How to Study and Learn SAML

Working Draft, 23 October 2006

Document identifier: draft-hodges-HowToLearnSAML-01

Location: http://www.oasis-open.org/committees/security/

Editors: Jeff Hodges, NeuStar, Inc.

Contributors:

Abstract: This brief whitepaper provides a functional introduction to the SAMLv2 specifications. It is tailored to protocol designer and developer’s perspectives. First a conceptual introduction is presented, next suggestions on how to study and learn SAML are given, and then more detailed aspects are discussed.

Status: This is an individual submission.

Committee members should submit comments to the security-services@lists.oasis-open.org list. Others should submit them by following the instructions at http://www.oasis-open.org/committees/comments/form.php?wg_abbrev=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 Intellectual Property Rights web page for the SSTC (http://www.oasis-open.org/committees/security/ipr.php).

[@@Additional template instructions: Give the specification a document ID/filename of the form sstc-saml-descrip[-Vn.m]-{wd|cd}-nn. Sort editor and contributor lists first by affiliation (must be an OASIS institutional member or say “individual”), then by surname. Every time a revision is published, update the revision number and date that appear both on the title page and in the footer, and update the Table of Contents. When a Working Draft becomes a Committee Draft, delete the Revision History appendix and change the first paragraph of the Status section to “This is a Committee Draft approved by the Security Services Technical Committee (SSTC) on month 2006.” The document ID/filename will change as well. Currently, change-tracking is on; reflect any per-revision changes by recording them in this manner.]
## Table of Contents

1 Introduction ........................................................................................................................................... 3  
   1.1 Notation ......................................................................................................................................... 3  
2 Next Section ........................................................................................................................................ 5  
3 New Profile .......................................................................................................................................... 6  
   3.1 Required Information ..................................................................................................................... 6  
4 References ........................................................................................................................................... 7  
5 Revision History .................................................................................................................................... 11  
   Appendix A. Acknowledgements ........................................................................................................ 12  
   Appendix B. Notices ............................................................................................................................ 13
This brief whitepaper provides a functional introduction to the SAMLv2 specifications. It is tailored to protocol designer and developer's perspectives. First a conceptual introduction is presented, next suggestions on how to study and learn SAML are given, and then more detailed aspects are discussed.

### 1.1 Notation

Typographical conventions used in this document are:

- Listings of XML schemas appear like this.
- Example code listings appear like this.

This specification uses the following typographical conventions in text: `<SAMLElement>`, `<ns:ForeignElement>`, Attribute, **Datatype**, OtherKeyword.
2 Conceptual Introduction to SAML

SAML \([\text{SAMLEncOvw}]\) defines an XML-based framework for crafting "security assertions", and exchanging them between entities. In the course of creating, or relying upon such assertions, SAML system entities may use SAML protocols, or other protocols, to convey an assertion itself, or to communicate about the "subject" of an assertion.

Thus one can employ SAML to make statements such as:

"Alice has these profile attributes and her domain's certificate is available over there, and I'm making this statement, and here's who I am."

Then one can cause such an assertion to be conveyed to some party who can then rely on it in some fashion for some purpose, for example input it into a local policy evaluation gating access to some resource.

Such applications of SAML are done in a particular "context of use". A particular context of use could be, for example, deciding whether to accept and act upon a SIP-based invitation to initiate a communication session.

The specification of just how SAML is employed in any given context of use is known as a "SAML profile". The specification of how SAML assertions and/or protocol messages are conveyed in, or over, another protocol is known as a "SAML Binding". Typically, a SAML profile specifies the SAML bindings that may be used in its context. Both SAML profiles and SAML bindings in turn reference other SAML specifications, especially the SAML Assertions and Protocols, aka "SAML Core", specification \([\text{SAMLCore}]\).

This relationship between SAML specifications, as well as SAML-dependent specifications, is illustrated below in Illustration 1: Conceptual Dependencies between SAML Profiles, Bindings, and Core Specifications, as well as Target Protocols. The relationships between the various boxes in the diagrams is one of dependencies. Note how the boxes representing SAML Profiles—this means SAML profile—depends upon both the SAML Core specification as well as SAML Bindings, and of course also upon the specifications of the target profile(s).

Note that the SAML Assertions & Protocols specification, the SAML Core, is conceptually "abstract". It defines the bits and pieces that make up SAML Assertions, and their nominal semantics, but does not define how to actually put them to use in any particular context. That, as we've said, is left to SAML Profiles, of which there can be many.

