namespaces (see Section 1.2) as follows, whether or not a namespace declaration is present in the example:

- The prefix `saml:` stands for the SAML assertion namespace.
- The prefix `samlp:` stands for the SAML request-response protocol namespace.
- The prefix `ds:` stands for the W3C XML Signature namespace.
- The prefix `xsd:` stands for the W3C XML Schema namespace in example listings. In schema listings, this is the default namespace and no prefix is shown.

This specification uses the following typographical conventions in text: `<SAMLElement>`, `<ns:ForeignElement>`, `Attribute`, **Datatype**, `OtherCode`.

1.2 Schema Organization and Namespaces

The SAML assertion structures are defined in a schema **[SAML-XSD]** associated with the following XML namespace:

```
urn:oasis:names:tc:SAML:1.0:assertion
```

The SAML request-response protocol structures are defined in a schema **[SAMLP-XSD]** associated with the following XML namespace:

```
urn:oasis:names:tc:SAML:1.0:protocol
```

Note: The SAML namespace names may change when SAML 1.0 becomes an OASIS Standard.

The assertion schema is imported into the protocol schema. Also imported into both schemas is the schema for XML Signature **[XMLSig-XSD]**, which is associated with the following XML namespace:

```
http://www.w3.org/2000/09/xmldsig#
```

1.2.1 String and URI Values

All SAML string and URI values have the types string and anyURI respectively, which are built in to the W3C XML Schema Datatypes specification. All strings in SAML messages MUST consist of at least one non-whitespace character (whitespace is defined in the XML Recommendation **[XML]** §2.3). Empty and whitespace-only values are disallowed. Also, unless otherwise indicated in this specification, all URI values MUST consist of at least one non-whitespace character.

1.2.2 Time Values

All SAML time values have the type **dateTime**, which is built in to the W3C XML Schema Datatypes specification **[Schema2]** and MUST be expressed in UTC form.

SAML Requestors and Responders SHOULD NOT rely on other applications supporting time resolution finer than milliseconds. Implementations MUST NOT generate time instants that specify leap seconds.

1.2.3 Comparing SAML Values

Unless otherwise noted, all elements in SAML documents that have the XML Schema "string" type, or a type derived from that, MUST be compared using an exact binary comparison. In particular, SAML implementations and deployments MUST NOT depend on case-insensitive string comparisons, normalization or trimming of white space, or conversion of locale-specific formats such as numbers or currency. This requirement is intended to conform to the W3C Requirements for String Identity, Matching, and String Indexing **[W3C-CHAR]**.

If an implementation is comparing values that are represented using different character encodings, the implementation MUST use a comparison method that returns the same result as converting both values to the Unicode character encoding (http://www.unicode.org), Normalization Form C **[UNICODE-C]** and then performing an exact binary comparison. This requirement is intended to conform to the W3C Character Model for the World Wide Web **[W3C-CharMod]**, and in particular the rules for Unicode-normalized Text.

Applications that compare data received in SAML documents to data from external sources MUST take into account the normalization rules specified for XML. Text contained within elements is normalized so that line endings are represented using linefeed characters (ASCII code $10_{Decimal}$), as described in the XML Recommendation **[XML]** §2.11. Attribute values defined as strings (or types derived from strings) are normalized as described in **[XML]** §3.3.3. All white space characters are replaced with blanks (ASCII code $32_{Decimal}$).

The SAML specification does not define collation or sorting order for attribute or element values. SAML implementations MUST NOT depend on specific sorting orders for values, because these may differ depending on the locale settings of the hosts involved.

1.3 SAML Concepts (Non-Normative)

This section is informative only and is superseded by any contradicting information in the normative text in Section 2 and following. A glossary of SAML terms and concepts **[SAMLGloss]** is available.

1.3.1 Overview

The Security Assertion Markup Language (SAML) is an XML-based framework for exchanging security information. This security information is expressed in the form of assertions about subjects, where a

subject is an entity (either human or computer) that has an identity in some security domain. A typical example of a subject is a person, identified by his or her email address in a particular Internet DNS domain.

Assertions can convey information about authentication acts performed by subjects, attributes of subjects, and authorization decisions about whether subjects are allowed to access certain resources. Assertions are represented as XML constructs and have a nested structure, whereby a single assertion might contain several different internal statements about authentication, authorization, and attributes. Note that assertions containing authentication statements merely describe acts of authentication that happened previously.

Assertions are issued by SAML authorities, namely, authentication authorities, attribute authorities, and policy decision points. SAML defines a protocol by which clients can request assertions from SAML authorities and get a response from them. This protocol, consisting of XML-based request and response message formats, can be bound to many different underlying communications and transport protocols; SAML currently defines one binding, to SOAP over HTTP.

SAML authorities can use various sources of information, such as external policy stores and assertions that were received as input in requests, in creating their responses. Thus, while clients always consume assertions, SAML authorities can be both producers and consumers of assertions.

The following model is conceptual only; for example, it does not account for real-world information flow or the possibility of combining of authorities into a single system.

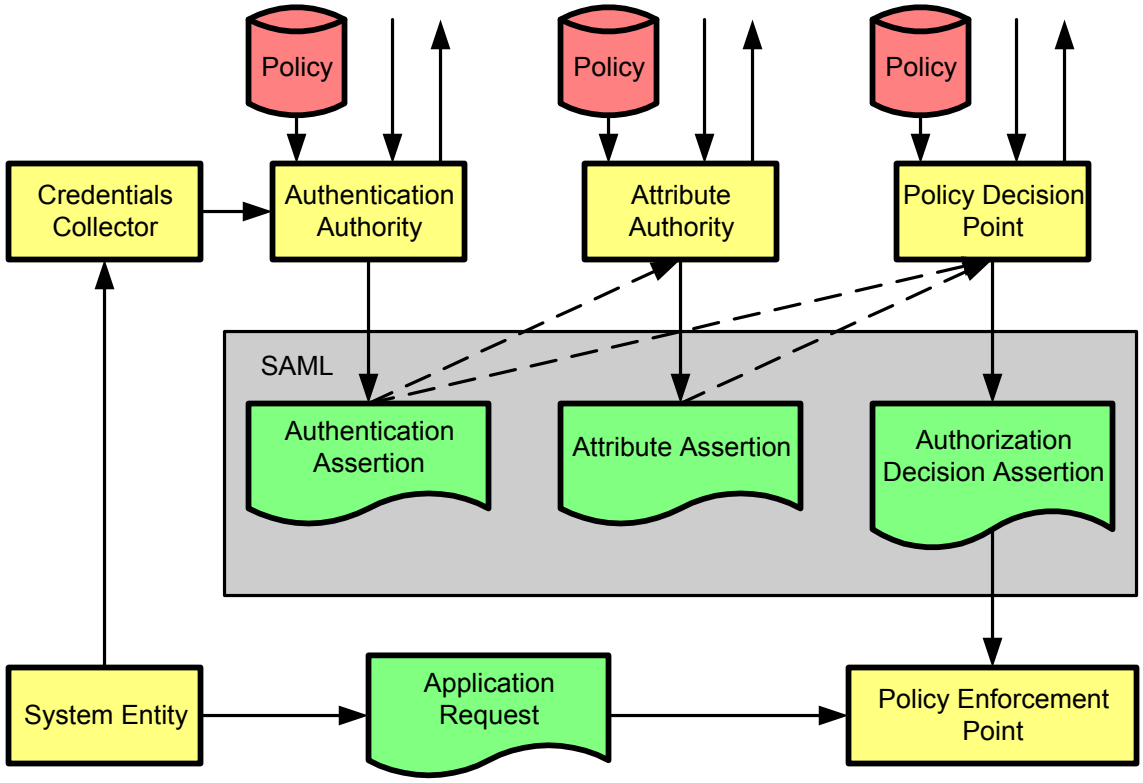

Figure 1 The SAML Domain Model

One major design goal for SAML is Single Sign-On (SSO), the ability of a user to authenticate in one domain and use resources in other domains without re-authenticating. However, SAML can be used in various configurations to support additional scenarios as well. Several profiles of SAML are currently being defined that support different styles of SSO and the securing of SOAP payloads.

The assertion and protocol data formats are defined in this specification. The bindings and profiles are defined in a separate specification **[SAMLBind]**. A conformance program for SAML is defined in the

conformance specification **[SAMLConform]**. Security issues are discussed in a separate security and privacy considerations specification **[SAMLSecure]**.

1.3.2 SAML and URI-Based Identifiers

SAML defines some identifiers to manage references to well-known concepts and sets of values. For example, the SAML-defined identifier for the password authentication method is as follows:

```
urn:oasis:names:tc:SAML:1.0:am:password
```

For another example, the SAML-defined identifier for the set of possible actions on a resource consisting of Read/Write/Execute/Delete/Control is as follows:

```
urn:oasis:names:tc:SAML:1.0:action:rwedc
```

These identifiers are defined as Uniform Resource Identifiers (URIs), but they are not necessarily able to be resolved to some Web resource. At times SAML authorities need to use identifier strings of their own design, for example, for assertion IDs or additional kinds of authentication methods not covered by SAML-defined identifiers. In these cases, using a URI form is not required; if it is used, it is not required to be resolvable to some Web resource. However, using URIs – particularly URLs based on the `http:` scheme – is likely to mitigate problems with clashing identifiers to some extent.

The Read/Write/Execute/Delete/Control identifier above is an example of a namespace (not in the sense of an XML namespace). SAML uses this namespace mechanism to manage the universe of possible types of actions and possible names of attributes.

See Section 7 for a list of SAML-defined identifiers.

1.3.3 SAML and Extensibility

The XML formats for SAML assertions and protocol messages have been designed to be extensible.

However, it is possible that the use of extensions will harm interoperability and therefore the use of extensions SHOULD be carefully considered.

2 SAML Assertions

An assertion is a package of information that supplies one or more statements made by an issuer. SAML allows issuers to make three different kinds of assertion statement:

- **Authentication:** The specified subject was authenticated by a particular means at a particular time.
- **Authorization Decision:** A request to allow the specified subject to access the specified resource has been granted or denied.
- **Attribute:** The specified subject is associated with the supplied attributes.

Assertions have a nested structure. A series of inner elements representing authentication statements, authorization decision statements, and attribute statements contain the specifics, while an outer generic assertion element provides information that is common to all of the statements.

