Level of Assurance Authentication Context Profiles for SAML 2.0

Working Draft 02

1824 March 2009

01 July 2008

Specification URIs:

This Version:
http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-loa-authncontext-profile-draft-02.html
http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-loa-authncontext-profile-draft-02.odt
http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-loa-authncontext-profile-draft-02.pdf

Previous Version:
http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-loa-authncontext-profile-draft-01.html
http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-loa-authncontext-profile-draft-01.odt
http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-loa-authncontext-profile-draft-01.pdf

Technical Committee:
OASIS Security Services[official name of technical committee] TC

Chair(s):
Hal Lockhart, BEA Systems, Inc.
Brian Campbell, Ping Identity Corporation

Editor(s):
Eric Tiffany, Liberty Alliance
Paul Madsen, NTT
Scott Cantor, Internet2

Related Work:
This specification profiles the SAML 2.0 Authentication Context [SAMLAC] mechanisms to allow SAML authentication requests and assertions to carry assurance policy information. Specifically, we profile SAML's Authentication Context for NIST 800-63 is a profile of the SAML 2.0 Authentication Context specification [SAMLAC].

Declared XML Namespace(s):

Abstract:

This document profiles the use of SAML’s Authentication Context mechanisms to express assurance policy on authentication requests and assertions. Level-of-Assurance (LOA) schemes are expressed as a set of authentication context classes. A general schema pattern for arbitrary assurance frameworks is presented, along with specific authentication classes corresponding to profile reduces the scope of the mechanisms described in the full Authentication Context specification so as to provide a simplified way of representing a Level of Assurance (LOA) authentication scheme. A general schema restriction is presented, along with specific examples implementing the NIST 800-63 levels of assurance [NIST 800-63].

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 .................................................................................................................. 6
   1.4 Normative References ................................................................................................. 6
   1.5 Non-normative References ......................................................................................... 7

2 General Level-of-Assurance Profile ....................................................................................... 8

3 NIST 800-63 LOA Using SAML LOA Profile ......................................................................... 9
   3.1 NIST 800-63 Level 1 Schema ...................................................................................... 9
   3.2 NIST 800-63 Level 2 Schema ...................................................................................... 9
   3.3 NIST 800-63 Level 3 Schema ..................................................................................... 10
   3.4 NIST 800-63 Level 4 Schema ..................................................................................... 11

4 SAML LOA Profile Conformance ........................................................................................... 12
   4.1 NIST 800-63 LOA Profile Conformance ..................................................................... 12
1 Introduction

The Level of Assurance Authentication Context Profiles for SAML 2.0 describes two profiles of the SAML Authentication Context [SAMLAC] specification:

- A general, restricted version of the AuthnContext schema that may be used as the basis for representing levels of assurance (or other abstract authentication models) defined by external documentation of any given assurance framework.
- A specific set of AuthnContext_class schema derived from the general case which corresponds to the 4 NIST 800 63_class schema derived from the general case which implements the [NIST 800-63] levels of assurance.

1.1 Motivation [Non-Normative]

Many existing (and potential) SAML federation deployments have adopted a “levels of assurance” (or LOA) model for categorizing the large number of possible combinations of registration processes, security procedures, and authentication methods that underly a given authentication statement. LOA serve to compress this large number into a smaller more manageable number of levels. Different combinations of processes and technology are rated according to the level of assurance they can engender. Typically, 3-5 sets are defined, with corresponding assurance level ranging from low to high. Relying parties then decide which level of assurance is required to access specific protected resources, based on an assessment of the risk associated with those resources – high risk requires high assurance etc wide variety of authentication methods into a small number of levels, typically based on some notion of the strength of the authentication. Federation members (service providers or “relying parties”) then decide which level of assurance is required to access specific protected resources, based on some assessment of “value” or “risk”.

The SAML authentication context mechanisms provide a variety of possible options for representing the details of a LOA scheme. However, this profile is motivated by two related considerations:

- The SAML authentication context scheme is comprehensive, but quite complex. Deployers find that this complexity is a barrier to designing authentication contexts that match their LOA requirements.
- Representing the details of a LOA scheme using the full expressiveness of the authentication context schema results in XML documents that must be passed in-band with authentication events and parsed by SAML implementations. In most cases, the processing requirements are not sustainable and interoperability issues have not been explored.

