



SAML 2.0 Shared Credentials Authentication Context Extension and Related Classes

Committee Specification 01

23 May 2007

Specification URIs:

This Version:

<http://docs.oasis-open.org/security/saml/SpecDrafts-Post2.0/sstc-saml-context-ext-sc-cs-01.html>

<http://docs.oasis-open.org/security/saml/SpecDrafts-Post2.0/sstc-saml-context-ext-sc-cs-01.odt>

<http://docs.oasis-open.org/security/saml/SpecDrafts-Post2.0/sstc-saml-context-ext-sc-cs-01.pdf>

Previous Version:

<http://docs.oasis-open.org/security/saml/SpecDrafts-Post2.0/sstc-saml-context-ext-sc-cd-03.html>

<http://docs.oasis-open.org/security/saml/SpecDrafts-Post2.0/sstc-saml-context-ext-sc-cd-03.odt>

<http://docs.oasis-open.org/security/saml/SpecDrafts-Post2.0/sstc-saml-context-ext-sc-cd-03.pdf>

Latest Version:

<http://docs.oasis-open.org/security/saml/SpecDrafts-Post2.0/sstc-saml-context-ext-sc.html>

<http://docs.oasis-open.org/security/saml/SpecDrafts-Post2.0/sstc-saml-context-ext-sc.odt>

<http://docs.oasis-open.org/security/saml/SpecDrafts-Post2.0/sstc-saml-context-ext-sc.pdf>

Technical Committee:

OASIS Security Services TC

Chair(s):

Hal Lockhart, BEA Systems, Inc

Prateek Mishra, Oracle

Editors:

Paul Madsen (paul.madsen@ntt-at.com), NTT

Ashish Patel (ashish.patel@rd.francetelecom.com), France Telecom

Abstract:

This specification defines an authentication context extension to the SAML 2.0 Authentication Context specification [SAMLAC](#) that allows providers to distinguish whether or not the credential by which a principal authenticates to the identity provider is known to be shared amongst a group of users or unique to that user. Two new Authentication Context classes and associated schemas are also introduced to distinguish between these two cases.

34 Readers should be familiar with [SAMLAC](#) before reading this document.

35 **Status**

36 This document was last revised or approved by the OASIS Security Services Technical
37 Committee on the above date. The level of approval is also listed above. Check the "Latest
38 Version" or "Latest Approved Version" location noted above for possible later revisions of this
39 document.

40 Committee members should submit comments and potential errata to the [security-
41 services@lists.oasis-open.org](mailto:security-services@lists.oasis-open.org) list. Others should submit them by filling out the web form located
42 at http://www.oasis-open.org/committees/comments/form.php?wg_abbrev=security.

43 For information on whether any patents have been disclosed that may be essential to
44 implementing this specification, and any offers of patent licensing terms, please refer to the
45 Intellectual Property Rights web page for the Security Services TC ([http://www.oasis-
open.org/committees/security/ipr.php](http://www.oasis-
46 open.org/committees/security/ipr.php)).

Table of Contents

48		
49	1 Introduction.....	4
50	1.1 Notation.....	4
51	2 Shared Credential SAML Authentication Context Extension.....	5
52	2.1 Element <sc:SharedCredential>.....	5
53	2.2 Example.....	5
54	2.3 Processing Rules.....	6
55	3 Authentication Context Shared Credential Classes.....	7
56	3.1.1 Shared Credential	7
57	3.1.2 Unique Credential.....	8
58	4 References.....	11
59	4.1 Normative References.....	11
60	Appendix A. Acknowledgements.....	12
61	Appendix B. Notices.....	13
62		

63 1 Introduction

64 The SAML Authentication Context schema [SAMLAC Schema](#) provides extension points through the
65 <Extension> element so that elements in non-SAML namespaces can be added to declarations and
66 class definitions.

