Subject-based Profiles for SAML V1.1 Assertions

Committee Specification 01

7 October 2008

Specification URIs:

This Version:

http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml1-profiles-assertion-subject-cs-01.html

http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml1-profiles-assertion-subject-cs-01.odt (Authoritative)

http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml1-profiles-assertion-subject-cs-01.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-cd-02.html

http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml1-profiles-assertion-subject-cd-02.odt (Authoritative)

http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml1-profiles-assertion-subject-cd-02.pdf

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.pdf

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):

urn:oasis:names:tc:SAML:1.1:profiles:assertion:subject

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.

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

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:

Prefix	***XML Namespace***	***Comments***
`saml:`	urn:oasis:names:tc:SAML:1.0:assertion	This is the SAML V1.1 assertion namespace [SAMLCore].
`saml2:`	urn:oasis:names:tc:SAML:2.0:assertion	This is the SAML V2.0 assertion namespace [SAML2Core].

Prefix	***XML Namespace***	***Comments***
`samlsap:`	urn:oasis:names:tc:SAML:1.1:profiles:assertion:subject	This is the SAML V1.1 subject-based assertion namespace defined by this document and its accompanying schema [SAMLSAP-XSD].
`ds:`	http://www.w3.org/2000/09/xmldsig#	This is the W3C XML Signature namespace, defined in the XML-Signature Syntax and Processing specification [XMLSig] and schema [XMLSig-XSD].
`xs:`	http://www.w3.org/2001/XMLSchema	This is the XML Schema namespace [Schema1]. This is the default namespace used throughout this document.
`xsi:`	http://www.w3.org/2001/XMLSchema-instance	This is the XML Schema namespace for schema-related markup that appears in XML instances [Schema1].

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

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

[SAML2Core] 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

[SAMLCore] E. Maler et al. *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V1.1*. OASIS Standard, September 2003. Document ID oasis-sstc-saml-core-1.1. See http://www.oasis-open.org/committees/download.php/3406/oasis-sstc-saml-core-1.1.pdf

[SAMLSAP-XSD] *Schema for Subject-based Profiles for SAML V1.1 Assertions*. OASIS, December 2007. Document ID sstc-saml1-profiles-assertion-subject.xsd. See http://www.oasis-open.org/committees/download.php/26573/sstc-saml1-profiles-assertion-subject.xsd

[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/

[XMLSig] D. Eastlake et al. *XML-Signature Syntax and Processing*. World Wide Web Consortium Recommendation, February 2002. See http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/

[XMLSig-XSD] *Schema for XML Signatures*. World Wide Web Consortium Recommendation, February 2002. See http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/xmldsig-core-schema.xsd

1.4 Non-Normative References

[MACEAttrib] S. Cantor et al. *MACE-Dir SAML Attribute Profiles*. Internet2 MACE, April 2006. See http://middleware.internet2.edu/dir/docs/internet2-mace-dir-saml-attributes-200604.pdf

[RFC2246] T. Dierks and C. Allen. *The TLS Protocol Version 1.0*. IETF RFC 2246, January 1999. See http://www.ietf.org/rfc/rfc2246.txt

[SAMLDiffs] *Differences between SAML 2.0 and 1.1*. SAML XML.org. See http://saml.xml.org/differences-between-saml-2-0-and-1-1

[WSSSAML] R. Monzillo et al. *Web Services Security: SAML Token Profile 1.1*. OASIS Standard, 1 February 2006. See http://www.oasis-open.org/committees/download.php/16768/wss-v1.1-spec-os-SAMLTokenProfile.pdf