2.1 Schema Header and Namespace Declarations

The following schema fragment defines the XML namespaces and other header information for the assertion schema:

```
<schema
   targetNamespace="urn:oasis:names:tc:SAML:1.0:assertion"
   xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
   xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
   xmlns="http://www.w3.org/2001/XMLSchema"
   elementFormDefault="unqualified">
   <import namespace="http://www.w3.org/2000/09/xmldsig#"
   schemaLocation="http://www.w3.org/TR/xmldsig-core/xmldsig-core-
schema.xsd"/>
   <annotation>
          <documentation>
                Document identifier: cs-sstc-schema-assertion-01
                Location: http://www.oasis-open.org/committees/security/docs/
          </documentation>
   </annotation>
…
</schema>
```

2.2 Simple Types

The following sections define the SAML assertion-related simple types.

2.2.1 Simple Types IDType and IDReferenceType

The **IDType** simple type is used to declare identifiers to assertions, requests, and responses. The **IDReferenceType** is used to reference identifiers of type **IDType**.

Values declared to be of type **IDType** MUST satisfy the following properties:

- Any party that assigns an identifier MUST ensure that there is negligible probability that that party or any other party will accidentally assign the same identifier to a different data object.
- Where a data object declares that it has a particular identifier, there MUST be exactly one such declaration.

The mechanism by which the SAML Requestor or Responder ensures that the identifier is unique is left to the implementation. In the case that a pseudorandom technique is employed, the probability of two randomly chosen identifiers being identical MUST be less than 2^{-128} and SHOULD be less than 2^{-160}. This

requirement MAY be met by applying Base64 encoding to a randomly chosen value 128 or 160 bits in length.

It is OPTIONAL for an identifier based on **IDType** to be resolvable in principle to some resource. In the case that the identifier is resolvable in principle (for example, the identifier is in the form of a URI reference), it is OPTIONAL for the identifier to be dereferenceable.

The following schema fragment defines the **IDType** and **IDReferenceType** simple types:

```
<simpleType name="IDType">
   <restriction base="string"/>
</simpleType>
<simpleType name="IDReferenceType">
   <restriction base="string"/>
</simpleType>
```

2.2.2 Simple Type DecisionType

The **DecisionType** simple type defines the possible values to be reported as the status of an authorization decision statement.

`Permit`

The specified action is permitted.

`Deny`

The specified action is denied.

`Indeterminate`

The issuer cannot determine whether the specified action is permitted or denied.

The `Indeterminate` decision value is used in situations where the issuer requires the ability to provide an affirmative statement that it is not able to issue a decision. Additional information as to the reason for the refusal or inability to provide a decision MAY be returned as <StatusDetail> elements.

The following schema fragment defines the **DecisionType** simple type:

```
<simpleType name="DecisionType">
   <restriction base="string">
          <enumeration value="Permit"/>
          <enumeration value="Deny"/>
          <enumeration value="Indeterminate"/>
   </restriction>
</simpleType>
```

2.3 Assertions

The following sections define the SAML constructs that contain assertion information.

2.3.1 Element <AssertionIDReference>

The `<AssertionIDReference>` element makes a reference to a SAML assertion.

The following schema fragment defines the `<AssertionIDReference>` element:

```
<element name="AssertionIDReference" type="saml:IDReferenceType"/>
```

2.3.2 Element <Assertion>

The `<Assertion>` element is of **AssertionType** complex type. This type specifies the basic information that is common to all assertions, including the following elements and attributes:

373 `MajorVersion` [Required]

374 The major version of this assertion. The identifier for the version of SAML defined in this specification
375 is `1`. Processing of this attribute is specified in Section 3.4.4.

376 `MinorVersion` [Required]

377 The minor version of this assertion. The identifier for the version of SAML defined in this specification
378 is `0`. Processing of this attribute is specified in Section 3.4.4.

379 `AssertionID` [Required]

380 The identifier for this assertion. It is of type **IDType**, and MUST follow the requirements specified by
381 that type for identifier uniqueness.

382 `Issuer` [Required]

383 The issuer of the assertion. The name of the issuer is provided as a string. The issuer name
384 SHOULD be unambiguous to the intended relying parties. SAML authorities may use an identifier
385 such as a URI reference that is designed to be unambiguous regardless of context.

386 `IssueInstant` [Required]

387 The time instant of issue in UTC as described in Section 1.2.2.

388 `<Conditions>` [Optional]

389 Conditions that MUST be taken into account in assessing the validity of the assertion.

390 `<Advice>` [Optional]

391 Additional information related to the assertion that assists processing in certain situations but which
392 MAY be ignored by applications that do not support its use.

393 `<ds:Signature>` [Optional]

394 An XML Signature that authenticates the assertion, see Section 5.

395 One or more of the following statement elements:

396 `<Statement>`

397 A statement defined in an extension schema.

398 `<SubjectStatement>`

399 A subject statement defined in an extension schema.

400 `<AuthenticationStatement>`

401 An authentication statement.

402 `<AuthorizationDecisionStatement>`

403 An authorization decision statement.

404 `<AttributeStatement>`

405 An attribute statement.

406 The following schema fragment defines the `<Assertion>` element and its **AssertionType** complex type:

```
407 <element name="Assertion" type="saml:AssertionType"/>
408 <complexType name="AssertionType">
409    <sequence>
410           <element ref="saml:Conditions" minOccurs="0"/>
411           <element ref="saml:Advice" minOccurs="0"/>
412           <choice maxOccurs="unbounded">
413                 <element ref="saml:Statement"/>
414                 <element ref="saml:SubjectStatement"/>
415                 <element ref="saml:AuthenticationStatement"/>
416                 <element ref="saml:AuthorizationDecisionStatement"/>
417                 <element ref="saml:AttributeStatement"/>
418           </choice>
419           <element ref="ds:Signature" minOccurs="0"/>
```

```
   </sequence>
   <attribute name="MajorVersion" type="integer" use="required"/>
   <attribute name="MinorVersion" type="integer" use="required"/>
   <attribute name="AssertionID" type="saml:IDType" use="required"/>
   <attribute name="Issuer" type="string" use="required"/>
   <attribute name="IssueInstant" type="dateTime" use="required"/>
</complexType>
```

2.3.2.1 Element <Conditions>

The <Conditions> element MAY contain the following elements and attributes:

NotBefore [Optional]

Specifies the earliest time instant at which the assertion is valid. The time value is encoded in UTC as described in Section 1.2.2.

NotOnOrAfter [Optional]

Specifies the time instant at which the assertion has expired. The time value is encoded in UTC as described in Section 1.2.2.

<Condition> [Any Number]

Provides an extension point allowing extension schemas to define new conditions.

<AudienceRestrictionCondition> [Any Number]

Specifies that the assertion is addressed to a particular audience.

The following schema fragment defines the <Conditions> element and its **ConditionsType** complex type:

```
<element name="Conditions" type="saml:ConditionsType"/>
<complexType name="ConditionsType">
   <choice minOccurs="0" maxOccurs="unbounded">
          <element ref="saml:AudienceRestrictionCondition"/>
          <element ref="saml:Condition"/>
   </choice>
   <attribute name="NotBefore" type="dateTime" use="optional"/>
   <attribute name="NotOnOrAfter" type="dateTime" use="optional"/>
</complexType>
```

If an assertion contains a <Conditions> element, the validity of the assertion is dependent on the sub-elements and attributes provided. When processing the sub-elements and attributes of a <Conditions> element, the following rules MUST be used in the order shown to determine the overall validity of the assertion:

1. If no sub-elements or attributes are supplied in the <Conditions> element, then the assertion is considered to be **Valid**.
2. If any sub-element or attribute of the <Conditions> element is determined to be invalid, then the assertion is **Invalid**.
3. If any sub-element or attribute of the <Conditions> element cannot be evaluated, then the validity of the assertion cannot be determined and is deemed to be **Indeterminate**.
4. If all sub-elements and attributes of the <Conditions> element are determined to be **Valid**, then the assertion is considered to be **Valid**.

The <Conditions> element MAY be extended to contain additional conditions. If an element contained within a <Conditions> element is encountered that is not understood, the status of the condition cannot be evaluated and the validity status of the assertion MUST be deemed to be **Indeterminate** in accordance with rule 3 above.

Note that an assertion that has validity status **Valid** may not be trustworthy by reasons such as not being issued by a trustworthy issuer or not being authenticated by a trustworthy means.

2.3.2.1.1 Attributes NotBefore and NotOnOrAfter

The `NotBefore` and `NotOnOrAfter` attributes specify time limits on the validity of the assertion.

The `NotBefore` attribute specifies the time instant at which the validity interval begins. The `NotOnOrAfter` attribute specifies the time instant at which the validity interval has ended.

If the value for either `NotBefore` or `NotOnOrAfter` is omitted it is considered unspecified. If the `NotBefore` attribute is unspecified (and if any other conditions that are supplied evaluate to `Valid`), the assertion is valid at any time before the time instant specified by the `NotOnOrAfter` attribute. If the `NotOnOrAfter` attribute is unspecified (and if any other conditions that are supplied evaluate to `Valid`), the assertion is valid from the time instant specified by the `NotBefore` attribute with no expiry. If neither attribute is specified (and if any other conditions that are supplied evaluate to `Valid`), the assertion is valid at any time.

The `NotBefore` and `NotOnOrAfter` attributes are defined to have the **dateTime** simple type that is built in to the W3C XML Schema Datatypes specification **[Schema2]**. All time instants are specified in Universal Coordinated Time (UTC) as described in Section 1.2.2. Implementations MUST NOT generate time instants that specify leap seconds.

2.3.2.1.2 Element <Condition>

The `<Condition>` element serves as an extension point for new conditions. Its **ConditionAbstractType** complex type is abstract; extension elements MUST use the `xsi:type` attribute to indicate the derived type.

The following schema fragment defines the `<Condition>` element and its **ConditionAbstractType** complex type:

```
<element name="Condition" type="saml:ConditionAbstractType"/>
<complexType name="ConditionAbstractType" abstract="true"/>
```

2.3.2.1.3 Elements <AudienceRestrictionCondition> and <Audience>

The `<AudienceRestrictionCondition>` element specifies that the assertion is addressed to one or more specific audiences identified by `<Audience>` elements. Although a party that is outside the audiences specified is capable of drawing conclusions from an assertion, the issuer explicitly makes no representation as to accuracy or trustworthiness to such a party. It contains the following elements:

`<Audience>`

A URI reference that identifies an intended audience. The URI reference MAY identify a document that describes the terms and conditions of audience membership.

The `AudienceRestrictionCondition` evaluates to `Valid` if and only if the relying party is a member of one or more of the audiences specified.

The issuer of an assertion cannot prevent a party to whom it is disclosed from making a decision on the basis of the information provided. However, the `<AudienceRestrictionCondition>` element allows the issuer to state explicitly that no warranty is provided to such a party in a machine- and human-readable form. While there can be no guarantee that a court would uphold such a warranty exclusion in every circumstance, the probability of upholding the warranty exclusion is considerably improved.

