SAML V2.0 Identity Assurance Profiles
Version 1.0
Committee Draft 02
10 August 2010

Specification URIs:
This Version:
http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-assurance-profile-cd-02.html
http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-assurance-profile-cd-02.odt
(Authoritative)

Previous Version:
http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-assurance-profile-draft-02.html
http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-assurance-profile-draft-02.odt
(Authoritative)
http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-assurance-profile-draft-02.pdf

Latest Version:
http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-assurance-profile.html
http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-assurance-profile.odt (Authoritative)
http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-assurance-profile.pdf

Latest Approved Version:
http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-assurance-profile-cd-02.html
http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-assurance-profile-cd-02.odt
(Authoritative)

Technical Committee:
OASIS Security Services TC

Chair(s):
Nathan Klingenstein, Internet2
Thomas Hardjono, MIT Kerberos Consortium

Editor(s):
RL “Bob” Morgan, Internet2
Paul Madsen, NTT
Scott Cantor, Internet2
Related Work:
This specification defines how to use existing SAML mechanisms to express identity assurance information - 1) the SAML 2.0 Authentication Context [SAMLAC] mechanisms in order to allow SAML authentication requests and assertions to carry assurance information and 2) extensions to SAML metadata [SAMLMA] to represent assurance certification information about a SAML entity within the corresponding metadata.

Declared XML Namespace(s):
N/A

Abstract:
This document specifies methods of representing assurance information in two different aspects of SAML. It provides guidelines for the use of SAML's Authentication Context [SAMLAC] mechanisms to express authentication assurance information within authentication requests and assertions. Separately, it defines an attribute suitable for inclusion in SAML Metadata [SAMLMeta] for enumerating an Identity Provider's assurance certifications.

Status:
This document was last revised or approved by the SSTC on the above date. The level of approval is also listed above. Check the current location noted above for possible later revisions of this document. This document is updated periodically on no particular schedule.

TC members should send comments on this specification to the TC’s email list. Others should send comments to the TC by using the “Send A Comment” button on the TC’s web page at http://www.oasis-open.org/committees/security.

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 IPR section of the TC web page (http://www.oasis-open.org/committees/security/ipr.php).

The non-normative errata page for this specification is located at http://www.oasis-open.org/committees/security.
# Table of Contents

1 Introduction ................................................................................................................................. 5
   1.1 Motivation [Non-Normative] ................................................................................................. 5
   1.2 Limitations [Non-Normative] ............................................................................................... 5
   1.3 Terminology .......................................................................................................................... 5
   1.4 Normative References .......................................................................................................... 6
   1.5 Non-normative References ................................................................................................. 7

2 AuthnContext Identity Assurance Guidelines .................................................................................. 8
   2.1 AuthnContext Schema Guidelines ....................................................................................... 8
   2.2 Example .................................................................................................................................. 8

3 Identity Assurance Certification Attribute Profile ........................................................................... 10
   3.1 Required Information .......................................................................................................... 10
   3.2 Profile Overview .................................................................................................................. 10
   3.3 SAML Attribute Naming ..................................................................................................... 10
   3.4 Profile-Specific XML Attributes .......................................................................................... 10
   3.5 SAML Attribute Values ....................................................................................................... 10
   3.6 Example .................................................................................................................................. 11

4 Conformance .................................................................................................................................. 12
   4.1 Identity Assurance Certification Attribute Profile Conformance .......................................... 12

Appendix A.Acknowledgments ......................................................................................................... 13
Appendix B.Revision History .......................................................................................................... 14
1 Introduction

This specification defines conventions for parties using SAML to exchange information regarding identity assurance. First, it provides guidelines for the definition of SAML Authentication Context [SAMLAC] classes corresponding to different assurance criteria – thereby allowing the corresponding URIs for those assurance-based classes to be inserted within authentication requests and responses. Secondly, it defines a SAML attribute profile that may be used to represent the certification status of an issuer of authentication statements (i.e., an Identity Provider) regarding its conformance with the requirements of an identity assurance framework.

1.1 Motivation [Non-Normative]

Many organizations using federated service access have found it useful to define or adopt “identity assurance frameworks,” such as [KIIAF]. Such frameworks offer a model for categorizing the large number of possible combinations of registration processes, security mechanisms, and authentication methods that underlie authentication processes into a smaller, more manageable set. The term “levels of assurance” (LOA) is often used to refer to this concept, or to a particular set of criteria (“assurance profile” is also used). Different combinations of processes and technology are rated according to the quality of assurance they can provide. Typically, a framework defines 3-5 levels or profiles, ranging from low to high assurance.

Two key use cases for assurance are:

1. Allowing an IdP to advertise those LOA for which it has been certified able to meet the associated requirements.
2. Allowing an RP to express its expectations for the LOA at which a user should be authenticated and, conversely, allow an IdP to indicate the actual LOA in its responses.