67 This specification defines an extension to the SAML 2.0 Authentication Context core schema specification
68 that can be optionally used to distinguish whether the credential used by a principal to authenticate is
69 known to be shared with other principals – an important aspect of authentication in many telco use cases.

70 To simplify how providers describe this aspect of authentication context, this specification also introduces
71 two new Authentication Context classes that differ only in this aspect.

72 1.1 Notation

73 This specification uses normative text.

74 The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD
75 NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this specification are to be interpreted as
76 described in Error: Reference source not found:

77 ...they MUST only be used where it is actually required for interoperability or to limit
78 behavior which has potential for causing harm (e.g., limiting retransmissions)...

79 These keywords are thus capitalized when used to unambiguously specify requirements over protocol
80 and application features and behavior that affect the interoperability and security of implementations.
81 When these words are not capitalized, they are meant in their natural-language sense.

82 Listings of XML schemas appear like this.

83
84 Example code listings appear like this.

85 Conventional XML namespace prefixes are used throughout the listings in this specification to stand for
86 their respective namespaces as follows, whether or not a namespace declaration is present in the
87 example:

Prefix	XML Namespace	Comments
saml:	urn:oasis:names:tc:SAML:2.0:assertion	This is the SAML V2.0 assertion namespace SAMLCore
samlp:	urn:oasis:names:tc:SAML:2.0:protocol	This is the SAML V2.0 protocol namespace SAMLCore
md:	urn:oasis:names:tc:SAML:2.0:metadata	This is the SAML V2.0 metadata namespace SAMLMeta
sc:	urn:oasis:names:tc:SAML:context:ext:sc	This is the shared credential authentication context extension namespace developed herein. SC-XSD
xsd:	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.

88 This specification uses the following typographical conventions in text: <SAMLElement>,
89 <ns:ForeignElement>, Attribute, **Datatype**, OtherCode.

2 Shared Credential SAML Authentication Context Extension

Certain telco use cases demand the ability for IDPs and SPs to distinguish between whether a principal is authenticated with a credential that is known to be shared amongst a group (e.g. a home phone or an internet kiosk) or unique to that principal. The existing SAML AC core schema does not explicitly support this aspect of authentication.

This section defines an extension to the SAML 2.0 authentication context schema that can be optionally used to express this aspect of authentication context. The extension may optionally appear within the `<ac:PrincipalAuthenticationMechanism>` element to either further qualify the specific authentication mechanism (e.g. Password, Token, Smartcard, etc) used by the principal or on its own.

2.1 Element `<sc:SharedCredential>`

The `<sc:SharedCredential>` element is used to distinguish between the two cases of a credential used to authenticate known to be shared amongst a group of users or not.

The following schema fragment defines the `<sc:SharedCredential>` element:

```
<element name="SharedCredential" type="SharedCredentialType"/>
<xs:annotation>
  <xs:documentation> The SharedCredential Extension MUST NOT occur any other
place than in the Extension element of the PrincipalAuthenticationMechanism
element within an Authentication Context declaration. A value of '0' for the
extensions content indicates that the credential by which a user authenticated
was not shared, a value of '1' that the credential was shared
  </xs:documentation>
</xs:annotation>
<complexType name="SharedCredentialType">
  <SimpleContent>
    <extension base="xs:boolean"/>
  </SimpleContent>
</complexType>
```

2.2 Example

The following is an example of an Authentication Context declaration in which the identity provider is, in addition to the other aspects of the context, indicating that the principal authenticated with a credential that the identity provider knew to be shared.

```
<ac:AuthnContextDeclaration>
  <ac:Identification/>
  <ac:TechnicalProtection/>
  <ac:OperationalProtection/>
  <ac:AuthnMethod>
    <ac:PrincipalAuthenticationMechanism>
      <ac:Extension>
        <sc:SharedCredential>1</sc:SharedCredential>
      </ac:Extension>
    </ac:PrincipalAuthenticationMechanism>
    <ac:Authenticator>
      <ac:SubscriberLineNumber/>
    </ac:Authenticator>
  </ac:AuthnMethod>
</ac:AuthnContextDeclaration>
```

```
137     <ac:AuthenticatorTransportProtocol/>
138     </ac:AuthnMethod>
139 </ac:AuthnContextDeclaration>
140
```

