Subject-based Profiles for SAML V1.1 Assertions

Working Draft 03

23 March 2008

Specification URIs:

This Version:
- http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml1-profiles-assertion-subject-draft-03.html
- http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml1-profiles-assertion-subject-draft-03.odt
- http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml1-profiles-assertion-subject-draft-03.pdf
- http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml1-profiles-assertion-subject.xsd

Previous Version:
- http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml1-profiles-assertion-subject-draft-02.html
- http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml1-profiles-assertion-subject-draft-02.odt
- http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml1-profiles-assertion-subject.xsd

Latest Version:
- http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml1-profiles-assertion-subject.html
- http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml1-profiles-assertion-subject.odt
- http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml1-profiles-assertion-subject.xsd

Technical Committee:
- OASIS Security Services TC

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

Editor(s):
- Tom Scavo, National Center for Supercomputing Applications (NCSA)

Related Work:
- NA

Declared XML Namespace(s):
Abstract:
This profile places constraints upon SAML V1.1 subjects and assertions so that they have properties similar to SAML V2.0 subjects and assertions.

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 Terminology................................................................................................................................. 5  
1.2 Outline........................................................................................................................................... 6  
1.3 Normative References.................................................................................................................. 6  
1.4 Non-Normative References.......................................................................................................... 7  
2 SAML V1.1 Subject Profile............................................................................................................... 8  
2.1 Required Information...................................................................................................................... 8  
2.2 Profile Description.......................................................................................................................... 8  
2.3 Usage of `<saml:Subject>` Element............................................................................................. 8  
2.4 Example.......................................................................................................................................... 8  
2.5 Strongly Matching Subjects.......................................................................................................... 9  
3 SAML V1.1 Subject-based Assertion Profile.................................................................................... 10  
3.1 Required Information...................................................................................................................... 10  
3.2 Profile Description.......................................................................................................................... 10  
3.3 Usage of `<saml:Assertion>` Element.......................................................................................... 10  
3.4 Example.......................................................................................................................................... 11  
4 SAML V1.1 Extensions..................................................................................................................... 13  
4.1 Complex type SubjectStatementType......................................................................................... 13  
5 Implementation Conformance.......................................................................................................... 14  
6 Acknowledgments............................................................................................................................. 15  
7 Revision History............................................................................................................................... 16  

1 Introduction

The Subject-based Profiles for SAML V1.1 Assertions specifies two profiles:

- SAML V1.1 Subject Profile
- SAML V1.1 Subject-based Assertion Profile

The primary goal of the SAML V1.1 Subject-based Assertion Profile (which relies on the SAML V1.1 Subject Profile) is to provide guidance to deployments that support both SAML V1.1 and V2.0. In that case, there is some flexibility in SAML V1.1 that is not present in SAML V2.0 (and vice versa). This profile places constraints upon SAML V1.1 subjects and assertions so that they have properties similar to SAML V2.0 subjects and assertions. This may aid interoperability and speed the ultimate transition from SAML V1.1 to SAML V2.0.

An implementation of the SAML V1.1 Web Browser SSO Profile is very likely conformant to this profile. Other applications of SAML may not be conformant, however. For example, the Web Services Security SAML Token Profile [WSSSAML] provides for both SAML V1.1 and SAML V2.0 tokens. Due to differences between the two versions of SAML [SAMLDiffs], an implementation that wished to support both would tend to constrain the tokens such that they exhibited an equivalent semantic. This profile provides one such set of constraints.

A major difference between SAML V1.1 and SAML V2.0 is that the latter elevates the `<saml2:Subject>` element to be a child element of the `<saml2:Assertion>` element, and therefore the `<saml2:Subject>` element applies to all the statements in the assertion. In SAML V1.1, on the other hand, each statement has its own `<saml:Subject>` element, which opens the door to a wide range of possibilities. This profile constrains SAML V1.1 assertions so that each statement contains an equivalent `<saml:Subject>` element. Formally, this is done by extending the notion of strongly matches to an equivalence relation, which culminates in section 3.3.

1.1 Terminology

This specification uses normative text to describe the contents of conforming SAML subjects and assertions.