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

Identification:
`urn:oasis:names:tc:SAML:1.1:profiles:subject`

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:SubjectConfirmation>
    <saml:ConfirmationMethod>
      urn:oasis:names:tc:SAML:1.0:cm:holder-of-key
    </saml:ConfirmationMethod>
    <ds:KeyInfo>
      <ds:X509Data>
        <!-- subject's X.509 cert -->
        <ds:X509Certificate>
MIICiDCCAXACCQDE+9eiWrm62jANBgkqhkiG9w0BAQQFADBFMQswCQYDVQQGEwJV
UzESMBAGA1UEChMJTkNTQS1URVNUMQ0wCwYDVQQLEwRVc2VyMRMwEQYDVQQDEwpT
UC1TZXJ2aWNlMB4XDTA2MDcxNzIwMjE0MVoXDTA2MDcxODIwMjE0MVowSzELMAkG
A1UEBhMCVVMxEjAQBgNVBAoTCU5DU0EtVEVTVDENMAsGA1UECxMEVXNlcjEZMBcG
A1UEAwwQdHJzY2F2b0B1aXVjLmVkdTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkC
gYEAv9QMe4lRl3XbWPcflbCjGK9gty6zBJmp+tsaJINM0VaBaZ3t+tSXknelYife
nCc2O3yaX76aq53QMXy+5wKQYe8Rzdw28Nv3a73wfjXJXoUhGkvERcscs9EfIWcC
g2bHOg8uSh+Fbv3lHih4lBJ5MCS2buJfsR7dlr/xsadU2RcCAwEAATANBgkqhkiG
9w0BAQQFAAOCAQEAdyIcMTob7TVkelfJ7+I1j0LO24UlKvbLzd2OPvcFTCv6fVHx
Ejk0QxaZXJhreZ6+rIdiMXrEzlRdJEsNMxtDW8++sVp6avoB5EX1y3ez+CEAIL4g
cjvKZUR4dMryWshWIBHKFFul+r7urUgvWI12KbMeE9KP+kiiiiTskLcKgFzngw1J
selmHhTcTCrcDocn5yO2+d3dog52vSOtVFDBsBuvDixO2hv679JR6Hlqjtk4GExp
E9iVI0wdPE038uQIJJTXlhsMMLvUGVh/c0ReJBn92Vj4dI/yy6PtY/8ncYLYNkjg
oVN0J/ymOktn9lTlFyTiuY4OuJsZRO1+zWLy9g==
        </ds:X509Certificate>
      </ds:X509Data>
    </ds:KeyInfo>
  </saml:SubjectConfirmation>
</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, then S1 MUST contain 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

