



1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21

Differences between OASIS Security Assertion Markup Language (SAML) V1.1 and V1.0

21 May 2003

Document identifier:
sstc-saml-diff-1.1-draft-01

Location:
http://www.oasis-open.org/committees/documents.php?wg_abbrev=security

Editor:
Prateek Mishra, Netegrity (pmishra@netegrity.com)

Contributors:
Dipak Chopra, SAP
Jahan Moreh, Sigaba
Robert Philpott, RSA Security

Abstract:
This non-normative document provides an overview of the differences between SAML 1.1 and SAML 1.0.

Table of Contents

23	1	Introduction	3
24		1.1 Schema Organization and Namespaces	3
25		1.2 Changes to SAML 1.0 schema	3
26		1.2.1 Removal of IDType and IDReferenceType	3
27		1.2.2 Element <DoNotCacheCondition>	4
28		1.2.3 Element <Conditions>	4
29		1.3 Deprecated SAML 1.0 Elements and URIs	4
30		1.3.1 NameIdentifier Format Identifiers	4
31		1.3.2 Element <AuthorityBinding>	4
32		1.3.3 Element <RespondWith>	4
33		1.3.4 SAML Artifact Confirmation Method Identifier	4
34		1.4 Changes to Digital Signature Guidelines	5
35		1.5 SAML Versioning	5
36		1.6 Clarification of Processing Rules	5
37		1.6.1 SAML Protocol	5
38		1.6.2 Browser/POST Profile	5
39		1.6.3 Treatment of <SubjectConfirmation> in Browser Profiles	5
40		1.6.4 Alternative SAML Artifact Format	5
41		1.7 Corrections	5
42		1.7.1 Error Reporting in the SAML SOAP Binding	5
43		1.7.2 Incorrect Alternative SAML Artifact Identification URI	5
44	2	References	6

1 Introduction

The proposed SAML 1.1 specification (see reference section for a list of normative SAML 1.1 documents) includes changes to SAML 1.0 schema, deprecation of several SAML 1.0 elements and URIs, changes to the digital signature guidelines, clarification of processing rules, corrections and editorial changes.

Comment: This sounds like we are deprecating all SAML 1.0 elements and URIs. How about "...deprecation of some SAML 1.0 elements and URIs...."

1.1 Schema Organization and Namespaces

The SAML assertion structures are defined in a schema [SAML1.1A-XSD] associated with the following XML namespace:

```
urn:oasis:names:tc:SAML:1.0:assertion
```

Comment: No. The assertion and protocol namespace URN's have NOT been changed from 1.0 to 1.1.

The SAML request-response protocol structures are defined in a schema [SAML1.1P-XSD] associated with the following XML namespace:

```
urn:oasis:names:tc:SAML:1.0:protocol
```

Comment: Shouldn't this be.... :SAML:1.1:assertion?

The assertion schema is imported into the protocol schema. Also imported into both schemas is the schema for XML Signature **Error! Reference source not found.**, which is associated with the following XML namespace:

```
http://www.w3.org/2000/09/xmldsig#
```

Comment: Shouldn't this be.... :SAML:1.1:protocol?

1.2 Changes to SAML 1.0 schema

1.2.1 Removal of IDType and IDReferenceType

The following definitions of IDType and IDReferenceType are taken from [SAML1.0Core].

```
<simpleType name="IDType">  
  <restriction base="string"/>  
</simpleType>  
<simpleType name="IDReferenceType">  
  <restriction base="string"/>  
</simpleType>
```

These type definitions have been removed from [SAML1.1Core]. Instead, attributes AssertionID, RequestID and ResponseID directly reference the xsd:ID type. Element AssertionIDReference is defined to be of type xsd:NCName as in:

```
<element name="AssertionIDReference" type="NCName"/>
```

The motivation for these changes is to ensure that SAML assertions, requests and responses include an attribute with type "ID" as defined in XML Schema [Schema2]. References to these elements are of type "NCName". This simplifies digital signature processing as the <ds:Reference> can directly point to the unique fragment identifier associated via an attribute (e.g., AssertionID, RequestID, ResponseID) of the relevant top-level node being signed.

82 1.2.2 Element <DoNotCacheCondition>

```
83 <element name="DoNotCacheCondition" type="saml:DoNotCacheConditionType"/>
84 <complexType name="DoNotCacheConditionType">
85   <complexContent>
86     <extension base="saml:ConditionAbstractType"/>
87   </complexContent>
88 </complexType>
```

89
90 <saml:DoNotCacheCondition> is a new element that allows an asserting party to express that an
91 assertion should not be cached by the relying party for future use. In other words, such an assertion is
92 meant only for "one-time" use by the relying party.