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 [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>saml:</td>
<td>urn:oasis:names:tc:SAML:1.1:assertion</td>
<td>This is the SAML V1.1 assertion namespace [SAMLCore].</td>
</tr>
<tr>
<td>saml2:</td>
<td>urn:oasis:names:tc:SAML:2.0:assertion</td>
<td>This is the SAML V2.0 assertion namespace [SAML2Core].</td>
</tr>
<tr>
<td>Prefix</td>
<td>XML Namespace</td>
<td>Comments</td>
</tr>
<tr>
<td>---------</td>
<td>--------------------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>samlsap</td>
<td>urn:oasis:names:tc:SAML:1.1:profiles:assertion:subject</td>
<td>This is the SAML V1.1 subject-based assertion namespace defined by this document and its accompanying schema [SAMLSAP-XSD].</td>
</tr>
<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 W3C XML Signature namespace, defined in the XML-Signature Syntax and Processing specification [XMLSig] and schema [XMLSig-XSD].</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 is the XML Schema namespace [Schema1]. This is the default namespace used throughout this document.</td>
</tr>
<tr>
<td>xsi</td>
<td><a href="http://www.w3.org/2001/XMLSchema-instance">http://www.w3.org/2001/XMLSchema-instance</a></td>
<td>This is the XML Schema namespace for schema-related markup that appears in XML instances [Schema1].</td>
</tr>
</tbody>
</table>

This specification uses the following typographical conventions in text: <UnqualifiedElement>, <ns:QualifiedElement>, Attribute, Datatype, OtherKeyword.

1.2 Outline

Section 2 describes a profile that constrains SAML V1.1 subjects so that they have properties similar to SAML V2.0 subjects. Section 3 describes a profile that places constraints upon SAML V1.1 assertions so that they have properties similar to SAML V2.0 assertions. Section 4 describes a SAML V1.1 extension that provides a SAML V2.0 capability not present in SAML V1.1. Finally, section 5 specifies requirements that all conforming implementations must follow.

1.3 Normative References


1.4 Non-Normative References


2 SAML V1.1 Subject Profile

This SAML V1.1 Subject Profile constrains SAML V1.1 subjects so that they have properties similar to SAML V2.0 subjects.

2.1 Required Information


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

Description: Given below.

Updates: N/A

Extends: N/A

2.2 Profile Description

This profile specifies a SAML V1.1 <saml:Subject> element that can be readily mapped to SAML V2.0.

2.3 Usage of <saml:Subject> Element

Neither SAML V1.1 nor SAML V2.0 explicitly requires a name identifier, but certain SAML V2.0 profiles (most notably the Single Logout Profile) implicitly require one, so a <saml:Subject> element that conforms to this profile SHOULD contain a <saml:NameIdentifier> element. To further align with SAML V2.0, the NameQualifier attribute on the <saml:NameIdentifier> element SHOULD be omitted unless the identifier’s type definition explicitly defines its use and semantics. In particular, if the Format attribute on the <saml:NameIdentifier> element has a value specified in section 7.3 of [SAMLCore], the NameQualifier attribute SHOULD be omitted.

Certain deprecated features of SAML V1.1 were removed in SAML V2.0. Thus a <saml:Subject> that conforms to this profile MUST NOT contain a <saml:NameIdentifier> element with any of the following Format attribute values:

- urn:oasis:names:tc:SAML:1.0:assertion#emailAddress
- urn:oasis:names:tc:SAML:1.0:assertion#X509SubjectName
- urn:oasis:names:tc:SAML:1.0:assertion#WindowsDomainQualifiedName

See section 7.3 of [SAMLCore] for the URIs to be used in lieu of these deprecated values.

In SAML V1.1, a <saml:Subject> element contains at most one <saml:SubjectConfirmation> element containing one or more <saml:ConfirmationMethod> elements. In SAML V2.0, on the other hand, there may be multiple <saml2:SubjectConfirmation> elements, each with a required Method attribute. Therefore, a <saml:Subject> element that conforms to this profile MAY contain a <saml:SubjectConfirmation> element, but that element MUST contain one and only one <saml:ConfirmationMethod> element.