The following schema fragment defines the `<AudienceRestrictionCondition>` element and its **AudienceRestrictionConditionType** complex type:

```
<element name="AudienceRestrictionCondition"
   type="saml:AudienceRestrictionConditionType"/>
<complexType name="AudienceRestrictionConditionType">
```

```
   <complexContent>
         <extension base="saml:ConditionAbstractType">
               <sequence>
                     <element ref="saml:Audience" maxOccurs="unbounded"/>
               </sequence>
         </extension>
   </complexContent>
</complexType>
<element name="Audience" type="anyURI"/>
```

2.3.2.2 Element <Advice>

The <Advice> element contains any additional information that the issuer wishes to provide. This information MAY be ignored by applications without affecting either the semantics or the validity of the assertion.

The <Advice> element contains a mixture of zero or more <Assertion> elements, <AssertionIDReference> elements and elements in other namespaces, with lax schema validation in effect for these other elements.

Following are some potential uses of the <Advice> element:

- Include evidence supporting the assertion claims to be cited, either directly (through incorporating the claims) or indirectly (by reference to the supporting assertions).
- State a proof of the assertion claims.
- Specify the timing and distribution points for updates to the assertion.

The following schema fragment defines the <Advice> element and its **AdviceType** complex type:

```
<element name="Advice" type="saml:AdviceType"/>
<complexType name="AdviceType">
   <choice minOccurs="0" maxOccurs="unbounded">
         <element ref="saml:AssertionIDReference"/>
         <element ref="saml:Assertion"/>
         <any namespace="##other" processContents="lax"/>
   </choice>
</complexType>
```

2.4 Statements

The following sections define the SAML constructs that contain statement information.

2.4.1 Element <Statement>

The <Statement> element is an extension point that allows other assertion-based applications to reuse the SAML assertion framework. Its **StatementAbstractType** complex type is abstract; extension elements MUST use the xsi:type attribute to indicate the derived type.

The following schema fragment defines the <Statement> element and its **StatementAbstractType** complex type:

```
<element name="Statement" type="saml:StatementAbstractType"/>
<complexType name="StatementAbstractType" abstract="true"/>
```

2.4.2 Element <SubjectStatement>

The <SubjectStatement> element is an extension point that allows other assertion-based applications to reuse the SAML assertion framework. It contains a <Subject> element that allows an issuer to describe a subject. Its **SubjectStatementAbstractType** complex type, which extends

StatementAbstractType, is abstract; extension elements MUST use the `xsi:type` attribute to indicate the derived type.

The following schema fragment defines the `<SubjectStatement>` element and its **SubjectStatementAbstractType** abstract type:

```
<element name="SubjectStatement" type="saml:SubjectStatementAbstractType"/>
<complexType name="SubjectStatementAbstractType" abstract="true">
   <complexContent>
          <extension base="saml:StatementAbstractType">
                <sequence>
                      <element ref="saml:Subject"/>
                </sequence>
          </extension>
   </complexContent>
</complexType>
```

2.4.2.1 Element <Subject>

The `<Subject>` element specifies the principal that is the subject of the statement. It contains either or both of the following elements:

`<NameIdentifier>`

An identification of a subject by its name and security domain.

`<SubjectConfirmation>`

Information that allows the subject to be authenticated.

If the `<Subject>` element contains both a `<NameIdentifier>` and a `<SubjectConfirmation>`, the issuer is asserting that if the relying party performs the specified `<SubjectConfirmation>`, it can be confident that the entity presenting the assertion to the relying party is the entity that the issuer associates with the `<NameIdentifier>`. A `<Subject>` element SHOULD NOT identify more than one principal.

The following schema fragment defines the `<Subject>` element and its **SubjectType** complex type:

```
<element name="Subject" type="saml:SubjectType"/>
<complexType name="SubjectType">
   <choice>
          <sequence>
                <element ref="saml:NameIdentifier"/>
                <element ref="saml:SubjectConfirmation" minOccurs="0"/>
          </sequence>
          <element ref="saml:SubjectConfirmation"/>
   </choice>
</complexType>
```

2.4.2.2 Element <NameIdentifier>

The <NameIdentifier> element specifies a subject by a combination of a name qualifier, a name and a format. It has the following attributes:

`NameQualifier` [Optional]

The security or administrative domain that qualifies the name of the subject. The NameQualifier attribute provides a means to federate names from disparate user stores without collision.

`Format` [Optional]

The syntax used to describe the name of the subject.

The format value MUST be a URI reference. The following URI references are defined by this specification, where only the fragment identifier portion is shown, assuming a base URI of the SAML assertion namespace name.

#emailAddress

Indicates that the content of the NameIdentifier element is in the form of an email address, specifically "addr-spec" as defined in IETF RFC 2822 **[RFC 2822]** §3.4.1. An addr-spec has the form local-part@domain. Note that an addr-spec has no phrase (such as a common name) before it, has no comment (text surrounded in parentheses) after it, and is not surrounded by "<" and ">".

#X509SubjectName

Indicates that the content of the NameIdentifier element is in the form specified for the contents of <ds:X509SubjectName> element in the XML Signature Recommendation **[XMLSig]**. Implementors should note that the XML Signature specification specifies encoding rules for X.509 subject names that differ from the rules given in IETF RFC 2253 **[RFC 2253]**.

#WindowsDomainQualifiedName

Indicates that the content of the NameIdentifier element is a Windows domain qualified name. A Windows domain qualified user name is a string of the form "DomainName\UserName". The domain name and "\" separator may be omitted.

The following schema fragment defines the <NameIdentifier> element and its **NameIdentifierType** complex type:

```
<element name="NameIdentifier" type="saml:NameIdentifierType"/>
<complexType name="NameIdentifierType">
  <simpleContent>
        <extension base="string">
              <attribute name="NameQualifier" type="string" use="optional"/>
              <attribute name="Format" type="anyURI" use="optional"/>
        </extension>
  </simpleContent>
</complexType>
```

The interpretation of the NameQualifier, and NameIdentifier's content in the case of a Format not specified in this document, are left to individual implementations.

Regardless of format, issues of anonymity, pseudonymity, and the persistence of the identifier with respect to the asserting and relying parties, are also implementation-specific.

2.4.2.3 Elements <SubjectConfirmation>, <ConfirmationMethod>, and <SubjectConfirmationData>

The <SubjectConfirmation> element specifies a subject by supplying data that allows the subject to be authenticated. It contains the following elements in order:

<ConfirmationMethod> [One or more]

A URI reference that identifies a protocol to be used to authenticate the subject. URI references identifying SAML-defined confirmation methods are currently defined with the SAML profiles in the SAML Binding and Profiles specification **[SAMLBind]**. Additional methods may be added by defining new profiles or by private agreement.

<SubjectConfirmationData> [Optional]

Additional authentication information to be used by a specific authentication protocol.

<ds:KeyInfo> [Optional]

An XML Signature **[XMLSig]** element that specifies a cryptographic key held by the subject.

The following schema fragment defines the <SubjectConfirmation> element and its **SubjectConfirmationType** complex type, along with the <SubjectConfirmationData> element and the <ConfirmationMethod> element:

```
<element name="SubjectConfirmation" type="saml:SubjectConfirmationType"/>
<complexType name="SubjectConfirmationType">
```

```
   <sequence>
          <element ref="saml:ConfirmationMethod" maxOccurs="unbounded"/>
          <element ref="saml:SubjectConfirmationData" minOccurs="0"/>
          <element ref="ds:KeyInfo" minOccurs="0"/>
   </sequence>
</complexType>
<element name="SubjectConfirmationData" type="anyType"/>
<element name="ConfirmationMethod" type="anyURI"/>
```

2.4.3 Element <AuthenticationStatement>

The `<AuthenticationStatement>` element supplies a statement by the issuer that its subject was authenticated by a particular means at a particular time. It is of type **AuthenticationStatementType**, which extends **SubjectStatementAbstractType** with the addition of the following element and attributes:

`AuthenticationMethod` [Required]

A URI reference that specifies the type of authentication that took place. URI references identifying common authentication protocols are listed in Section 7.

`AuthenticationInstant` [Required]

Specifies the time at which the authentication took place. The time value is encoded in UTC as described in Section 1.2.2.

`<SubjectLocality>` [Optional]

Specifies the DNS domain name and IP address for the system entity from which the Subject was apparently authenticated.

`<AuthorityBinding>` [Any Number]

Indicates that additional information about the subject of the statement may be available.

The following schema fragment defines the `<AuthenticationStatement>` element and its **AuthenticationStatementType** complex type:

```
<element name="AuthenticationStatement"
                type="saml:AuthenticationStatementType"/>
<complexType name="AuthenticationStatementType">
   <complexContent>
          <extension base="saml:SubjectStatementAbstractType">
                <sequence>
                      <element ref="saml:SubjectLocality" minOccurs="0"/>
                      <element ref="saml:AuthorityBinding"
                               minOccurs="0" maxOccurs="unbounded"/>
                </sequence>
                <attribute name="AuthenticationMethod" type="anyURI"
use=”required”/>
                <attribute name="AuthenticationInstant" type="dateTime"
use=”required”/>
          </extension>
   </complexContent>
</complexType>
```

2.4.3.1 Element <SubjectLocality>

The `<SubjectLocality>` element specifies the DNS domain name and IP address for the system entity that was authenticated. It has the following attributes:

`IPAddress` [Optional]

The IP address of the system entity that was authenticated.

`DNSAddress` [Optional]

The DNS address of the system entity that was authenticated.

This element is entirely advisory, since both these fields are quite easily “spoofed,” but current practice appears to require its inclusion.

The following schema fragment defines the `<SubjectLocality>` element and its **SubjectLocalityType** complex type:

```
<element name="SubjectLocality"
                type="saml: SubjectLocalityType"/>
<complexType name="SubjectLocalityType">
   <attribute name="IPAddress" type="string" use="optional"/>
   <attribute name="DNSAddress" type="string" use="optional"/>
</complexType>
```

2.4.3.2 Element <AuthorityBinding>

The `<AuthorityBinding>` element may be used to indicate to a relying party receiving an AuthenticationStatement that a SAML authority may be available to provide additional information about the subject of the statement. A single SAML authority may advertise its presence over multiple protocol bindings, at multiple locations, and as more than one kind of authority by sending multiple elements as needed.