Identification:
`urn:oasis:names:tc:SAML:1.1:profiles:assertion:subject`

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).

```
<!-- 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="1">
  <!-- 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>
  <saml:AuthenticationStatement
    AuthenticationInstant="2006-07-17T20:31:41Z"
    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>
            <!-- subject's X.509 cert -->
            <ds:X509Certificate>
MIICiDCCAXACCQDE+9eiWrm62jANBgkqhkiG9w0BAQQFADBFMQswCQYDVQQGEwJV
UzESMBAGA1UEChMJTkNTQS1URVNUMQ0wCwYDVQQLEwRVc2VyMRMwEQYDVQQDEwpT
UC1TZXJ2aWNlMB4XDTA2MDcxNzIwMjE0MVoXDTA2MDcxODIwMjE0MVowSzELMAkG
A1UEBhMCVVMxEjAQBgNVBAoTCU5DU0EtVEVTVDENMAsGA1UECxMEVXNlcjEZMBcG
A1UEAwwQdHJzY2F2b0B1aXVjLmVkdTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkC
gYEAv9QMe4lRl3XbWPcflbCjGK9gty6zBJmp+tsaJINM0VaBaZ3t+tSXknelYife
nCc2O3yaX76aq53QMXy+5wKQYe8Rzdw28Nv3a73wfjXJXoUhGkvERcscs9EfIWcC
g2bHOg8uSh+Fbv3lHih4lBJ5MCS2buJfsR7dlr/xsadU2RcCAwEAATANBgkqhkiG
9w0BAQQFAAOCAQEAdyIcMTob7TVkelfJ7+I1j0LO24UlKvbLzd2OPvcFTCv6fVHx
Ejk0QxaZXJhreZ6+rIdiMXrEzlRdJEsNMxtDW8++sVp6avoB5EX1y3ez+CEAIL4g
cjvKZUR4dMryWshWIBHKFFul+r7urUgvWI12KbMeE9KP+kiiiiTskLcKgFzngw1J
selmHhTcTCrcDocn5yO2+d3dog52vSOtVFDBsBuvDixO2hv679JR6Hlqjtk4GExp
E9iVI0wdPE038uQIJJTXlhsMMLvUGVh/c0ReJBn92Vj4dI/yy6PtY/8ncYLYNkjg
oVN0J/ymOktn9lTlFyTiuY4OuJsZRO1+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:SubjectConfirmation>
        <saml:ConfirmationMethod>
```

```
          urn:oasis:names:tc:SAML:1.0:cm:holder-of-key
        </saml:ConfirmationMethod>
        <ds:KeyInfo>
          <ds:X509Data>
            <!-- subject's X.509 cert -->
            <ds:X509Certificate>
MIICiDCCAXACCQDE+9eiWrm62jANBgkqhkiG9w0BAQQFADBFMQswCQYDVQQGEwJV
UzESMBAGA1UEChMJTkNTQS1URVNUMQ0wCwYDVQQLEwRVc2VyMRMwEQYDVQQDEwpT
UC1TZXJ2aWNlMB4XDTA2MDcxNzIwMjE0MVoXDTA2MDcxODIwMjE0MVowSzELMAkG
A1UEBhMCVVMxEjAQBgNVBAoTCU5DU0EtVEVTVDENMAsGA1UECxMEVXNlcjEZMBcG
A1UEAwwQdHJzY2F2b0B1aXVjLmVkdTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkC
gYEAv9QMe4lRl3XbWPcflbCjGK9gty6zBJmp+tsaJINM0VaBaZ3t+tSXknelYife
nCc2O3yaX76aq53QMXy+5wKQYe8Rzdw28Nv3a73wfjXJXoUhGkvERcscs9EfIWcC
g2bHOg8uSh+Fbv3lHih4lBJ5MCS2buJfsR7dlr/xsadU2RcCAwEAATANBgkqhkiG
9w0BAQQFAAOCAQEAdyIcMTob7TVkelfJ7+I1j0LO24UlKvbLzd2OPvcFTCv6fVHx
Ejk0QxaZXJhreZ6+rIdiMXrEzlRdJEsNMxtDW8++sVp6avoB5EX1y3ez+CEAIL4g
cjvKZUR4dMryWshWIBHKFFul+r7urUgvWI12KbMeE9KP+kiiiiTskLcKgFzngw1J
selmHhTcTCrcDocn5yO2+d3dog52vSOtVFDBsBuvDixO2hv679JR6Hlqjtk4GExp
E9iVI0wdPE038uQIJJTXlhsMMLvUGVh/c0ReJBn92Vj4dI/yy6PtY/8ncYLYNkjg
oVN0J/ymOktn9lTlFyTiuY4OuJsZRO1+zWLy9g==
            </ds:X509Certificate>
          </ds:X509Data>
        </ds:KeyInfo>
      </saml:SubjectConfirmation>
    </saml:Subject>
    <saml:Attribute
      AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri"
      AttributeName="urn:mace:dir:attribute-def:eduPersonPrincipalName">
      <saml:AttributeValue Scope="uiuc.edu">
        trscavo
      </saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute
      AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri"
      AttributeName="urn:mace:dir:attribute-def:givenName">
      <saml:AttributeValue xsi:type="xs:string">
        Tom
      </saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute
      AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri"
      AttributeName="urn:mace:dir:attribute-def:sn">
      <saml:AttributeValue xsi:type="xs:string">
        Scavo
      </saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute
      AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri"
      AttributeName="urn:mace:dir:attribute-def:mail">
      <saml:AttributeValue xsi:type="xs:string">
        trscavo@gmail.com
      </saml:AttributeValue>
    </saml:Attribute>
  </saml:AttributeStatement>
  <ds:Signature>...</ds:Signature>
</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 [SAMLDiffs]. 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**:

```
<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**.

```
<saml:Assertion
  xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
  xmlns:samlsap="urn:oasis:names:tc:SAML:1.1:profiles:assertion:subject"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  AssertionID="cT_S_T-vKMwidT8_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
- Tom Scavo, National Center for Supercomputing Applications (NCSA)
- Jeff Hodges, NeuStar, Inc.
- 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
- Anil Saldhana, Red Hat
- Eric Tiffany, Liberty Alliance Project
- George Fletcher, AOL

7 Revision History

Document ID	***Date***	***Committer***	***Comment***
sstc-saml1-profiles-assertion-subject-draft-01	17 Dec 2007	T. Scavo	Initial draft
sstc-saml1-profiles-assertion-subject-draft-02	26 Feb 2008	T. Scavo	
sstc-saml1-profiles-assertion-subject-draft-03	23 Mar 2008	T. Scavo	
sstc-saml1-profiles-assertion-subject-cd-01	22 Apr 2008	T. Scavo	For Public Review
sstc-saml1-profiles-assertion-subject-cd-02	7 Sep 2008	T. Scavo	Minor typo