2.4 Example

<!-- SAML V1.1 Subject -->
<saml:Subject>
  <saml:NameIdentifier Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
    C=US, O=NCSA-TEST, OU=User, CN=trscavo@uiuc.edu
  </saml:NameIdentifier>
</saml:Subject>
2.5 Strongly Matching Subjects

In general, the notion of strongly matches defined in section 3.4.4 of [SAMLCore] is overly restrictive, for at least two reasons: 1) a <saml:NameIdentifier> element with no Format attribute is semantically equivalent to a <saml:NameIdentifier> element with Format equal to "urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified", and 2) a <saml:SubjectConfirmation> element with confirmation method "urn:oasis:names:tc:SAML:1.0:cm:holder-of-key" must have a <ds:KeyInfo> element, but two distinct <ds:KeyInfo> elements can refer to the same key so two distinct <saml:SubjectConfirmation> elements can be semantically equivalent. For these reasons, especially the latter, this profile adopts an alternate definition of strongly matches that more closely aligns with SAML V2.0.

The name identifier parts of the definition of strongly matches in the two versions of SAML are the same if we ignore the language regarding encryption in the SAML V2.0 definition (which of course SAML V1.1 does not support). On the other hand, the subject confirmation part of strongly matches has a distinctly different flavor, so we reformulate the subject confirmation part of strongly matches in SAML V1.1 so that it aligns with SAML V2.0.

Under the assumption that a <saml:SubjectConfirmation> element contains only and only one <saml:ConfirmationMethod> element (section 2.3), we define strongly matches as follows:

A <saml:Subject> element S1 strongly matches S2 if and only if the following two conditions both apply:

- If S2 includes a <saml:NameIdentifier> element, then S1 MUST include an identical <saml:NameIdentifier> element.

- If S2 contains a <saml:SubjectConfirmation> element such that the subject identified by S1 can be confirmed in the manner described by the <saml:SubjectConfirmation> element in S2.

Like the definition of strongly matches in [SAMLCore], the above relation is not symmetric since S1 strongly matches S2 does not imply that S2 strongly matches S1. In other words, the order of operands S1,S2 matters.
3 SAML V1.1 Subject-based Assertion Profile

This SAML V1.1 Subject-based Assertion Profile places constraints upon SAML V1.1 assertions so that they have properties similar to SAML V2.0 assertions.

In SAML V1.1, each statement contains a <saml:Subject> element, but in SAML V2.0, there is one <saml2:Subject> element per assertion. Thus, in SAML V2.0, every statement necessarily applies to the same subject. To achieve an equivalent semantic in SAML V1.1, this profile places suitable restrictions on multi-statement assertions.

See section 2 of the SAML V1.1 Assertions and Protocols specification [SAMLCore] for general requirements regarding SAML assertions. Where this profile conflicts with [SAMLCore], the former takes precedence.

3.1 Required Information


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

Description: Given below.

Updates: N/A

Extends: N/A

3.2 Profile Description

This profile places the following constraints upon conforming assertions:

• Deprecated elements must not be used.
• Each statement of the assertion must have a <saml:Subject> element.
• Each <saml:Subject> element must satisfy the SAML V1.1 Subject Profile described in section 2. Moreover, each pair of <saml:Subject> elements must very strongly match, a notion made precise in the next section.

Such an assertion is called a subject-based assertion.

3.3 Usage of <saml:Assertion> Element

An assertion that conforms to this profile MUST satisfy the following general requirements:

• The assertion MUST NOT contain a <saml:AuthorityBinding> element.
• Every statement in the assertion MUST have a type derived from abstract type saml:SubjectStatementAbstractType [SAMLCore].
• The <saml:Subject> element of each statement MUST satisfy the SAML V1.1 Subject Profile described in section 2.
• If the <saml:Assertion> element contains more than one statement, each pair of <saml:Subject> elements MUST very strongly match, which we now define. Let S1 and S2 be two <saml:Subject> elements. S1 very strongly matches S2 if S1 strongly matches S2 and S2 strongly matches S1. Note that this definition depends on the notion of strongly matches defined in section 2.5.