AuthorityKind [Required]

The type of SAML Protocol queries to which the authority described by this element will respond. The value is specified as an XML Schema QName. The acceptable values for `AuthorityKind` are the namespace-qualified names of element types or elements derived from the SAML Protocol Query element (see Section 3.3). For example, an attribute authority would be identified by `AuthorityKind="samlp:AttributeQuery"`. For extension schemas, where the actual type of the `<samlp:Query>` would be identified by an `xsi:type` attribute, the value of `AuthorityKind` MUST be the same as the value of the `xsi:type` attribute for the corresponding query.

`Location` [Required]

A URI reference describing how to locate and communicate with the authority, the exact syntax of which depends on the protocol binding in use. For example, a binding based on HTTP will be a web URL, while a binding based on SMTP might use the "mailto" scheme.

`Binding` [Required]

A URI reference identifying the SAML protocol binding to use in communicating with the authority. All SAML protocol bindings will have an assigned URI reference.

The following schema fragment defines the `<AuthorityBinding>` element and its **AuthorityBindingType** complex type:

```
<element name="AuthorityBinding" type="saml:AuthorityBindingType"/>
<complexType name="AuthorityBindingType">
   <attribute name="AuthorityKind" type="QName" use="required"/>
   <attribute name="Location" type="anyURI" use="required"/>
   <attribute name="Binding" type="anyURI" use="required"/>
</complexType>
```

2.4.4 Element <AuthorizationDecisionStatement>

The `<AuthorizationDecisionStatement>` element supplies a statement by the issuer that the request for access by the specified subject to the specified resource has resulted in the specified decision on the basis of some optionally specified evidence.

The resource is identified by means of a URI reference. In order for the assertion to be interpreted correctly and securely the issuer and relying party MUST interpret each URI reference in a consistent manner. Failure to achieve a consistent URI reference interpretation can result in different authorization decisions depending on the encoding of the resource URI reference. Rules for normalizing URI references are to be found in IETF RFC 2396 **[RFC 2396]** §6:

> In general, the rules for equivalence and definition of a normal form, if any, are scheme dependent. When a scheme uses elements of the common syntax, it will also use the common syntax equivalence rules, namely that the scheme and hostname are case insensitive and a URL with an explicit ":port", where the port is the default for the scheme, is equivalent to one where the port is elided.

To avoid ambiguity resulting from variations in URI encoding SAML requestors and responders SHOULD employ the URI normalized form wherever possible as follows:

- The assertion issuer SHOULD encode all resource URIs in normalized form.
- Relying parties SHOULD convert resource URIs to normalized form prior to processing.

Inconsistent URI interpretation can also result from differences between the URI syntax and the semantics of an underlying file system. Particular care is required if URIs are employed to specify an access control policy language. The following security conditions should be satisfied by the system which employs SAML assertions:

- Parts of the URI syntax are case sensitive. If the underlying file system is case insenstive a requestor SHOULD NOT be able to gain access to a denied resource by changing the case of a part of the resource URI.
- Many file systems support mechanisms such as logical paths and symbolic links which allow users to establish logical equivalences between file system entries. A requestor SHOULD NOT be able to gain access to a denied resource by creating such an equivalence.

The `<AuthorizationDecisionStatement>` element is of type **AuthorizationDecisionStatementType**, which extends **SubjectStatementAbstractType** with the addition of the following elements (in order) and attributes:

`Resource` [Required]

A URI reference identifying the resource to which access authorization is sought. It is permitted for this attribute to have the value of the empty URI reference (""), and the meaning is defined to be "the start of the current document", as specified by IETF RFC 2396 **[RFC 2396]** §4.2.

`Decision` [Required]

The decision rendered by the issuer with respect to the specified resource. The value is of the **DecisionType** simple type.

`<Action>` [One or more]

The set of actions authorized to be performed on the specified resource.

`<Evidence>` [Optional]

A set of assertions that the issuer relied on in making the decision.

The following schema fragment defines the `<AuthorizationDecisionStatement>` element and its **AuthorizationDecisionStatementType** complex type:

```
<element name="AuthorizationDecisionStatement"
type="saml:AuthorizationDecisionStatementType"/>
<complexType name="AuthorizationDecisionStatementType">
  <complexContent>
        <extension base="saml:SubjectStatementAbstractType">
              <sequence>
                    <element ref="saml:Action" maxOccurs="unbounded"/>
                    <element ref="saml:Evidence" minOccurs="0"/>
              </sequence>
              <attribute name="Resource" type="anyURI" use="required"/>
```

```
                <attribute name="Decision" type="saml:DecisionType"
use="required"/>
            </extension>
    </complexContent>
</complexType>
```

2.4.4.1 Element <Action>

The `<Action>` element specifies an action on the specified resource for which permission is sought. It has the following attribute and string-data content:

`Namespace` [Optional]

A URI reference representing the namespace in which the name of the specified action is to be interpreted. If this element is absent, the namespace urn:oasis:names:tc:SAML:1.0:action:rwedc-negation specified in Section 7.2.2 is in effect.

`string data` [Required]

An action sought to be performed on the specified resource.

The following schema fragment defines the `<Action>` element and its **ActionType** complex type:

```
<element name="Action" type="saml:ActionType"/>
<complexType name="ActionType">
    <simpleContent>
        <extension base="string">
            <attribute name="Namespace" type="anyURI"/>
        </extension>
    </simpleContent>
</complexType>
```

2.4.4.2 Element <Evidence>

The `<Evidence>` element contains an assertion that the issuer relied on in issuing the authorization decision. It has the **EvidenceType** complex type. It contains one of the following elements:

`<AssertionIDReference>`

Specifies an assertion by reference to the value of the assertion's `AssertionID` attribute.

`<Assertion>`

Specifies an assertion by value.

The provision of an assertion as evidence MAY affect the reliance agreement between the requestor and the Authorization Authority. For example, in the case that the requestor presented an assertion to the Authorization Authority in a request, the Authorization Authority MAY use that assertion as evidence in making its response without endorsing the assertion as valid either to the requestor or any third party.

The following schema fragment defines the `<Evidence>` element and its **EvidenceType** complex type:

```
<element name="Evidence" type="saml:EvidenceType"/>
<complexType name="EvidenceType">
    <choice maxOccurs="unbounded">
        <element ref="saml:AssertionIDReference"/>
        <element ref="saml:Assertion"/>
    </choice>
</complexType>
```

2.4.5 Element <AttributeStatement>

The `<AttributeStatement>` element supplies a statement by the issuer that the specified subject is associated with the specified attributes. It is of type **AttributeStatementType**, which extends **SubjectStatementAbstractType** with the addition of the following element:

<Attribute> [One or More]

The <Attribute> element specifies an attribute of the subject.

The following schema fragment defines the <AttributeStatement> element and its **AttributeStatementType** complex type:

```
<element name="AttributeStatement" type="saml:AttributeStatementType"/>
<complexType name="AttributeStatementType">
   <complexContent>
         <extension base="saml:SubjectStatementAbstractType">
               <sequence>
                     <element ref="saml:Attribute" maxOccurs="unbounded"/>
               </sequence>
         </extension>
   </complexContent>
</complexType>
```

2.4.5.1 Elements <AttributeDesignator> and <Attribute>

The <AttributeDesignator> element identifies an attribute name within an attribute namespace. It has the **AttributeDesignatorType** complex type. It is used in an attribute query to request that attribute values within a specific namespace be returned (see Section 3.3.4 for more information). The <AttributeDesignator> element contains the following XML attributes:

AttributeNamespace [Required]

The namespace in which the AttributeName elements are interpreted.

AttributeName [Required]

The name of the attribute.

The following schema fragment defines the <AttributeDesignator> element and its **AttributeDesignatorType** complex type:

```
<element name="AttributeDesignator" type="saml:AttributeDesignatorType"/>
<complexType name="AttributeDesignatorType">
   <attribute name="AttributeName" type="string" use="required"/>
   <attribute name="AttributeNamespace" type="anyURI" use="required"/>
</complexType>
```

The <Attribute> element supplies the value for an attribute of an assertion subject. It has the **AttributeType** complex type, which extends **AttributeDesignatorType** with the addition of the following element:

<AttributeValue> [Any Number]

The value of the attribute.

The following schema fragment defines the <Attribute> element and its **AttributeType** complex type:

```
<element name="Attribute" type="saml:AttributeType"/>
<complexType name="AttributeType">
   <complexContent>
         <extension base="saml:AttributeDesignatorType">
               <sequence>
                     <element ref="saml:AttributeValue"
maxOccurs="unbounded"/>
               </sequence>
         </extension>
   </complexContent>
</complexType>
```

2.4.5.1.1 Element <AttributeValue>

The <AttributeValue> element supplies the value of a specified attribute. It is of the **anyType** simple type, which allows any well-formed XML to appear as the content of the element.

If the data content of an AttributeValue element is of a XML Schema simple type (e.g. interger, string, etc) the data type MAY be declared explicitly by means of an xsi:type declaration in the <AttributeValue> element. If the attribute value contains structured data the necessary data elements may be defined in an extension schema introduced by means of the xmlns= mechanism.

The following schema fragment defines the <AttributeValue> element:

```
<element name="AttributeValue" type="anyType"/>
```

3 SAML Protocol

SAML assertions MAY be generated and exchanged using a variety of protocols. The bindings and profiles specification for SAML **[SAMLBind]** describes specific means of transporting assertions using existing widely deployed protocols.

SAML-aware requestors MAY in addition use the SAML request-response protocol defined by the `<Request>` and `<Response>` elements. The requestor sends a `<Request>` element to a SAML authority, and the authority generates a `<Response>` element, as shown in Figure 2.

Figure 2: SAML Request-Response Protocol

3.1 Schema Header and Namespace Declarations

The following schema fragment defines the XML namespaces and other header information for the protocol schema:

```
<schema
   targetNamespace="urn:oasis:names:tc:SAML:1.0:protocol"
   xmlns="http://www.w3.org/2001/XMLSchema"
   xmlns:samlp="urn:oasis:names:tc:SAML:1.0:protocol"
   xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
   xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
   elementFormDefault="unqualified">
   <import namespace="urn:oasis:names:tc:SAML:1.0:assertion"
          schemaLocation="cs-sstc-schema-assertion-01.xsd"/>
   <import namespace="http://www.w3.org/2000/09/xmldsig#"
          schemaLocation="xmldsig-core-schema.xsd"/>
   <annotation>
          <documentation>
               Document identifier: cs-sstc-schema-protocol-01
               Location: http://www.oasis-open.org/committees/security/docs/
          </documentation>
   </annotation>
…
</schema>
```

3.2 Requests

The following sections define the SAML constructs that contain request information.