94 1.2.3 Element <Conditions>

```
95 <element name="Conditions" type="saml:ConditionsType"/>
96 <complexType name="ConditionsType">
97   <choice minOccurs="0" maxOccurs="unbounded">
98     <element ref="saml:AudienceRestrictionCondition"/>
99     <element ref="saml:DoNotCacheCondition"/>
100    <element ref="saml:Condition"/>
101   </choice>
102   <attribute name="NotBefore" type="dateTime" use="optional"/>
103   <attribute name="NotOnOrAfter" type="dateTime" use="optional"/>
104 </complexType>
```

105
106 The <saml:Conditions> element is extended to act as a container for the
107 <saml:DoNotCacheCondition> element.

108 1.3 Deprecated SAML 1.0 Elements and URIs

109 Several SAML 1.0 elements, attributes and URIs are deprecated in SAML 1.1 and are likely to be
110 removed in the next major revision of the SAML specification.

111 1.3.1 NameIdentifier Format Identifiers

112 Section 7.3 of [SAML1.1Core] deprecates several URIs defined in Section 2.4.2.2 of [SAML1.0Core].

113 1.3.2 Element <AuthorityBinding>

114 Element <AuthorityBinding> is deprecated in SAML 1.1

115 1.3.3 Element <RespondWith>

116 Element <RespondWith> is deprecated in SAML 1.1.

117 1.3.4 SAML Artifact Confirmation Method Identifier

118 A new SAML artifact confirmation method identifier is defined and the existing SAML artifact confirmation
119 method identifier is deprecated as described in Section 5.3 of [SAML1.1Bind] .

120 **1.4 Changes to Digital Signature Guidelines**

121 Section 5 of **[SAML1.0Core]** has been substantively changed in **[SAML1.1Core]**. The <ds:Reference>
122 elements pointing to the elements covered by a signature must use a URI reference to the root element
123 being signed. Recommendations for the use of the canonical XML transform is replaced by
124 recommended use of the exclusive canonicalization transform.

125 **1.5 SAML Versioning**

126 Section 4 of **[SAML1.0Core]** has been substantially revised in **[SAML1.1Core]**. Most of the changes may
127 be considered clarifications and expansion of text in **[SAML1.0Core]**.

128 **1.6 Clarification of Processing Rules**

129 **1.6.1 SAML Protocol**

130 Section 3 of **[SAML1.0Core]** has been enhanced in **[SAML1.1Core]** with additional material clarifying the
131 semantics of the different forms of SAML request and query messages (Sections 3.2 and 3.3), use of the
132 status code element (section 3.4.3) and subject element matching rules (section 3.4.4).

133 **1.6.2 Browser/POST Profile**

134 Section 4.1.2.4 of **[SAML1.1Bind]** clarifies the use of Base64 Content-Transfer-Encoding within an HTML
135 form.

136 **1.6.3 Treatment of <SubjectConfirmation> in Browser Profiles**

137 Sections 4.1.1.6 and 4.1.2.5 of **[SAML1.1Bind]** clarify the range of admissible values of the
138 <SubjectConfirmation> element in the browser profiles.

139 **1.6.4 Alternative SAML Artifact Format**

140 Section 7.2 of **[SAML1.1Bind]** specifies the use of UTF-8 in converting a URL into a byte sequence.

141 **1.7 Corrections**

142 **1.7.1 Error Reporting in the SAML SOAP Binding**

143 Section 3.1.3.6 of **[SAML1.1Bind]** recommends returning SAML processing errors within <Response>
144 elements. It deprecates the placement of SAML status codes as a direct child of the SOAP body element.

145 **1.7.2 Incorrect Alternative SAML Artifact Identification URI**

146 Section 7.1 of **[SAML1.1Bind]** provides the correct identification URI for the Alternative SAML artifact
147 format.

148

149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171

2 References

- [SAML1.0Core]** P. Hallam-Baker, Eve Maler, *Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML)*, OASIS Standard, 5 November 2002. Available from <http://www.oasis-open.org>.
- [SAML1.1Core]** Eve Maler, Prateek Mishra, Robert Philpott, *Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML)*, Last Call Working Draft 10, 2 May 2003. Available from <http://www.oasis-open.org>.
- [SAML1.1Bind]** Eve Maler, Prateek Mishra, Robert Philpott, *Bindings and Profiles for the OASIS Security Assertion Markup Language (SAML)*, Last Call Working Draft 06, 2 May 2003. Available from <http://www.oasis-open.org>.
- [XMLSig]** D. Eastlake et al., *XML-Signature Syntax and Processing*, World Wide Web Consortium, February 2002. <http://www.w3.org/TR/xmlsig-core/>.
- [SAML1.1A-XSD]** Eve Maler et al. *SAML assertion schema*, sstc-saml-schema-assertion-1.1-draft-02.xsd, May 2003. Available from <http://www.oasis-open.org>.
- [SAML1.1P-XSD]** Eve Maker et al. *SAML protocol schema*, sstc-saml-schema-protocol-1.1-draft-03.xsd, May 2003. Available from <http://www.oasis-open.org>.
- [Schema2]** P. V. Biron et al., *XML Schema Part 2: Datatypes*, World Wide Web Consortium Recommendation, May 2001. <http://www.w3.org/TR/xmlschema-2>, World Wide Web Consortium Recommendation, May 2001./.