SAML V2.0 Identity Assurance Profiles, Version 1.0

Committee Draft 01

22 September 2009

Specification URIs:

This Version:

http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-assurance-profile-cd-01.html

http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-assurance-profile-cd-01.odt (Authoritative)

http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-assurance-profile-cd-01.pdf

Previous Version:

N/A

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

Technical Committee:

OASIS Security Services TC

Chair(s):

Hal Lockhart, Oracle Corporation
Thomas Hardjono, MIT Kerberos Consortium

Editor(s):

RL “Bob” Morgan, Internet2
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 information. It relies the features specified in [SAMLMA]to represent information about a SAML entity as a SAML attribute associated with a metadata entry.

Declared XML Namespace(s):

N/A

Abstract:

This document specifies methods of representing assurance information as used in two aspects of SAML. It profiles the use of SAML's Authentication Context mechanisms to express per-authentication assurance information via authentication requests and assertions. Level-of-Assurance (LOA) definitions in Identity Assurance Frameworks are expressed as a set of authentication context classes. The document also specifies a means for representing assurance certification status of entities in SAML metadata.

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 name "OASIS" is a trademark 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

Expressing Identity Assurance in SAML 2.0 provides standard means for parties using SAML to exchange information regarding identity assurance. It defines, as a profile of the SAML Authentication Context [SAMLAC] specification, a restricted version of the AuthnContext schema for representing assurance indicators (sometimes called levels of assurance) defined by external documentation of any given assurance framework. In addition, 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 [LibertyIAF]. 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 a particular such set ("assurance profiles" 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. Relying parties then decide which LOA is required to access specific protected resources, based on an assessment of the risk associated with those resources – high risk requires high assurance, for example – and work with identity providers to ensure that the requirements of that level are met.

Given this interest, it is useful for parties using SAML for federation to express in SAML authentication messages the LOA requested by a relying party, and the LOA that is applicable to an authentication response. The SAML authentication context specification [SAMLAC] defines a variety of options for representing the details of identity management processes and mechanisms. The LOA profile in this document 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 definition 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 LOA in an assurance framework as a separate authentication context class. Each LOA class is characterized by a URI, and the body of the schema simply contains a reference to the external documentation that defines the LOA. These URI values are conveyed in the `<RequestedAuthnContext>` element of an authentication request and the `<AuthnContextClassRef>` element in the assertion within any authentication response.

Another common element in assurance programs is certification. See section 5.2 for background and motivation for expressing assurance certification status in a standard fashion in SAML.

1.2 Limitations [Non-Normative]

A limitation to the LOA profile defined in this document 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
`saml:`	urn:oasis:names:tc:SAML:2.0:assertion	This is the SAML V2.0 assertion namespace defined in the SAML V2.0 core specification [SAMLCore].
`samlp:`	urn:oasis:names:tc:SAML:2.0:protocol	This is the SAML V2.0 protocol namespace defined in the SAML V2.0 core specification [SAMLCore].
`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] OASIS Standard, *Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0,* March 2005. http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf

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

[SAMLMA] OASIS Committee Specification, *SAML V2.0 Metadata Extension for Entity Attributes*. August 2009. http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-attr-cs-01.odt

[SAMLMeta] OASIS Standard, *Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0*, March 2005. http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-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-

197 xmlschema-1-20010502/. Note that this specification normatively references
198 [Schema2], listed below.

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

202 1.5 Non-normative References

203 **[LibertyIAF]** Russ Cutler, ed. Liberty Identity Assurance Framework 1.0, Liberty Alliance
204 Project, 2008.

2 AuthnContext Level-of-Assurance Profile

2.1 Required Information

Identification: urn:oasis:names:tc:SAML:2.0:ac:profiles:assurance

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

Description: Given below.

Updates: None.

2.2 AuthnContext Schema

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 assurance framework 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.

2.3 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.

3 Identity Assurance Certification Attribute Profile

A SAML attribute is defined to represent the certification status of an Identity Provider regarding its conformance to the elements of an identity assurance framework.

3.1 Required Information

Identification: urn:oasis:names:tc:SAML:2.0:attribute:profiles:assurance-certification

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 means for information about SAML entities to be represented and communicated securely.

This profile defines a SAML attribute that can be applied to entries in a SAML metadata document 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 entity metadata as described in [SAMLMA]. This may be done using a `<saml:Attribute>` or a `<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

The `NameFormat` XML attribute in `<Attribute>` elements MUST be `urn:oasis:names:tc:SAML:2.0:attrname-format:uri`.

This profile defines a single SAML attribute name:

`urn:oasis:names:tc:SAML:attribute:assurance-certification`

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 defined 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 multiple values are 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 would place the SAML attribute statement in the IdP's entity descriptor to indicate that the practices of the indicated IdP had been certified as conformant with the requirements of the stated LOA. A party relying on this metadata could use this value as part of determining whether and how to accept SAML authentication assertions from this IdP.

```
<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>
    <IDPSSODescriptor WantAuthnRequestsSigned="true"
       protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
      <KeyDescriptor use="signing"> ... </KeyDescriptor>
      <NameIDFormat>...</NameIDFormat>
      <SingleSignOnService
        Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
        Location="https://IdentityProvider.example.com/SAML/SSO/Browser"/>
      ...
    </IDPSSODescriptor>
    ...
</EntityDescriptor>
```

4 Conformance

4.1 AuthnContext Level-of-Assurance Profile Conformance

To conform to this profile, implementations MUST support the use of the `<samlp:RequestedAuthnContext>` and `<saml:AuthnContext>` elements defined by [SAMLCore].

4.2 Identity Assurance Certification Attribute Profile Conformance

An asserting party (typically, a metadata publisher) conforms to this profile if it can generate valid SAML instances containing the SAML attribute defined in this profile.

A relying party (typically, a metadata consumer) conforms to this profile if it can process the SAML attribute defined in this profile 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:

- Rob Philpott, EMC Corporation
- Richard Franck, IBM
- John Bradley, Individual
- Scott Cantor, Internet2
- Nate Klingenstein, Internet2
- RL "Bob" Morgan, Internet2
- Thomas Hardjono, M.I.T.
- Tom Scavo, National Center for Supercomputing Applications (NCSA)
- Frederick Hirsch, Nokia Corporation
- Paul Madsen, NTT Corporation
- Ari Kermaier, Oracle Corporation
- Hal Lockhart, Oracle Corporation
- Anil Saldhana, Red Hat
- Kent Spaulding, Skyworth TTG Holdings Limited
- Duane DeCouteau, Veterans Health Administration
- David Staggs, Veterans Health Administration

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, cosmetic edits.