3.2.1 Complex Type RequestAbstractType

All SAML requests are of types that are derived from the abstract **RequestAbstractType** complex type. This type defines common attributes and elements that are associated with all SAML requests:

`RequestID` [Required]

An identifier for the request. It is of type **IDType**, and MUST follow the requirements specified by that type for identifier uniqueness. The values of the `RequestID` attribute in a request and the `InResponseTo` attribute in the corresponding response MUST match.

`MajorVersion` [Required]

The major version of this request. The identifier for the version of SAML defined in this specification is

`1`. Processing of this attribute is specified in Section 3.4.2.

`MinorVersion` [Required]

The minor version of this request. The identifier for the version of SAML defined in this specification is `0`. Processing of this attribute is specified in Section 3.4.2.

`IssueInstant` [Required]

The time instant of issue of the request. The time value is encoded in UTC as described in Section 1.2.2.

`<RespondWith>` [Any Number]

Each `<RespondWith>` element specifies a type of response that is acceptable to the requester.

`<ds:Signature>` [Optional]

An XML Signature that authenticates the request, see Section 5.

The following schema fragment defines the **RequestAbstractType** complex type:

```
<complexType name="RequestAbstractType" abstract="true">
   <sequence>
          <element ref="samlp:RespondWith"
                   minOccurs="0" maxOccurs="unbounded"/>
          <element ref = "ds:Signature" minOccurs="0"/>
   </sequence>
   <attribute name="RequestID" type="saml:IDType" use="required"/>
   <attribute name="MajorVersion" type="integer" use="required"/>
   <attribute name="MinorVersion" type="integer" use="required"/>
   <attribute name="IssueInstant" type="dateTime" use="required"/>
</complexType>
```

3.2.1.1 Element <RespondWith>

The `<RespondWith>` element specifies the type of Statement the requestor wants from the responder. Multiple `<RespondWith>` elements MAY be included to indicate that the requestor will accept assertions containing any of the specified types. If no `<RespondWith>` element is given, the responder may return assertions containing statements of any type.

If the requestor sends one or more `<RespondWith>` elements, the responder MUST NOT respond with assertions containing statements of any type not specified in one of the `<RespondWith>` elements.

NOTE: Inability to find assertions that meet `<RespondWith>` criteria should be treated identical to any other query for which no assertions are available. In both cases a status of success would normally be returned in the Response message, but no assertions to be found therein.

`<RespondWith>` element values are XML QNames. The XML namespace and name specifically refer to the namespace and element name of the Statement element, exactly as for the `saml:AuthorityKind` attribute; see Section 2.4.3.2. For example, a requestor that wishes to receive assertions containing only attribute statements must specify `<RespondWith>saml:AttributeStatement</RespondWith>`. To specify extension types, the `<RespondWith>` element MUST contain exactly the extension element type as specified in the `xsi:type` attribute on the corresponding element.

The following schema fragment defines the `<RespondWith>` element:

```
<element name="RespondWith" type="QName"/>
```

3.2.2 Element <Request>

The `<Request>` element specifies a SAML request. It provides either a query or a request for a specific assertion identified by `<AssertionIDReference>` or `<AssertionArtifact>`. It has the complex type **RequestType**, which extends **RequestAbstractType** by adding a choice of one of the following elements:

<Query>

An extension point that allows extension schemas to define new types of query.

<SubjectQuery>

An extension point that allows extension schemas to define new types of query that specify a single SAML subject.

<AuthenticationQuery>

Makes a query for authentication information.

<AttributeQuery>

Makes a query for attribute information.

<AuthorizationDecisionQuery>

Makes a query for an authorization decision.

<AssertionIDReference> [One or more]

Requests assertions by reference to its assertion identifier.

<AssertionArtifact> [One or more]

Requests assertions by supplying an assertion artifact that represents it.

The following schema fragment defines the <Request> element and its **RequestType** complex type:

```
<element name="Request" type="samlp:RequestType"/>
<complexType name="RequestType">
   <complexContent>
         <extension base="samlp:RequestAbstractType">
               <choice>
                     <element ref="samlp:Query"/>
                     <element ref="samlp:SubjectQuery"/>
                     <element ref="samlp:AuthenticationQuery"/>
                     <element ref="samlp:AttributeQuery"/>
                     <element ref="samlp:AuthorizationDecisionQuery"/>
                     <element ref="saml:AssertionIDReference"
maxOccurs="unbounded"/>
                     <element ref="samlp:AssertionArtifact"
maxOccurs="unbounded"/>
               </choice>
         </extension>
   </complexContent>
</complexType>
```

3.2.3 Element <AssertionArtifact>

The <AssertionArtifact> element is used to specify the assertion artifact that represents an assertion.

The following schema fragment defines the <AssertionArtifact> element:

```
<element name="AssertionArtifact" type="string"/>
```

3.3 Queries

The following sections define the SAML constructs that contain query information.

3.3.1 Element <Query>

The <Query> element is an extension point that allows new SAML queries to be defined. Its **QueryAbstractType** is abstract; extension elements MUST use the xsi:type attribute to indicate the derived type. **QueryAbstractType** is the base type from which all SAML query elements are derived.

The following schema fragment defines the <Query> element and its **QueryAbstractType** complex type:

```
<element name="Query" type="samlp:QueryAbstractType"/>
<complexType name="QueryAbstractType" abstract="true"/>
```

3.3.2 Element <SubjectQuery>

The <SubjectQuery> element is an extension point that allows new SAML queries that specify a single SAML subject. Its **SubjectQueryAbstractType** complex type is abstract; extension elements MUST use the xsi:type attribute to indicate the derived type. **SubjectQueryAbstractType** adds the <Subject> element.

The following schema fragment defines the <SubjectQuery> element and its **SubjectQueryAbstractType** complex type:

```
<element name="SubjectQuery" type="samlp:SubjectQueryAbstractType"/>
<complexType name="SubjectQueryAbstractType" abstract="true">
  <complexContent>
    <extension base="samlp:QueryAbstractType">
      <sequence>
        <element ref="saml:Subject"/>
      </sequence>
    </extension>
  </complexContent>
</complexType>
```

3.3.3 Element <AuthenticationQuery>

The <AuthenticationQuery> element is used to make the query "What assertions containing authentication statements are available for this subject?" A successful response will be in the form of assertions containing authentication statements.

Note: The <AuthenticationQuery> MAY NOT be used as a request for a new authentication using credentials provided in the request. The <AuthenticationQuery> is a request for statements about authentication acts which have occurred in a previous interaction between the indicated principal and the Authentication Authority.

This element is of type **AuthenticationQueryType**, which extends **SubjectQueryAbstractType** with the addition of the following element:

<AuthenticationMethod> [Optional]

A filter for possible responses. If it is present, the query made is "What assertions containing authentication statements do you have for this subject with the supplied authentication method?"

In response to an authentication query, a responder returns assertions with authentication statements as follows:

- First, rules given in Section 3.4.4 for matching against the <Subject> element of the query identify the assertions that may be returned.
- Further, if the <AuthenticationMethod> element is present in the query, at least one <AuthenticationMethod> element in the set of returned assertions MUST match. It is OPTIONAL for the complete set of all such matching assertions to be returned in the response.

The following schema fragment defines the <AuthenticationQuery> type and its **AuthenticationQueryType** complex type:

```
<element name="AuthenticationQuery" type="samlp:AuthenticationQueryType"/>
<complexType name="AuthenticationQueryType">
  <complexContent>
    <extension base="samlp:SubjectQueryAbstractType">
      <attribute name="AuthenticationMethod" type="anyURI"/>
    </extension>
```

```
   </complexContent>
</complexType>
```

3.3.4 Element <AttributeQuery>

The <AttributeQuery> element is used to make the query “Return the requested attributes for this subject.” A successful response will be in the form of assertions containing attribute statements. This element is of type **AttributeQueryType**, which extends **SubjectQueryAbstractType** with the addition of the following element and attribute:

Resource [Optional]

The Resource attribute if present specifies that the attribute query is made in response to a specific authorization decision relating to the resource. The responder MAY use the resource attribute to establish the scope of the request. It is permitted for this attribute to have the value of the empty URI reference (""), and the meaning is defined to be "the start of the current document", as specified by **[RFC 2396]** §4.2.

If the resource attribute is specified and the responder does not wish to support resource-specific attribute queries, or if the resource value provided is invalid or unrecognized, then it SHOULD respond with a top-level StatusCode value of Responder and a second-level code value of ResourceNotRecognized

<AttributeDesignator> [Any Number] (see Section 2.4.5.1)

Each <AttributeDesignator> element specifies an attribute whose value is to be returned. If no attributes are specified, it indicates that all attributes allowed by policy are requested.

The following schema fragment defines the <AttributeQuery> element and its **AttributeQueryType** complex type:

```
<element name="AttributeQuery" type="samlp:AttributeQueryType"/>
<complexType name="AttributeQueryType">
   <complexContent>
         <extension base="samlp:SubjectQueryAbstractType">
               <sequence>
                     <element ref="saml:AttributeDesignator"
                           minOccurs="0" maxOccurs="unbounded"/>
               </sequence>
               <attribute name="Resource" type="anyURI reference"
use="optional"/>
         </extension>
   </complexContent>
</complexType>
```

3.3.5 Element <AuthorizationDecisionQuery>

The <AuthorizationDecisionQuery> element is used to make the query “Should these actions on this resource be allowed for this subject, given this evidence?” A successful response will be in the form of assertions containing authorization decision statements. This element is of type **AuthorizationDecisionQueryType**, which extends **SubjectQueryAbstractType** with the addition of the following elements and attribute:

`Resource` [Required]

A URI reference indicating the resource for which authorization is requested.

`<Action>` [One or More]

The actions for which authorization is requested.

`<Evidence>` [Optional]

A set of assertions that the responder MAY rely on in making its response.

The following schema fragment defines the `<AuthorizationDecisionQuery>` element and its **AuthorizationDecisionQueryType** complex type:

```
<element name="AuthorizationDecisionQuery"
type="samlp:AuthorizationDecisionQueryType"/>
<complexType name="AuthorizationDecisionQueryType">
   <complexContent>
         <extension base="samlp:SubjectQueryAbstractType">
               <sequence>
                     <element ref="saml:Action" maxOccurs="unbounded"/>
                     <element ref="saml:Evidence" minOccurs="0"
maxOccurs="1"/>
               </sequence>
               <attribute name="Resource" type="anyURI" use="required"/>
         </extension>
   </complexContent>
</complexType>
```

3.4 Responses

The following sections define the SAML constructs that contain response information.

3.4.1 Complex Type ResponseAbstractType

All SAML responses are of types that are derived from the abstract **ResponseAbstractType** complex type. This type defines common attributes and elements that are associated with all SAML responses:

1142 `ResponseID` [Required]

1143 An identifier for the response. It is of type **IDType**, and MUST follow the requirements specified by
1144 that type for identifier uniqueness.