The original SAML profiles, which concentrate on the problem domain of "Web Single Sign-On", are specified in \([\text{SAMLProf}]\) (note that this specification is called out in the "SAML Profiles" box in Illustration 1: Conceptual Dependencies between SAML Profiles, Bindings, and Core Specifications, as well as Target Protocols). An example of a different, non-Web-SSO SAML profile is given in \([\text{SIP-SAML}]\).
3 How to Study and Learn SAML

Given the gist of the above discussion—that the descriptions of SAML applied in concrete contexts is given in SAML profiles—here is a suggested approach for reading the SAML specification set if one has as their goal “learning SAML”:

- Begin by studying various SAML Profiles, e.g. those given in [[SAMLProf]] and [SIP-SAML]. One will likely find the SAML Technical Overview whitepaper [[SAMLTechOvw]] helpful in this endeavor. It provides a detailed, illustrated expose of several of the SAML Web SSO profiles.
- Only refer to the SAML Core specification [[SAMLCore]] as necessary for definitions and semantics of particular items refered to in the profiles and bindings you are studying.
- Also, refer to the other SAML specifications and documents as necessary:
  - The SAML glossary [[SAMLGloss]] defines many of the key terms used throughout the SAML specification set.
• SAML profiles often reference the SAML Metadata specification [[SAMLMeta]]. This spec defines how one "discovers" various configuration aspects of a SAML deployment. Often one needs to determine this information in order to establish communication.

• The characteristics of specific SAML entity implementations—based upon the profiles in [[SAMLProf]], such as a "SAML Authority", or a "SAML-based service provider"—are given in the SAML Conformance specification [[SAMLConf]].

• Various security aspects of the SAML profiles and bindings given in the SAMLv2 specification set are discussed and analyzed in the SAML Security Considerations specification [[SAMLSec]].

Studying SAML in this fashion is a more concrete, context-rich, practical-application approach than, say, starting cold with reading the rather abstract SAML Core specification.
4 SAML in More Detail

This section first discusses the notion of "SAML assertion profiles", and then follows with a more detailed description of SAML assertions as well as the abstract SAML request/response protocol, both of which are defined in the SAML Core specification [[SAMLCore]].

4.1 SAML Assertion Profiles

There is an additional subtle aspect of SAML profiles that is worth highlighting: the notion of "SAML assertion profiles". A SAML assertion profile is the specification of the specific SAML assertion contents in the context of a particular SAML profile. It is possibly further qualified by a particular implementation and/or deployment context. Two condensed examples of SAML assertion profiles are:

- The SAML assertion must contain at least one authentication statement and no other statements. The relying party must be represented in the <AudienceRestriction> element. The SubjectConfirmation Method must be Foo. etc.
- The SAML assertion must contain at least one attribute statement and may contain more than one. The values for the subject's profile attributes named "Foo" and "Bar" must be present. An authentication statement may be present. etc.

For a more in-depth example of an explicit SAML assertion profile, see section 6.1.4 "Assertion Profile Description" of [SIP-SAML].

Note that all SAML profiles will more or less explicitly encompass one or more assertion profiles. For example, all the SAML profiles specified in [[SAMLProf]] do so, however their "assertion profiles" are not explicitly labeled as such.

4.2 SAML Assertions

A SAML assertion is a package of information including issuer and subject, conditions and advice, and/or attribute statements, and/or authentication statements and/or other statements. Statements may or may not be present. The SAML assertion "container" itself contains the following information:

- **Issuing information**: Who issued the assertion, when was it issued and the assertion identifier.
- **Subject information**: The name of the subject, the security domain and optional subject information, like public key.
- **Conditions under which the assertion is valid**: Special kind of conditions like assertion validity period, audience restriction and target restriction.
- **Additional advice**: Explaining how the assertion was made, for example.

In terms of SAML assertions containing SAML attribute statements or SAML authentication statements, here are explanatory examples:

- With a SAML assertion containing a SAML attribute statement, an issuing authority is asserting that the subject is associated with certain attributes with certain subject profile attribute values. For example, user jon@cs.example.com is associated with the attribute "Department", which has the value "Computer Science".
• With a SAML assertion containing a SAML authentication statement, an issuing authority is asserting that the subject was authenticated by certain means at a certain time.
• With a SAML assertion containing both a SAML attribute statement and a SAML authentication statement, an issuing authority is asserting the union of the above.

Examples of actual SAML assertions are given below in Section 5.

4.3 Abstract Request/Response Protocol

SAML defines an abstract request/response protocol for obtaining assertions. See Section 3 "SAML Protocols" of [[SAMLCore]]. A request asks for an assertion. A response returns the requested assertion or an error. This abstract protocol may then be cast into particular contexts of use by binding it to specific underlying protocols, e.g., HTTP or SIP, and "profiling" it for the specific use case at hand. The SAML HTTP-based web single sign-on profile is one such example (see Section 4.1 Web Browser SSO Profile of [[SAMLProf]]). Trait-based SIP communication session establishment, the topic of this specification, is another.
5 Example SAML Assertions

This section presents two examples of a SAML assertion, one unsigned, the other signed and thus is integrity protected, and attests to the originating author.