This document profiles SAML Metadata to satisfy the first use case, and provides guidelines for using SAML’s Authentication Context class mechanism to address the second.

1.2 Limitations [Non-Normative]

The URIs representing LOA must be configured into every system in a deployment, and the relative ordering of the levels, if any, must be decided and configured out-of-band.

1.3 Terminology

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this specification are to be interpreted as described in IETF [RFC 2119]:

…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 XML schemas appear like this.
Example code listings appear like this.
Conventional XML namespace prefixes are used throughout the listings in this specification to stand for their respective namespaces as follows, whether or not a namespace declaration is present in the example:

<table>
<thead>
<tr>
<th>Prefix</th>
<th>XML Namespace</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>attr:</td>
<td>urn:oasis:names:tc:SAML:metadata:attribute</td>
<td>This is the namespace defined in the SAML V2.0 Metadata Extension for Entity Attributes Version 1.0 specification [SAMLMA].</td>
</tr>
<tr>
<td>md:</td>
<td>urn:oasis:names:tc:SAML:2.0:metadata</td>
<td>This is the SAML V2.0 metadata namespace defined in the SAML V2.0 Metadata specification [SAMLMeta].</td>
</tr>
<tr>
<td>saml:</td>
<td>urn:oasis:names:tc:SAML:2.0:assertion</td>
<td>This is the SAML V2.0 assertion namespace defined in the SAML V2.0 core specification [SAMLCore].</td>
</tr>
<tr>
<td>samlp:</td>
<td>urn:oasis:names:tc:SAML:2.0:protocol</td>
<td>This is the SAML V2.0 protocol namespace defined in the SAML V2.0 core specification [SAMLCore].</td>
</tr>
<tr>
<td>xs:</td>
<td><a href="http://www.w3.org/2001/XMLSchema">http://www.w3.org/2001/XMLSchema</a></td>
<td>This namespace is defined in the W3C XML Schema specification [Schema1]. In schema listings, this is the default namespace and no prefix is shown.</td>
</tr>
</tbody>
</table>

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

### 1.4 Normative References

1.5 Non-normative References

2 AuthnContext Identity Assurance Guidelines

It is useful for parties using SAML to express in SAML authentication messages the assurance level or criteria (LOA) requested by a relying party, and the LOA that is applicable to an authentication assertion. Both constructs have a parameter to carry such information, specifically the <saml:AuthnContextClassRef> element.

The SAML Authentication Context specification [SAMLAC] requires that XML schemas be created to define the various criteria for a given authentication context class. The approach suggested below represents each LOA in an assurance framework as a separate authentication context class. Each LOA is characterized by a URI that defines the authentication context class, and the body of the schema contains a reference to the external documentation that defines the LOA.

These LOA/class URIs can be conveyed in the <samlp:RequestedAuthnContext> element of an authentication request and the <saml:AuthnContext> element in an assertion via the <saml:AuthnContextClassRef> element – just as for the authentication context classes defined by the original Authentication Context specification.

2.1 AuthnContext Schema Guidelines

An authentication context class schema uses XML schema constructs to stipulate the requirements of the corresponding class (e.g., to stipulate that the user authenticate to the IdP with an OTP credential). As the requirements of a given LOA are generally defined within some existing human-readable policy document, the class schema for that LOA will, rather than try to duplicate the requirements as documented, simply point to the appropriate document (or section within).

The <GoverningAgreements> element within the Authentication Context schema will be used to refer to the LOA documentation.

Therefore, to define class schemas for a set of LOA:

1. Define a URI for each LOA.
2. Determine a URL to an appropriate document (or section) for each LOA (this may be, but does not have to be, the same as the URI in the previous step).
3. Create an XML schema for each LOA:
   a) The schema should redefine the base authentication context types schema (saml-schema-authn-context-types-2.0.xsd) as per the class schemas in the SAML Authentication Context specification.
   b) The schema's target namespace should be the URI from step 1.
   c) The schema should restrict the AuthnContextDeclarationBaseType complex type so that only a single <GoverningAgreements> element, with no other children, is allowed.
   d) The value of the governingAgreementRef should be fixed to point to the corresponding URL from step 2.

2.2 Example

To demonstrate how the above model might be used in practice, we show here a class schema for a fictional FAF (Foo Assurance Framework) with three different levels of assurance. The 3 LOA will each have a corresponding schema, each referencing the appropriate section of the FAF documentation.