1145 `InResponseTo` [Optional]

1146 A reference to the identifier of the request to which the response corresponds, if any. If the response
1147 is not generated in response to a request, or if the RequestID of a request cannot be determined
1148 (because the request is malformed), then this attribute MUST NOT be present. Otherwise, it MUST
1149 be present and match the value of the corresponding RequestID attribute.

1150 `MajorVersion` [Required]

1151 The major version of this response. The identifier for the version of SAML defined in this specification
1152 is `1`. Processing of this attribute is specified in Section 3.4.4.

1153 `MinorVersion` [Required]

1154 The minor version of this response. The identifier for the version of SAML defined in this specification
1155 is `0`. Processing of this attribute is specified in Section 3.4.4.

1156 `IssueInstant` [Required]

1157 The time instant of issue of the response. The time value is encoded in UTC as described in
1158 Section1.2.2.

1159 `Recipient` [Optional]

1160 The intended recipient of this response. This is useful to prevent malicious forwarding of responses to
1161 unintended recipients, a protection that is required by some use profiles. It is set by the generator of
1162 the response to a URI reference that identifies the intended recipient. If present, the actual recipient
1163 MUST check that the URI reference identifies the recipient or a resource managed by the recipient. If
1164 it does not, the response MUST be discarded.

1165 `<ds:Signature>` [Optional]

1166 An XML Signature that authenticates the response, see Section 5.

1167 The following schema fragment defines the **ResponseAbstractType** complex type:

```
1168 <complexType name="ResponseAbstractType" abstract="true">
1169   <sequence>
1170         <element ref = "ds:Signature" minOccurs="0"/>
1171   </sequence>
1172   <attribute name="ResponseID" type="saml:IDType" use="required"/>
1173   <attribute name="InResponseTo" type="saml:IDReferenceType" use="optional"/>
1174   <attribute name="MajorVersion" type="integer" use="required"/>
1175   <attribute name="MinorVersion" type="integer" use="required"/>
1176   <attribute name="IssueInstant" type="dateTime" use="required"/>
1177   <attribute name="Recipient" type="anyURI" use="optional"/>
1178 </complexType>
```

1179 3.4.2 Element <Response>

1180 The `<Response>` element specifies the status of the corresponding SAML request and a list of zero or
1181 more assertions that answer the request. It has the complex type **ResponseType**, which extends
1182 **ResponseAbstractType** by adding the following elements (in an unbounded mixture):

1183 `<Status>` [Required] (see Section 3.4.3)

1184 A code representing the status of the corresponding request.

1185 `<Assertion>` [Any Number] (see Section 2.3.2)

1186 Specifies an assertion by value.

1187 The following schema fragment defines the `<Response>` element and its **ResponseType** complex type:

```
<element name="Response" type="samlp:ResponseType"/>
<complexType name="ResponseType">
   <complexContent>
          <extension base="samlp:ResponseAbstractType">
                <sequence>
                      <element ref="samlp:Status"/>
                      <element ref="saml:Assertion" minOccurs="0"
maxOccurs="unbounded"/>
                </sequence>
          </extension>
   </complexContent>
</complexType>
```

3.4.3 Element <Status>

The <Status> element:

<StatusCode> [Required]

A code representing the status of the corresponding request.

<StatusMessage> [Optional]

A message which MAY be returned to an operator.

<StatusDetail> [Optional]

Specifies additional information concerning an error condition.

The following schema fragment defines the <Status> element and its **StatusType** complex type:

```
<element name="Status" type="samlp:StatusType"/>
<complexType name="StatusType">
   <sequence>
          <element ref="samlp:StatusCode"/>
          <element ref="samlp:StatusMessage" minOccurs="0" maxOccurs="1"/>
          <element ref="samlp:StatusDetail" minOccurs="0"/>
   </sequence>
</complexType>
```

3.4.3.1 Element <StatusCode>

The <StatusCode> element specifies one or more nested codes representing the status of the corresponding request. top-most code value MUST be one of the values defined below. Subsequent nested code values, if present, may provide more specific information concerning a particular error.

Value [Required]

The status code value as defined below.

<StatusCode> [Optional]

An optional subordinate status code value that provides more specific information on an error condition.

The following top-level **StatusCode** Value QNames are defined. The responder MUST NOT include a code not listed below except by nesting it below one of the listed values.

1228 `Success`

1229 The request succeeded.

1230 `VersionMismatch`

1231 The receiver could not process the request because the version was incorrect.

1232 `Requester`

1233 The request could not be performed due to an error on the part of the requester.

1234 `Responder`

1235 The request could not be performed due to an error on the part of the responder.

1236 The following second-level status codes are referenced at various places in the specification. Additional
1237 subcodes MAY be defined in future versions of the SAML specification.

1238 `RequestVersionTooHigh`

1239 The protocol version specified in the request is a major upgrade from the highest protocol version
1240 supported by the responder.

1241 `RequestVersionTooLow`

1242 The responder cannot respond to the particular request using the SAML version specified in the
1243 request because it is too low.

1244 `RequestVersionDeprecated`

1245 The responder does not respond to any requests with the protocol version specified in the request.

1246 `TooManyResponses`

1247 The response would contain more elements than the responder will return.

1248 `RequestDenied`

1249 The responder is able to process the request but has chosen not to respond. MAY be used when the
1250 responder is concerned about the security context of the request or the sequence of requests
1251 received from a particular client.

1252 `ResourceNotRecognized`

1253 The responder does not wish to support resource-specific attribute queries, or the resource value
1254 provided is invalid or unrecognized.

1255 All status code values defined in this document are QNames associated with the SAML protocol
1256 namespace, urn:oasis:names:tc:SAML:1.0:protocol, and MUST be prefixed appropriately when they appear
1257 in SAML messages. SAML extensions and SAML Responders are free to define more specific status
1258 codes in other namespaces, but MAY NOT define additional codes in either the SAML assertion or
1259 protocol namespaces.

1260 The QNames defined as status codes SHOULD only be used in the StatusCode element's Value attribute
1261 and have the above semantics only in that context.

1262 The following schema fragment defines the `<StatusCode>` element and its **StatusCodeType** complex
1263 type:

```
1264 <element name="StatusCode" type="samlp:StatusCodeType"/>
1265 <complexType name="StatusCodeType">
1266   <sequence>
1267         <element ref="samlp:StatusCode" minOccurs="0"/>
1268   </sequence>
1269   <attribute name="Value" type="QName" use="required"/>
1270 </complexType>
```

1271 3.4.3.2 Element <StatusMessage>

1272 The `<StatusMessage>` element specifies a message that MAY be returned to an operator:

The following schema fragment defines the <StatusMessage> element and its **StatusMessageType** complex type:

```
<element name="StatusMessage" type="string"/>
```

3.4.3.3 Element <StatusDetail>

The <StatusDetail> element MAY be used to specify additional information concerning an error condition.

The following schema fragment defines the <StatusDetail> element and its **StatusDetailType** complex type:

```
<element name="StatusDetail" type="samlp:StatusDetailType"/>
<complexType name="StatusDetailType">
   <sequence>
          <any namespace="##any" processContents="lax" minOccurs="0"
maxOccurs="unbounded"/>
   </sequence>
</complexType>
```

3.4.4 Responses to <AuthenticationQuery> and <AttributeQuery>

Responses to Authentication and Attribute queries are constructed by matching against the <saml:Subject> element found within the <AuthenticationQuery> or <AttributeQuery> elements. In response to these queries, every assertion returned by a SAML responder MUST contain at least one statement whose <saml:Subject> element **strongly matches** the <saml:Subject> element found in the query.

A <saml:Subject> element S1 strongly matches S2 if and only if:

1. If S2 includes a <saml:NameIdentifier> element, then S1 must include an identical <saml:NameIdentifier> element.
2. If S2 includes a <saml:SubjectConfirmation> element, then S1 must include an identical <saml:SubjectConfirmation> element.

If the responder cannot provide an assertion with any statement(s) satisfying the constraints expressed by a query, the <saml:Response> element MUST NOT contain an <Assertion> element and MUST include a <saml:StatusCode> with value "Success". It MAY return a <saml:StatusMessage> with additional information.

4 SAML Versioning

SAML version information appears in the following elements:

- `<Assertion>`
- `<Request>`
- `<Response>`

The version numbering of the SAML assertion is independent of the version numbers of the SAML request-response protocol. The version information for each consists of a major version number and a minor version number, both of which are integers. In accordance with industry practice a version number SHOULD be presented to the user in the form *Major*.*Minor*. This document defines SAML Assertions 1.0 and SAML Protocol 1.0.

The version number $Major_B.Minor_B$ is higher than the version number $Major_A.Minor_A$ if and only if:

$$Major_B > Major_A \vee ((Major_B = Major_A) \wedge Minor_B > Minor_A)$$

Each revision of SAML SHALL assign version numbers to assertions, requests, and responses that are the same as or higher than the corresponding version number in the SAML version that immediately preceded it. The specifications may be revised without a change to the SAML major or minor version number, as long as the specification changes raise no compatibility issues with SAML implementations.

New versions of SAML SHALL assign new version numbers as follows:

- **Minor upgrade:** $(Major_B = Major_A) \wedge (Minor_B > Minor_A)$
  If the major version number of versions *A* and *B* are the same and the minor version number of *B* is higher than that of *A*, the new SAML version MAY introduce changes to the SAML schema and semantics but any changes that are introduced in *B* SHALL be compatible with version *A*.
- **Major upgrade:** $Major_B > Major_A$
  If the major version of *B* number is higher than the major version of *A*, Version *B* MAY introduce changes to the SAML schema and semantics that are incompatible with *A*.

4.1 Assertion Version

A SAML authority MUST NOT issue any assertion whose version number is not supported.

A SAML relying party MUST reject any assertion whose major version number is not supported.

A SAML relying party MAY reject any assertion whose version number is higher than the highest supported version.

4.2 Request Version

A SAML authority SHOULD issue requests that specify the highest SAML version supported by both the sender and recipient.

If the SAML authority does not know the capabilities of the recipient it should assume that it supports the highest SAML version supported by the sender.

4.3 Response Version

A SAML authority MUST NOT issue responses that specify a higher SAML version number than the corresponding request.

A SAML authority MUST NOT issue a response that has a major version number that is lower than the major version number of the corresponding request except to report the error `RequestVersionTooHigh`.

An error response resulting from incompatible protocol versions MUST result in reporting a top-level StatusCode value of VersionMismatch, and MAY result in reporting one of the following second-level values:

`RequestVersionTooHigh`

The protocol version specified in the request is a major upgrade from the highest protocol version supported by the responder.

