Candidate Solution – Work Item 28d
Attribute Reconciliation between
SAML and XACML

29 September 2003

Abstract:
This non-normative document describes a solution proposal for work item 28d from the
This document describes the use case, the current SAML components affected by the
use case, a proposed solution and finally the motivation for the solution.

Current Representation

Description
Version 1.1 of the SAML specification addresses the Assertion element in section 2.3.2.
The relevant fragments of the SAML core schema is shown here:

Assertion:

```xml
<element name="Assertion" type="saml:AssertionType"/>
<complexType name="AssertionType">
  <sequence>
    <element ref="saml:Conditions" minOccurs="0"/>
    <element ref="saml:Advice" minOccurs="0"/>
    <choice maxOccurs="unbounded">
      <element ref="saml:Statement"/>
      <element ref="saml:SubjectStatement"/>
      <element ref="saml:AuthenticationStatement"/>
      <element ref="saml:AuthorizationDecisionStatement"/>
      <element ref="saml:AttributeStatement"/>
    </choice>
  </sequence>
  <element ref="ds:Signature" minOccurs="0"/>
  <attribute name="MajorVersion" type="integer" use="required"/>
  <attribute name="MinorVersion" type="integer" use="required"/>
  <attribute name="AssertionID" type="ID" use="required"/>
  <attribute name="Issuer" type="string" use="required"/>
  <attribute name="IssueInstant" type="dateTime" use="required"/>
</complexType>
```
Rationale for current representation

An assertion packages the basic information common to all assertions. To reason about the issuer of an assertion, the Issuer attribute is a string value representation of the issuing authority.

Issuer

Currently SAML specifies a string that the RP will interpret to correctly identify the issuer that created the assertion containing one or more Statements. The SAML TC assumed a wide variety of RP would request attributes from a relatively small number of authorities issuing assertions. The issuer of an assertion should be unambiguous to the intended relying party so it may accept or reject the assertion as coming from a trusted authority. As only intended audiences are assumed to interpret the value, those audiences were presumed to understand the data format of the issuer value via out of band agreement.

Proposed Solution

The proposed solution affects only the AssertionType complex type.

Schema Changes

AssertionType:

```
<complexType name="AssertionType">
  <sequence>
    <element ref="saml:Conditions" minOccurs="0"/>
    <element ref="saml:Advice" minOccurs="0"/>
    <choice maxOccurs="unbounded">
      <element ref="saml:Statement"/>
      <element ref="saml:SubjectStatement"/>
      <element ref="saml:AuthenticationStatement"/>
      <element ref="saml:AuthorizationDecisionStatement"/>
      <element ref="saml:AttributeStatement"/>
    </choice>
    <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="ID" use="required"/>
  <attribute name="Issuer" type="string" use="required"/>
  <attribute name="Format" type="string" use="required"/>
  <attribute name="IssueInstant" type="dateTime" use="required"/>
</complexType>
```

Affected facets

Format

An optional attribute will be added to each Assertion construct. The Format attribute contains a URI that indicates how the value of the Issuer attribute should be interpreted.
Standard URIs should be defined, as they are defined for the Format attribute of the NameIdentifier construct.

**Motivation for modifications**

Including both an issuer and issuer format standardizes the interpretation of common types of communicated values to determine whether the assertion issuer represents a trusted authority. Further, specification of the issuer format provides a clue regarding how to lookup an issuer-name during the verification process.

**Compatibility with SAML 1.x**

As the IssuerFormat attribute is defined as optional, a SAML 1.x assertion that does not carry the attribute should still be readily interpreted. Of course, any relying party will need out-of-band data to correctly interpret the Issuer attribute value if the IssuerFormat attribute is not present.