We define the following URIs to represent the 3 LOA
The schema for LOA1 might look like:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
  targetNamespace="http://foo.example.com/assurance/loa1"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="http://foo.example.com/assurance/loa1"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">
  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">
    <xs:annotation>
      <xs:documentation>
        Class identifier: http://foo.example.com/assurance/loa1
      </xs:documentation>
      Defines Level 1 of FAF
    </xs:annotation>
    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="GoverningAgreements"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>
    <xs:complexType name="GoverningAgreementRefType">
      <xs:complexContent>
        <xs:restriction base="GoverningAgreementRefType">
          <xs:attribute name="governingAgreementRef" type="xs:anyURI" fixed="http://foo.example.com/assurance.pdf#section1" use="required"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>
  </xs:redefine>
</xs:schema>
```
3 Identity Assurance Certification Attribute Profile

This profile defines a SAML attribute to represent the certification status of an Identity Provider regarding its conformance to the requirements of an identity assurance framework.

3.1 Required Information


Contact Information: security-services-comment@lists.oasis-open.org

Description: Given below.

Updates: None.

3.2 Profile Overview

In some relatively simple scenarios where identity assurance is used, a relying party may have a direct business relationship with an organization operating an Identity Provider that satisfies the relying party that the practices of the Identity Provider conform to the requirements of an assurance framework. In a larger-scale scenario, a relying party may wish to rely on a third party (a "certification service") to certify the practices of the Identity Provider organization. In this scenario, it is useful for the IdP's certification status as determined by that certification service to be represented in a standard fashion, in a way that can be communicated securely among the various parties involved. The SAML Metadata specification [SAMLMeta] defines a means for information about SAML entities to be represented and communicated securely.

This profile defines a SAML attribute that can be applied to entities in a SAML metadata instance to express certification status. To indicate that an Identity Provider (or group of Identity Providers) is certified as conformant with an LOA, the attribute defined in this profile is added to that Identity Provider's <md:EntityDescriptor> element (or a parent <md:EntitiesDescriptor> element) using the <attr:EntityAttributes> extension element defined in [SAMLMA]. This extension permits the use of a <saml:Attribute> element alone, or its inclusion within an <saml:Assertion> element. A <saml:Assertion> element can be used to include an assurance certification attribute that is signed independently from the enclosing metadata.

3.3 SAML Attribute Naming


This profile defines a single SAML attribute name:


3.4 Profile-Specific XML Attributes

No additional XML attributes are defined for use with this attribute.

3.5 SAML Attribute Values

Values of this attribute are URIs representing LOAs as suggested in section 2 of this document. Multiple values MAY be present. This document does not define any relationship between LOAs or define relying party behavior if specific value(s) are, or are not, present. It is the responsibility of assurance framework
documentation to specify whether, for example, certification at a “higher” LOA implies approval to assert a “lower” LOA.

### 3.6 Example

In this example a metadata publisher places the `<saml:Attribute>` element in the IdP’s `<md:EntityDescriptor>` to indicate that the practices of the IdP have been certified as conformant with the requirements of the stated LOA. A party relying on this metadata could use this value as input to policy as to whether to accept SAML authentication assertions from this IdP.

```xml
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
                  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
                  xmlns:attr="urn:oasis:names:tc:SAML:metadata:attribute"
                  xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
                  entityID="https://IdentityProvider.example.com/SAML">
  <Extensions>
    <attr:EntityAttributes>
      <saml:Attribute
        NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
        Name="urn:oasis:names:tc:SAML:attribute:assurance-certification">
        <saml:AttributeValue>
          http://foo.example.com/assurance/loa1
        </saml:AttributeValue>
      </saml:Attribute>
    </attr:EntityAttributes>
  </Extensions>
</EntityDescriptor>
```
4 Conformance

4.1 Identity Assurance Certification Attribute Profile Conformance

An metadata publisher conforms to this profile if it can generate SAML metadata instances containing the SAML attribute defined in section 3.

A metadata consumer (typically a relying party) conforms to this profile if it can process the SAML attribute defined in section 3 and make the results available for further processing.

All parties must also meet the conformance requirements in [SAMLMA].
Appendix A. Acknowledgments

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

- TBD
Appendix B. Revision History

- Draft 01 – first draft of sstc-saml-loa-authncontext-profile
- Draft 02 - minor tweaks to text. Removed editorial comments. Removed example class derived from base class.
- Draft 03 – removed the NIST 800 63 specific references and schema.
- Draft 00 sstc-saml-assurance-profile: renamed to reflect added material. Added certification motivation and specification.
- Draft 01 sstc-saml-assurance-profile: added attribute profile conformance, added attribute profile example, more description of certification usage, reorganized section numbering, put conformance material in section 1.
- Committee Draft 01, cosmetic edits.
- Draft 02 sstc-saml-assurance-profile: authncontext pieces reworked as guidelines rather than profile, editorial pass
- Committee Draft 02, editorial process changes only