The approach taken here simply represents each level in a LOA scheme as a separate authentication context class. Each level class is characterized by a URI, and the body of the schema simply contains a reference to the external documentation that defines the LOA scheme. These URI values are conveyed in the <RequestedAuthnContext> element of an authentication request and the <AuthnContextClassRef> element in the assertion within any authentication response

1.2 Limitations [Non-Normative]

A limitation to using this approach is that there are at least two limitations to using this approach:

- The URIs representing the levels must be configured into every system in the deployment, and the ordering of the URI levels must be decided and configured out-of-band.
The authentication assertions carrying these LOA authentication context URIs do not convey any details about the authentication event, although such details are implied by the level indicated by the URI.

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>ds:</td>
<td><a href="http://www.w3.org/2000/09/xmldsig#">http://www.w3.org/2000/09/xmldsig#</a></td>
<td>This is the XML Signature namespace Error: Reference source not found.</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

[Reference] [reference citation]
[Reference] [reference citation]
2 General Level-of-Assurance Profile

The following schema redefines the basic abstract `AuthnContextDeclarationBaseType` to limit the allowed elements to the `GoverningAgreements` element. It will be through this element that the appropriate external LOA scheme documentation will be referenced.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
  finalDefault="extension"
  blockDefault="substitution" version="2.0">
  <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">
    <xs:annotation>
      <xs:documentation>
        Base class for building level-of-assurance style AuthnContext class definitions.
      </xs:documentation>
    </xs:annotation>
    <xs:complexType name="AuthnContextDeclarationBaseType">
      <xs:complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="Identification" minOccurs="0" maxOccurs="0"/>
            <xs:element ref="TechnicalProtection" minOccurs="0" maxOccurs="0"/>
            <xs:element ref="OperationalProtection" minOccurs="0" maxOccurs="0"/>
            <xs:element ref="AuthnMethod" minOccurs="0" maxOccurs="0"/>
            <xs:element ref="GoverningAgreements" minOccurs="1" maxOccurs="1"/>
            <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
          </xs:sequence>
          <xs:attribute name="ID" type="xs:ID" use="optional"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>
  </xs:redefine>
</xs:schema>
```

The functional definition of the `GoverningAgreementRefType` is not changed from the original schema in [SAMLAC], but documentation is added to serve as a reminder that definitions derived from this schema should redefine `GoverningAgreementRefType` to suit a particular LOA purpose.
2.1 Example-Derived Class

The following schema is based on the general LOA schema above, and further constrains the governing agreements to be limited to an enumerated set of references:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema

targetNamespace="urn:oasis:loa:example"
 xmlns="http://www.w3.org/2001/XMLSchema"
 xmlns:oas="urn:oasis:loa:example"
 finalDefault="extension"
 blockDefault="substitution"
 version="2.0">

<xs:redefine schemaLocation="saml-schema-authn-context-loa-profile.xsd">

<xs:annotation>
 <xs:documentation>
 Class identifier: urn:oasis:loa:example
 </xs:documentation>
 </xs:annotation>

<xs:complexType name="GoverningAgreementRefType">
 <xs:complexContent>
  <xs:restriction base="GoverningAgreementRefType">
   <xs:attribute name="governingAgreementRef"
    use="required">
    <xs:simpleType>
     <xs:restriction base="xs:anyURI">
      <xs:enumeration
       value="http://example.com/loa-1.pdf"/>
      <xs:enumeration
       value="http://example.com/loa-2.pdf"/>
     </xs:restriction>
   </xs:simpleType>
  </xs:restriction>
 </xs:complexContent>
</xs:complexType>
</xs:redefine>
```

---

OASIS® 2008. All Rights Reserved.

Copyright © OASIS® 2008. All Rights Reserved.

Page 9 of 17
3 NIST 800-63 LOA Using SAML LOA Profile

The [NIST 800-63] LOA class schemas will extend the base LOA class schema. Each of the 4 NIST LOA class schemas will reference a particular section of the NIST 800063 document that stipulates the LOA requirements. We define the following URIs to represent the four levels of assurance described in [NIST 800-63].

