Level of Assurance Authentication Context Profile for SAML 2.0

Working Draft 03

11 May 2009

Specification URIs:

This Version:

http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-loa-authncontext-profile-draft-03.html

http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-loa-authncontext-profile-draft-03.odt

http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-loa-authncontext-profile-draft-03.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 TC

Chair(s):

Hal Lockhart, BEA Systems, Inc.

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.

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 by which assurance levels for arbitrary assurance frameworks can be expressed is presented.

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.

Notices

All capitalized terms in the following text have the meanings assigned to them in the OASIS Intellectual Property Rights Policy (the "OASIS IPR Policy"). The full Policy may be found at the OASIS website.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published, and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this section are included on all such copies and derivative works. However, this document itself may not be modified in any way, including by removing the copyright notice or references to OASIS, except as needed for the purpose of developing any document or deliverable produced by an OASIS Technical Committee (in which case the rules applicable to copyrights, as set forth in the OASIS IPR Policy, must be followed) or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and OASIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY OWNERSHIP RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

OASIS requests that any OASIS Party or any other party that believes it has patent claims that would necessarily be infringed by implementations of this OASIS Committee Specification or OASIS Standard, to notify OASIS TC Administrator and provide an indication of its willingness to grant patent licenses to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification.

OASIS invites any party to contact the OASIS TC Administrator if it is aware of a claim of ownership of any patent claims that would necessarily be infringed by implementations of this specification by a patent holder that is not willing to provide a license to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification. OASIS may include such claims on its website, but disclaims any obligation to do so.

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' procedures with respect to rights in any document or deliverable produced by an OASIS Technical Committee can be found on 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 implementers or users of this OASIS Committee Specification or OASIS Standard, can be obtained from the OASIS TC Administrator. OASIS makes no representation that any information or list of intellectual property rights will at any time be complete, or that any claims in such list are, in fact, Essential Claims.

The names "OASIS", [insert specific trademarked names, abbreviations, etc. here] are trademarks of OASIS, the owner and developer of this specification, and should be used only to refer to the organization and its official outputs. OASIS welcomes reference to, and implementation and use of, specifications, while reserving the right to enforce its marks against misleading uses. Please see http://www.oasis-open.org/who/trademark.php for above guidance.

Table of Contents

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.

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.

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:

- 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.

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:

Prefix	XML Namespace	Comments
`ds:`	http://www.w3.org/2000/09/xmldsig#	This is the XML Signature namespace .
`xs:`	http://www.w3.org/2001/XMLSchema	This namespace is defined in the W3C XML Schema specification [Schema1]. 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`.

1.4 Normative References

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

[SAMLAC] J. Kemp et al. *Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS SSTC, March 2005. Document ID saml-authn-context-2.0-os. See http://www.oasis-open.org/committees/security/.

[SAMLCore] S. Cantor et al. *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS Standard, March 2005. See http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

[Schema1] H. S. Thompson et al. *XML Schema Part 1: Structures.* World Wide Web Consortium Recommendation, May 2001. See http://www.w3.org/TR/2001/REC-xmlschema-1-20010502/. Note that this specification normatively references [Schema2], listed below.

[Schema2] Paul V. Biron, Ashok Malhotra. *XML Schema Part 2: Datatypes*. World Wide Web Consortium Recommendation, May 2001. See http://www.w3.org/TR/2001/REC-xmlschema-2-20010502/.

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 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:complexType name="GoverningAgreementRefType">
            <xs:annotation>
                <xs:documentation>
                    A specific restriction of this type specifying or
                    enumerating the governing document(s) and/or section
                    within such document(s) that define this particular
                    level of assurance.
                </xs:documentation>
            </xs:annotation>
            <xs:complexContent>
                <xs:restriction base="GoverningAgreementRefType">
                   <xs:attribute name="governingAgreementRef"
                                 type="xs:anyURI"  use="required"/>
                </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.

3 Example LOA Framework classes

We show here a set of LoA classes for a fictional FAF (Foo Assurance Framework) with three different levels of assurance. The 3 LOA schemas will extend the base LOA schema defined above. Each LOA schema will reference the corresponding section of the FAF documentation.

We define the following URIs to represent the 3 LOA

- http://foo.example.com/assurance/loa1
- http://foo.example.com/assurance/loa2
- http://foo.example.com/assurance/loa3

As an example, the schema for the level 1 might look like

```
<?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-loa-profile.xsd">

        <xs:annotation>
            <xs:documentation>
                Class identifier:
                    http://foo.example.com/assurance/loa1

                    Defines Level 1 of FAF
            </xs:documentation>
        </xs:annotation>

        <xs:complexType name="GoverningAgreementRefType">
            <xs:complexContent>
                <xs:restriction base="GoverningAgreementRefType">
                    <xs:attribute name="governingAgreementRef"
type="xs:anyURI"
                        fixed="http://foo.example.com/foo_assurance.pdf#sect
ion1"
                        use="required"/>
                </xs:restriction>
            </xs:complexContent>
        </xs:complexType>
    </xs:redefine>
</xs:schema>
```

The class schemas for the other 2 FAF LOA would refer to the corresponding section of the FAF documentation.

276 # 4

5 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>`.

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.
- Draft 03 – removed the NIST 800 63 specific references and schema.

Appendix C. Non-Normative Text