In the first example, below, the assertion is attesting with respect to the subject (lines 7-15) "Alice@example.com" (line 11). The validity conditions are expressed in lines 16-23, via both a validity period expressed as temporal endpoints, and an "audience restriction" stating that this assertion's semantics are valid only the relying party named "example2.com". Also, the assertion's issuer is noted in lines 4-5.

In lines 24-36, Alice's telephone number is conveyed, in a "typed" fashion, using LDAP/X.500 schema as the typing means.

```
<Assertion ID="_a75adf55-01d7-40cc-929f-dbd8372ebdfe"
    IssueInstant="2003-04-17T00:46:02Z" Version="2.0"
    xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
    <Issuer>
        example.com
    </Issuer>
    <Subject>
        <NameID
            Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress">
            Alice@example.com
        </NameID>
        <SubjectConfirmation
            Method="urn:oasis:names:tc:SAML:2.0:cm:sender-vouches"/>
    </Subject>
    <Conditions NotBefore="2003-04-17T00:46:02Z"
                NotOnOrAfter="2003-04-17T00:51:02Z">
        <AudienceRestriction>
            <Audience>
                example2.com
            </Audience>
        </AudienceRestriction>
    </Conditions>
    <AttributeStatement>
        <saml:Attribute
            xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute"
            NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
            Name="urn:oid:2.5.4.20"
            FriendlyName="telephoneNumber">
            <saml:AttributeValue xsi:type="xs:string">
                +1-888-555-1212
            </saml:AttributeValue>
        </saml:Attribute>
    </AttributeStatement>
</Assertion>
```

Example 1: Unsigned SAML Assertion Illustrating Conveyance of Subject Attribute

In the second example, below, the information described above is the same, the addition is that this version of the assertion is signed. All the signature information is conveyed in the <ds:Signature> element, lines 7-47. Thus this assertion's origin and its integrity are assured. Since this assertion is the same as the one in the first example above, other than having a signature added, the second example below addresses the same Security Considerations aspects, plus those requiring a Signature.

```
<Assertion ID="_a75adf55-01d7-40cc-929f-dbd8372ebdfe"
    IssueInstant="2003-04-17T00:46:02Z" Version="2.0"
    xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
    <Issuer>
        example.com
    </Issuer>
    <Subject>
        <NameID
            Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress">
            Alice@example.com
        </NameID>
        <SubjectConfirmation
            Method="urn:oasis:names:tc:SAML:2.0:cm:sender-vouches"/>
    </Subject>
    <Conditions NotBefore="2003-04-17T00:46:02Z"
                NotOnOrAfter="2003-04-17T00:51:02Z">
        <AudienceRestriction>
            <Audience>
                example2.com
            </Audience>
        </AudienceRestriction>
    </Conditions>
    <AttributeStatement>
        <saml:Attribute
            xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute"
            NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
            Name="urn:oid:2.5.4.20"
            FriendlyName="telephoneNumber">
            <saml:AttributeValue xsi:type="xs:string">
                +1-888-555-1212
            </saml:AttributeValue>
        </saml:Attribute>
    </AttributeStatement>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        ...
    </ds:Signature>
</Assertion>
```
Example 2: Signed SAML Assertion Illustrating Conveyance of Subject Attribute
6 References

6.1 Informative References


7 Revision History

Along with the title page and footer, update this table every time you publish. In general, people will want you to make change-bar PDFs available (with a filename of ...-diff.pdf). Upload at least the source file and one PDF to Kavi, setting the correct destination folder. This section should be removed before CD publication.

<table>
<thead>
<tr>
<th>Rev</th>
<th>Date</th>
<th>Who</th>
<th>What</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>nn Mon 2006</td>
<td>Hodges</td>
<td>Initial draft.</td>
</tr>
</tbody>
</table>
Appendix A. 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: [until Committee Draft publication, use "TBS"; at that time, get list from the SSTC Secretary; sort as for lists on title page]

- TBS
Appendix B. Notices

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's procedures with respect to rights in OASIS specifications can be found at 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 implementors or users of this specification, can be obtained from the OASIS Executive Director.

OASIS invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to implement this specification. Please address the information to the OASIS Executive Director.

Copyright © OASIS Open 2006. All Rights Reserved.

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 paragraph are included on all such copies and derivative works. However, this document itself does not need to be modified in any way, such as by removing the copyright notice or references to OASIS, except as needed for the purpose of developing OASIS specifications, in which case the procedures for copyrights defined in the OASIS Intellectual Property Rights document 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 RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.