We define the following URIs to represent the four levels of assurance:


The above URIs correspond to the class schema in the respective following sections. Each class schema extends the base LOA profile schema list of following schema define these URIs using the SAML LOA Profile described in section 2.

3.1 NIST 800-63 Level 1 Schema

Editors Note: it occurs to me that these schema might also be represented as AuthenticationContextDeclaration instances, based on a class defined with an enumeration such as the example above. One might also employ an extension to explicitly indicate the numeric level as an integer. I welcome comments as to whether this alternative approach should be presented.

3.2 Level 1 Schema

```xml
<xs:schema
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    finalDefault="extension"
    blockDefault="substitution"
    version="2.0">
    <xs:redefine schemaLocation="saml-schema-authn-context-loa-profile.xsd">
        <xs:annotation>
            <xs:documentation>
                Class identifier:
                Document identifier:
                saml-schema-authn-context-nist-level1.xsd
                Defines Level 1 of NIST LOA scheme.
                See Section 8.2.1 of SP800-63V1_0_2.pdf (URL below)
            </xs:documentation>
        </xs:annotation>
    </xs:redefine>
</xs:schema>
```
3.3 **NIST 800-63 Level 2 Schema**

```xml
<xs:complexType name="GoverningAgreementRefType">
  <xs:complexContent>
    <xs:restriction base="GoverningAgreementRefType">
      <xs:attribute name="governingAgreementRef" type="xs:anyURI" fixed="http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf" use="required"/>
    </xs:restriction>
  </xs:complexContent>
</xs:complexType>
```

3.4 **NIST 800-63 Level 3 Schema**

```xml
<xs:complexType name="GoverningAgreementRefType">
  <xs:complexContent>
    <xs:restriction base="GoverningAgreementRefType">
      <xs:attribute name="governingAgreementRef" type="xs:anyURI" fixed="http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf" use="required"/>
    </xs:restriction>
  </xs:complexContent>
</xs:complexType>
```
3.5 NIST 800-63 Level 4 Schema

```xml
<?xml version="1.0" encoding="UTF-8"?>
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">
  <xs:redefine schemaLocation="saml-schema-authn-context-loa-profile.xsd">
    <xs:annotation>
      <xs:documentation>
        Class identifier:
        Document identifier:
        saml-schema-authn-context-nist-level4.xsd
        Defines Level 4 of NIST LOA scheme.
        See Section 8.2.4 of SP800-63V1_0_2.pdf (URL below)
      </xs:documentation>
    </xs:annotation>
    <xs:complexType name="GoverningAgreementRefType">
      <xs:complexContent>
        <xs:restriction base="GoverningAgreementRefType">
          <xs:attribute name="governingAgreementRef" type="xs:anyURI" fixed="http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf" use="required"/>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>
  </xs:redefine>
</xs:schema>
```

Copyright © OASIS® 2008. All Rights Reserved.
<xs:restriction
    use="required"/>
</xs:restriction>
</xs:complexType>
</xs:redefine>
</xs:schema>
4 SAML LOA Profile Conformance

To conform to this profile, implementations MUST implement the provisions of sections 3.3.2.2.1 of [SAMLCore] concerning the processing of `<RequestedAuthnContext>`.

4.1 NIST 800-63 LOA Profile Conformance

To conform to the NIST 800-63 LOA profile, implementations MUST understand the URIs described in section 3, and MUST process these according to their relative ordering, where level 1 is weakest and level 4 is strongest.

Editors Note: We may want to add additional conformance clauses describing the specific SAML Bindings and other settings (e.g., encryption and signing) that must be used for each of the levels. This is described in the NIST document, but a concise statement here might be beneficial.
Appendix A. Acknowledgments

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

Participants:

- [Participant name, affiliation | Individual member]
- [Participant name, affiliation | Individual member]
- [Participant name, affiliation | Individual member]
Appendix B. Revision History

- Draft 01 – first draft
- Draft 02 - minor tweaks to text. Removed editorial comments. Removed example class derived from base class.

[optional; should not be included in OASIS standards]
Appendix C. Non-Normative Text