An assertion is valid according to this profile if and only if it satisfies the above requirements.
3.4 Example

The following SAML assertion was obtained by a principal who authenticated to an identity provider via TLS [RFC2246] client authentication. Note that the `<saml:Subject>` elements in the two statements very strongly match (indeed, the `<saml:Subject>` elements are identical).

```xml
<!-- SAML Assertion for an X.509 Subject -->
<saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
AssertionID="_33776a319493ad607b7ab3e689482e45"
IssueInstant="2006-07-17T20:31:41Z"
Issuer="https://idp.example.org/saml"
MajorVersion="1" MinorVersion="0">
  <!-- assertion lifetime constrained by principal's X.509 cert -->
  <saml:Conditions NotBefore="2006-07-17T20:31:41Z"
                NotOnOrAfter="2006-07-18T20:21:41Z">
  </saml:Conditions>
                                     AuthenticationMethod="urn:ietf:rfc:2246">
    <saml:Subject>
      <saml:NameIdentifier Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
        C=US, O=NCSA-TEST, OU=User, CN=trscavo@uiuc.edu
      </saml:NameIdentifier>
      <saml:SubjectConfirmation>
        <saml:ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:holder-of-key</saml:ConfirmationMethod>
        <ds:KeyInfo>
          <ds:X509Data>
            <ds:X509Certificate>
              MIICiDCCAXACQDE9ieiWrm62jANBgkqhkiG9w0DBAQQAQFDBFMQswCQYDVQQGEwJV
              UzESMBGQA1UEChMJTk3NTQISURVUMQ0wCwYDVQQLEwRVc2VyMRMwEQYDVQQDEwcn
              UCITEXJ2aWN1MB4XDTA2MDCxNzIwMjE0MVowMDEwTjIwMjE0MVowMjE0MjE0MjE0MjE0
              AIUUEhBMCVMVmxzjAQbNVuATCUC5DU0EtVEVTVDENMAgA1UECxMEXVXNiMzE2MdBcG
              AIUUEAwQAHJyZ2F0B1aVxJvlyKvKDCBnANBgkqhkiG9w0BAQEAFAAOBjAwgYkIkC
              qyeAv9QoMq41lRXkxWpcflbcj9G9ty6zBjmp+tsajJNMOVaBaZ3tt+sTXxen1Yife
              ncCc203ya7X6aq53QXMy+5wKQYe8Rzd5S28Nv3a73wJfXJX0uh6qkERccs39EflIwC
              g2hOgbsuhf+Vb3lIhi4I1B75MC52bu5fsR7d1r/xxsadU2RcCaWbAATANBgkqhkiG
              9w0BAQQAFAQAOCAQEAcd7mcWi7b7b7v7f7l7y1t7J7i7j7l0i7321h60d7Pv6c1v6c
              Ejk0Qxkz2KHheZ6+r1i1iX0e21R0J3EssMNxt5D8+wv6p6avoB5EXyL3ez+CEAI14g
              cjvZ2UR4dMryWahW1BHKFU1+7urUgyWII12KbMeE9KP+kiiiiTsKlKgFzngw1lJ
              selm5HtTcTcrDocn5y02+3d0g52E0tFVDsBuvDix02hv679JR6H1qjtk4GExp
              E911V10wPE038uQIJJTX1haMMLvUGVh/c0ReJbn92Vjv4dI/yy6PtY/8ncYLrNkg
              oVNO9j/yMoktn91TlFyTiuY4OuJsZRO1+zWLy9g==
            </ds:X509Certificate>
          </ds:X509Data>
        </ds:KeyInfo>
      </saml:SubjectConfirmation>
    </saml:Subject>
  </saml:AuthenticationStatement>
  <saml:AttributeStatement>
    <saml:Subject>
      <saml:NameIdentifier Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
        C=US, O=NCSA-TEST, OU=User, CN=trscavo@uiuc.edu
      </saml:NameIdentifier>
    </saml:Subject>
  </saml:AttributeStatement>
</saml:AuthenticationStatement>
</saml:Assertion>
```
The attributes in the above example conform to the MACE-Dir Attribute Profile for SAML 1.x [MACEAttrib] and are for illustration purposes only.
4 SAML V1.1 Extensions

SAML V2.0 provides a number of features and capabilities not present in SAML V1.1 [SAML2diffs]. Although backwards compatibility is not a primary goal of this specification, we have found the feature described in the next section to be quite useful, so we include it here for interoperability among SAML V1.1 implementations.