`RequestVersionTooLow`

The responder cannot respond to the particular request using the SAML version specified in the request because it is too low.

`RequestVersionDeprecated`

The responder does not respond to any requests with the protocol version specified in the request.

5 SAML and XML Signature Syntax and Processing

SAML Assertions, Request and Response messages may be signed, with the following benefits:

- An Assertion signed by the asserting party (AP). This supports:
  1. Message integrity.
  2. Authentication of the asserting party to a relying party (RP).
  3. If the signature is based on the asserting party's public-private key pair, then it also provides for non-repudiation of origin.
- A SAML request or a SAML response message signed by the message originator. This supports:
  1. Message integrity.
  2. Authentication of message origin to a destination.
  3. If the signature is based on the originator's public-private key pair, then it also provides for non-repudiation of origin.

Note:

- SAML documents may be the subject of signatures from different packaging contexts. **[XMLSig]** provides a framework for signing in XML and is the framework of choice. However, signing may also take place in the context of S/MIME or Java objects that contain SAML documents. One goal is to ensure compatibility with this type of "foreign" digital signing.
- It is useful to characterize situations when a digital signature is NOT required in SAML.

Assertions:

The asserting party has provided the assertion to the relying party, authenticated by means other than digital signature and the channel is secure. In other words, the RP has obtained the assertion from the AP directly (no intermediaries) through a secure channel and the AP has authenticated to the RP.

Request/Response messages:

The originator has authenticated to the destination and the destination has obtained the assertion directly from the originator (no intermediaries) through secure channel(s).

Many different techniques are available for "direct" authentication and secure channel between two parties. The list includes SSL, HMAC, password-based login etc. Also the security requirement depends on the communicating applications and the nature of the assertion transported.

All other contexts require the use of digital signature for assertions and request and response messages. Specifically:

1. An assertion obtained by a relying party from an entity other than the asserting party MUST be signed by the asserting party.
2. A SAML message arriving at a destination from an entity other than the originating site MUST be signed by the origin site.

5.1 Signing Assertions

All SAML assertions MAY be signed using the XML Signature. This is reflected in the assertion schema – Section 2.3.

5.2 Request/Response Signing

All SAML requests and responses MAY be signed using the XML Signature. This is reflected in the schema – Sections 3.2 and 3.4.

5.3 Signature Inheritance

A SAML assertion may be embedded within another SAML element, such as an enclosing <Assertion> or a <Request> or <Response>, which may be signed. When a SAML assertion does not contain a <ds:Signature> element, but is contained in an enclosing SAML element that contains a <ds:Signature> element, and the signature applies to the <Assertion> element and all its children, then the assertion can be considered to inherit the signature from the enclosing element. The resulting interpretation should be equivalent to the case where the assertion itself was signed with the same key and signature options.

Many SAML use cases involve SAML XML data enclosed within other protected data structures such as signed SOAP messages, S/MIME packages, and authenticated SSL connections. SAML profiles may define additional rules for interpreting SAML elements as inheriting signatures or other authentication information from the surrounding context, but no such inheritance should be inferred unless specifically identified by the profile.

5.4 XML Signature Profile

The XML Signature **[XMLSig]** specification calls out a general XML syntax for signing data with many flexibilities and choices. This section details the constraints on these facilities so that SAML processors do not have to deal with the full generality of XML Signature processing.

5.4.1 Signing Formats

XML Signature has three ways of representing signature in a document: enveloping, enveloped, and detached.

SAML assertions and protocols MUST use the enveloped signatures for signing assertions and protocols. SAML processors should support use of RSA signing and verification for public key operations.

5.4.2 Canonicalization Method

XML Signature REQUIRES the Canonical XML (omits comments) (http://www.w3.org/TR/2001/REC-xml-c14n-20010315). SAML implementations SHOULD use Canonical XML with no comments.

5.4.3 Transforms

[XMLSig] REQUIRES the enveloped signature transform http://www.w3.org/2000/09/xmldsig#enveloped-signature.

5.4.4 KeyInfo

SAML does not restrict or impose any restrictions in this area. Therefore, following **[XMLSig]**, <ds:KeyInfo> may be absent.

5.4.5 Binding Between Statements in a Multi-Statement Assertion

Use of signing does not affect semantics of statements within assertions in any way, as stated in this document Sections 1 through 4.

6 SAML Extensions

The SAML schemas support extensibility. An example of an application that extends SAML assertions is the XTAML system for management of embedded trust roots **[XTAML]**. The following sections explain how to use the extensibility features in SAML to create extension schemas.

Note that elements in the SAML schemas are not blocked from substitution, so that all SAML elements MAY serve as the head element of a substitution group. Also, types are not defined as `final`, so that all SAML types MAY be extended and restricted. The following sections discuss only elements that have been specifically designed to support extensibility.

6.1 Assertion Schema Extension

The SAML assertion schema is designed to permit separate processing of the assertion package and the statements it contains, if the extension mechanism is used for either part.

The following elements are intended specifically for use as extension points in an extension schema; their types are set to `abstract`, so that the use of an `xsi:type` attribute with these elements is REQUIRED:

- `<Assertion>`
- `<Condition>`
- `<Statement>`
- `<SubjectStatement>`

In addition, the following elements that are directly usable as part of SAML MAY be extended:

- `<AuthenticationStatement>`
- `<AuthorizationDecisionStatement>`
- `<AttributeStatement>`
- `<AudienceRestrictionCondition>`

Finally, the following elements are defined to allow elements from arbitrary namespaces within them, which serves as a built-in extension point without requiring an extension schema:

- `<AttributeValue>`
- `<Advice>`

6.2 Protocol Schema Extension

The following elements are intended specifically for use as extension points in an extension schema; their types are set to `abstract`, so that the use of an `xsi:type` attribute with these elements is REQUIRED:

- `<Query>`
- `<SubjectQuery>`

In addition, the following elements that are directly usable as part of SAML MAY be extended:

- `<Request>`
- `<AuthenticationQuery>`
- `<AuthorizationDecisionQuery>`
- `<AttributeQuery>`
- `<Response>`

6.3 Use of Type Derivation and Substitution Groups

W3C XML Schema **[Schema1]** provides two principal mechanisms for specifying an element of an extended type: type derivation and substitution groups.

For example, a <Statement> element can be assigned the type **NewStatementType** by means of the xsi:type attribute. For such an element to be schema-valid, **NewStatementType** needs to be derived from **StatementType**. The following example of a SAML assertion assumes that the extension schema (represented by the new: prefix) has defined this new type:

```
<saml:Assertion …>
  <saml:Statement xsi:type="new:NewStatementType">
  …
  </saml:Statement>
</saml:Assertion>
```

Alternatively, the extension schema can define a <NewStatement> element that is a member of a substitution group that has <Statement> as a head element. For the substituted element to be schema-valid, it needs to have a type that matches or is derived from the head element's type. The following is an example of an extension schema fragment that defines this new element:

```
<xsd:element "NewStatement" type="new:NewStatementType"
      substitutionGroup="saml:Statement"/>
```

The substitution group declaration allows the <NewStatement> element to be used anywhere the SAML <Statement> element can be used. The following is an example of a SAML assertion that uses the extension element:

```
<saml:Assertion …>
   <new:NewStatement>
      …
   </new:NewStatement>
</saml:Assertion>
```

The choice of extension method has no effect on the semantics of the XML document but does have implications for interoperability.

The advantages of type derivation are as follows:

- A document can be more fully interpreted by a parser that does not have access to the extension schema because a "native" SAML element is available.
- At the time of writing, some W3C XML Schema validators do not support substitution groups, whereas the xsi:type attribute is widely supported.

The advantage of substitution groups is that a document can be explained without the need to explain the functioning of the xsi:type attribute.

7 SAML-Defined Identifiers

The following sections define URI-based identifiers for common authentication protocols and actions.

Where possible an existing URN is used to specify a protocol. In the case of IETF protocols the URN of the most current RFC that specifies the protocol is used. URI references created specifically for SAML have the initial stem:

```
urn:oasis:names:tc:SAML:1.0:
```

7.1 Authentication Method Identifiers

The <AuthenticationMethod> and <SubjectConfirmationMethod> elements perform different functions within the SAML architecture, although both can refer to the same underlying mechanisms. <AuthenticationMethod> is a part of an Authentication Statement, which describes an authentication act which occured in the past. The <AuthenticationMethod> indicates how that authentication was done. Note that the authentication statement does not provide the means to perform that authentication, such as a password, key, or certificate.

In contrast, <SubjectConfirmationMethod> is a part of the <SubjectConfirmation>, which is used to allow the Relying Party to confirm that the request or message came from the System Entity that corresponds to the Subject in the statement. The <SubjectConfirmationMethod> indicates the method that the Relying Party can use to do this in the future. This may or may not have any relationship to an authentication that was performed previously. Unlike the Authentication Method, the <SubjectConfirmationMethod> may be accompanied with some piece of information, such as a certificate or key, which will allow the Relying Party to perform the necessary check.

Subject Confirmation Methods are defined in the SAML Profile or Profiles in which they are used **[SAMLBind]**. Additional methods may be added by defining new profiles or by private agreement.

The following identifiers refer to SAML specified Authentication methods.

7.1.1 Password

URI: urn:oasis:names:tc:SAML:1.0:am:password

The authentication was performed by means of a password.

7.1.2 Kerberos

URI: urn:ietf:rfc:1510

The authentication was performed by means of the Kerberos protocol **[RFC 1510]**, an instantiation of the Needham-Schroeder symmetric key authentication mechanism **[Needham78]**.

7.1.3 Secure Remote Password (SRP)

URI: urn:ietf:rfc:2945

The authentication was performed by means of Secure Remote Password protocol as specified in **[RFC 2945]**.

7.1.4 Hardware Token

URI: urn:oasis:names:tc:SAML:1.0:am:HardwareToken

The authentication was performed by means of an unspecified hardware token.

7.1.5 SSL/TLS Certificate Based Client Authentication:

URI: urn:ietf:rfc:2246

The authentication was performed using either the SSL or TLS protocol with certificate based client authentication. TLS is described in **[RFC 2246]**.

7.1.6 X.509 Public Key

URI: urn:oasis:names:tc:SAML:1.0:am:X509-PKI

The authentication was performed by some (unspecified) mechanism on a key authenticated by means of an X.509 PKI **[X.500][PKIX]**. It may have been one of the mechanisms for which a more specific identifier has been defined below.

7.1.7 PGP Public Key

URI: urn:oasis:names:tc:SAML:1.0:am:PGP

The authentication was performed by some (unspecified) mechanism on a key authenticated by means of a PGP web of trust **[PGP]**. It may have been one of the mechanisms for which a more specific identifier has been defined below.

7.1.8 SPKI Public Key

URI: urn:oasis:names:tc:SAML:1.0:am:SPKI

The authentication was performed by some (unspecified) mechanism on a key authenticated by means of a SPKI PKI **[SPKI]**. It may have been one of the mechanisms for which a more specific identifier has been defined below.

7.1.9 XKMS Public Key

URI: urn:oasis:names:tc:SAML:1.0:am:XKMS

The authentication was performed by some (unspecified) mechanism on a key authenticated by means of a XKMS trust service **[XKMS]**. It may have been one of the mechanisms for which a more specific identifier has been defined below.

7.1.10 XML Digital Signature

URI: urn:ietf:rfc:3075

The authentication was performed by means of an XML digital signature **[RFC 3075]**.

7.1.11 Unspecified

URI: urn:oasis:names:tc:SAML:1.0:am:unspecified

The authentication was performed by an unspecified means.

7.2 Action Namespace Identifiers

The following identifiers MAY be used in the `Namespace` attribute of the `<Action>` element (see Section 2.4.4.1) to refer to common sets of actions to perform on resources.

7.2.1 Read/Write/Execute/Delete/Control

URI: urn:oasis:names:tc:SAML:1.0: action:rwedc

Defined actions:

1574 `Read Write Execute Delete Control`

1575 These actions are interpreted in the normal manner, i.e.:

1576 `Read`

1577 The subject may read the resource.

1578 `Write`

1579 The subject may modify the resource.

1580 `Execute`

1581 The subject may execute the resource.

1582 `Delete`

1583 The subject may delete the resource.

1584 `Control`

1585 The subject may specify the access control policy for the resource.

1586 7.2.2 Read/Write/Execute/Delete/Control with Negation

1587 **URI:** urn:oasis:names:tc:SAML:1.0:action:rwedc-negation

1588 Defined actions:

1589 `Read Write Execute Delete Control ~Read ~Write ~Execute ~Delete ~Control`

1590 The actions specified in Section 7.2.1 are interpreted in the same manner described there. Actions
1591 prefixed with a tilde (~) are negated permissions and are used to affirmatively specify that the stated
1592 permission is denied. Thus a subject described as being authorized to perform the action `~Read` is
1593 affirmatively denied read permission.

1594 A SAML authority MUST NOT authorize both an action and its negated form.

1595 7.2.3 Get/Head/Put/Post

1596 **URI:** urn:oasis:names:tc:SAML:1.0: action:ghpp

1597 Defined actions:

1598 `GET HEAD PUT POST`

1599 These actions bind to the corresponding HTTP operations. For example a subject authorized to perform
1600 the `GET` action on a resource is authorized to retrieve it.

1601 The `GET` and `HEAD` actions loosely correspond to the conventional read permission and the `PUT` and
1602 `POST` actions to the write permission. The correspondence is not exact however since an HTTP GET
1603 operation may cause data to be modified and a POST operation may cause modification to a resource
1604 other than the one specified in the request. For this reason a separate Action URI reference specifier is
1605 provided.

1606 7.2.4 UNIX File Permissions

1607 **URI:** urn:oasis:names:tc:SAML:1.0:action:unix

1608 The defined actions are the set of UNIX file access permissions expressed in the numeric (octal) notation.

1609 The action string is a four-digit numeric code:

1610 *extended user group world*

1611 Where the *extended* access permission has the value

1612 +2 if sgid is set

1613 +4 if suid is set

1614 The *user group* and *world* access permissions have the value

+1 if execute permission is granted

+2 if write permission is granted

+4 if read permission is granted

For example, `0754` denotes the UNIX file access permission: user read, write and execute, group read and execute and world read.

8 References

[Kern-84] B. Kernighan, Rob Pike *The UNIX Programming Environment*, (March 1984) Prentice Hall Computer Books;

[Needham78] R. Needham et al., *Using Encryption for Authentication in Large Networks of Computers*, Communications of the ACM, Vol. 21 (12), pp. 993-999, December 1978.

[PGP] Atkins, D., Stallings, W. and P. Zimmermann, *PGP Message Exchange Formats*, RFC 1991, August 1996.

[PKCS1] B. Kaliski, *PKCS #1: RSA Encryption Version 2*.0, RSA Laboratories, also IETF RFC 2437, October 1998. http://www.ietf.org/rfc/rfc2437.txt

[PKCS7] B. Kaliski., *PKCS #7: Cryptographic Message Syntax, Version 1.5*, RFC 2315, March 1998.

[PKIX] R. Housley, W. Ford, W. Polk, D. Solo. *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*. RFC 2459, January 1999.

[RFC 1510] J. Kohl, C. Neuman. *The Kerberos Network Authentication Requestor (V5).* September 1993. http://www.ietf.org/rfc/rfc1510.txt

[RFC 2104] H. Krawczyk et al., *HMAC: Keyed Hashing for Message Authentication*, http://www.ietf.org/rfc/rfc2104.txt, IETF RFC 2104, February 1997.

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

[RFC 2246] T. Dierks, C. Allen. *The TLS Protocol Version 1.0*. January 1999. http://www.ietf.org/rfc/rfc2246.txt

[RFC 2253] M. Wahl et al., *Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names*. December 1997. http://www.ietf.org/rfc/rfc2253.txt

[RFC 2396] T. Berners-Lee et al., *Uniform Resource Identifiers (URI): Generic Syntax* http://www.ietf.org/rfc/rfc2396.txt IETF?

[RFC 2630] R. Housley. *Cryptographic Message Syntax*. June 1999. http://www.ietf.org/rfc/rfc630.txt

[RFC 2648] R. Moats. *A URN Namespace for IETF Documents.* August 1999. http://www.ietf.org/rfc/rfc2648.txt

[RFC 2822] P. Resnick. *Internet Message Format*. April 2001. http://www.ietf.org/rfc/rfc2822.txt

[RFC 2945] T. Wu, *The SRP Authentication and Key Exchange System*, September 2000, http://www.ietf.org/rfc/rfc2945.txt

[RFC 3075] D. Eastlake, J. Reagle, D. Solo. *XML-Signature Syntax and Processing*. March 2001. http://www.ietf.org/rfc/rfc3075.txt

[SAMLBind] P. Mishra et al., *Bindings and Profiles for the OASIS Security Assertion Markup Language (SAML)*, http://www.oasis-open.org/committees/security/, OASIS, November 2002.

[SAMLConform] *Conformance Program Specification for the OASIS Security Assertion Markup Language (SAML)* http://www.oasis-open.org/committees/security/, OASIS, November 2002.

[SAMLGloss] J. Hodges et al., *Glossary for the OASIS Security Assertion Markup Language (SAML)*, http://www.oasis-open.org/committees/security/, OASIS, November 2002.

[SAMLP-XSD] P. Hallam-Baker et al., *SAML protocol schema*, http://www.oasis-open.org/committees/security/, OASIS, November 2002.

[SAMLSecure] *Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML)*, http://www.oasis-open.org/committees/security/, OASIS, November 2002.

[SAML-XSD] P. Hallam-Baker et al., *SAML assertion schema*, http://www.oasis-open.org/committees/security/, OASIS, November 2002.

[Schema1] H. S. Thompson et al., *XML Schema Part 1: Structures*, http://www.w3.org/TR/xmlschema-1/, World Wide Web Consortium Recommendation, May 2001.

[Schema2] P. V. Biron et al., *XML Schema Part 2: Datatypes*, http://www.w3.org/TR/xmlschema-2, World Wide Web Consortium Recommendation, May 2001.

[SPKI] C. Ellison, B. Frantz, B. Lampson, R. Rivest, B. Thomas, T. Ylonen. *SPKI Certificate Theory*, RFC 2693, September 1999.

[UNICODE-C] M. Davis, M. J. Dürst, http://www.unicode.org/unicode/reports/tr15/tr15-21.html, UNICODE Consortium

[W3C-CHAR] M. J. Dürst, *Requirements for String Identity Matching and String Indexing* http://www.w3.org/TR/WD-charreq, World Wide Web Consortium.

[W3C-CharMod] M. J. Dürst, *Unicode Normalization Forms* http://www.w3.org/TR/charmod/, World Wide Web Consortium.

[X.500] ITU-T Recommendation X.501: *Information Technology - Open Systems Interconnection - The Directory: Models*, 1993.

[XKMS] W. Ford, P. Hallam-Baker, B. Fox, B. Dillaway, B. LaMacchia, J. Epstein, J. Lapp, XML Key Management Specification (XKMS), W3C Note 30 March 2001, http://www.w3.org/TR/xkms/.

[XML] T. Bray et. al. *Extensible Markup Language (XML) 1.0 (Second Edition),* http://www.w3.org/TR/REC-xml, World Wide Web Consortium.

[XMLEnc] *XML Encryption Specification*, In development.

[XMLSig] D. Eastlake et al., *XML-Signature Syntax and Processing*, http://www.w3.org/TR/xmldsig-core/, World Wide Web Consortium.

[XMLSig-XSD] XML Signature Schema available from http://www.w3.org/TR/2000/CR-xmldsig-core-20001031/xmldsig-core-schema.xsd.

[XTAML] P. Hallam-Baker, *XML Trust Axiom Markup Language 1.0*, http://www.xmltrustcenter.org/, VeriSign Inc. September 2001.

Appendix A. Acknowledgments

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

- Allen Rogers, Authentica
- Irving Reid, Baltimore Technologies
- Krishna Sankar, Cisco Systems
- Ronald Jacobson, Computer Associates
- Hal Lockhart, Entegrity
- Carlisle Adams, Entrust Inc.
- Robert Griffin, Entrust Inc.
- Robert Zuccherato, Entrust Inc.
- Don Flinn, Hitachi
- Joe Pato, Hewlett-Packard (co-chair)
- Jason Rouault, Hewlett-Packard
- Marc Chanliau, Netegrity
- Chris McLaren, Netegrity
- Prateek Mishra, Netegrity
- Charles Knouse, Oblix
- Steve Anderson, OpenNetwork
- Rob Philpott, RSA Security
- Jahan Moreh, Sigaba
- Bhavna Bhatnagar, Sun Microsystems
- Jeff Hodges, Sun Microsystems (co-chair)
- Eve Maler, Sun Microsystems (former chair)
- Aravindan Ranganathan, Sun Microsystems
- Emily Xu, Sun Microsystems
- Bob Morgan, University of Washington and Internet2
- Phillip Hallam-Baker, VeriSign

Appendix B. Notices

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

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