4.1 Complex type SubjectStatementType

Recall that a SAML V1.1 assertion contains at least one statement. SAML V2.0, on the other hand, permits empty assertions, that is, subject-based assertions with no statements. To duplicate this capability in SAML V1.1, we define a trivial extension of saml:SubjectStatementAbstractType:

```xml
<complexType name="SubjectStatementType">
  <complexContent>
    <extension base="saml:SubjectStatementAbstractType"/>
  </complexContent>
</complexType>
```

The following example illustrates a <saml:Assertion> containing a <saml:SubjectStatement> of type samlsap:SubjectStatementType.

```xml
<saml:Assertion
  xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  AssertionID="cT_S_T-vKMwT8_Pzkke8UKC68."
  IssueInstant="2006-07-17T20:31:41Z"
  Issuer="https://idp.example.org/saml"
  MajorVersion="1" MinorVersion="1">
  <saml:Conditions
    NotBefore="2006-07-17T20:31:41Z"
    NotOnOrAfter="2006-07-18T20:21:41Z">  
  </saml:Conditions>
  <saml:SubjectStatement
    xsi:type="samlsap:SubjectStatementType">
    <saml:Subject>
      <saml:NameIdentifier
        Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
        C=US, O=NCSA-TEST, OU=User, CN=trscavo@uiuc.edu
      </saml:NameIdentifier>
    </saml:Subject>
  </saml:SubjectStatement>
</saml:Assertion>
```

Note that the above <saml:SubjectStatement> element has no content apart from a <saml:Subject> element.
5 Implementation Conformance

An entity that produces a `<saml:Subject>` element satisfying the requirements of section 2 is conformant with respect to the SAML V1.1 Subject Profile. Likewise an identity provider that produces a `<saml:Assertion>` element satisfying the requirements of section 3 is conformant with respect to the SAML V1.1 Subject-based Assertion Profile. Such a `<saml:Assertion>` element is said to be valid with respect to this profile.

Note that a `<saml:Subject>` element contained by a `<saml:Assertion>` element that is conformant to the SAML V1.1 Subject-based Assertion Profile is necessarily conformant to the SAML V1.1 Subject Profile since the former depends on the latter. An important consequence of this fact is that a query requester wishing to obtain a valid `<saml:Assertion>` element MUST issue a query containing a conformant `<saml:Subject>` element. Otherwise the identity provider will not be able to meet the requirements of both this profile and section 3.4.4 of [SAMLCore].
6 Acknowledgments

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

- Hal Lockhart, BEA Systems, Inc.
- Rob Philpott, EMC Corporation
- Scott Cantor, Internet2
- Bob Morgan, Internet2
- Tom Scavo, National Center for Supercomputing Applications (NCSA)
- Peter Davis, Neustar, Inc.
- Jeff Hodges, NeuStar, Inc.
- Frederick Hirsch, Nokia Corporation
- Abbie Barbir, Nortel
- Paul Madsen, NTT Corporation
- Ari Kermaier, Oracle Corporation
- Prateek Mishra, Oracle Corporation
- Brian Campbell, Ping Identity Corporation
- Eve Maler, Sun Microsystems
- Emily Xu, Sun Microsystems
- David Staggs, Veteran's Health Administration
- Kent Spaulding, Tripod Technology Group, Inc.
- Anil Saldhana, Red Hat
- Eric Tiffany, Liberty Alliance Project
## 7 Revision History

<table>
<thead>
<tr>
<th>Document ID</th>
<th>Date</th>
<th>Committer</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>sstc-saml1-profiles-assertion-subject-draft-01</td>
<td>17 Dec 2007</td>
<td>T. Scavo</td>
<td>Initial draft</td>
</tr>
<tr>
<td>sstc-saml1-profiles-assertion-subject-draft-02</td>
<td>26 Feb 2008</td>
<td>T. Scavo</td>
<td></td>
</tr>
<tr>
<td>sstc-saml1-profiles-assertion-subject-draft-03</td>
<td>23 Mar 2008</td>
<td>T. Scavo</td>
<td></td>
</tr>
</tbody>
</table>