141 2.3 Processing Rules

142 To differentiate whether or not the principal authenticated with a credential known to be shared, the
143 identity provider MAY insert the `<sc:SharedCredential>` extension element in an `<ac:Extension>`
144 element within the `<ac:PrincipalAuthenticationMechanism>` in an authentication context
145 declaration.

146 There MUST be at most one `<sc:SharedCredential>` extension element within an authentication
147 context declaration.

148 A `<sc:SharedCredential>` element MUST NOT appear in any other `<ac:Extension>` element
149 within an authentication context declaration.

3 Authentication Context Shared Credential Classes

150

151 The following two Authentication Context classes are defined to represent the two different possibilities for
152 the SharedCredential extension.

3.1.1 Shared Credential

153

154 **URI:** urn:oasis:names:tc:SAML:2.0:ac:ext:classes:sc:shared

155 This URI reflects that the credential used to authenticate is known to be shared amongst two or more
156 users.

157 This class can be composed with other authentication context class URIs.

```
158 <?xml version="1.0" encoding="UTF-8"?>
159
160 <xs:schema
161 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:ext:classes:sc:shared"
162 xmlns:xs="http://www.w3.org/2001/XMLSchema"
163 xmlns="urn:oasis:names:tc:SAML:2.0:ac:ext:classes:sc:shared"
164 finalDefault="extension"
165 blockDefault="substitution"
166 version="2.0">
167
168 <xs:redefine schemaLocation=" sstc-saml-context-ext-sc.xsd">
169
170 <xs:annotation>
171 <xs:documentation>
172 This class is defined by a fixed value of '1' for the
173 SharedCredential extension, indicating that the credential was shared
174 </xs:documentation>
175 </xs:annotation>
176
177 <complexType name="SharedCredentialType">
178 <complexContent>
179 <restriction base="SharedCredentialType">
180 <simpleContent>
181 <extension base="xs:boolean" fixed="1"/>
182 </simpleContent>
183 </restriction>
184 </complexContent>
185 </complexType>
186 </redefine>
187
188 <redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">
189 <xs:annotation>
190 <xs:documentation>There MUST be an Extension element in the
191 PrincipalAuthenticationMechanism
192 </xs:documentation>
193 </xs:annotation>
194
195 <xs:complexType name="AuthnContextDeclarationBaseType">
196 <xs:complexContent>
197 <xs:restriction base="AuthnContextDeclarationBaseType">
198 <xs:sequence>
199 <xs:element ref="Identification" minOccurs="0"/>
```

```

200     <xs:element ref="TechnicalProtection" minOccurs="0"/>
201     <xs:element ref="OperationalProtection" minOccurs="0"/>
202     <xs:element ref="AuthnMethod"/>
203     <xs:element ref="GoverningAgreements" minOccurs="0"/>
204     <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
205   </xs:sequence>
206   <xs:attribute name="ID" type="xs:ID" use="optional"/>
207 </xs:restriction>
208 </xs:complexContent>
209 </xs:complexType>
210
211 <xs:complexType name="AuthnMethodBaseType">
212   <xs:complexContent>
213     <xs:restriction base="AuthnMethodBaseType">
214       <xs:sequence>
215         <xs:element ref="PrincipalAuthenticationMechanism"
216 minOccurs="0"/>
217         <xs:element ref="Authenticator"/>
218         <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
219         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
220       </xs:sequence>
221     </xs:restriction>
222   </xs:complexContent>
223 </xs:complexType>
224
225 <xs:complexType name="PrincipalAuthenticationMechanismType">
226   <xs:complexContent>
227     <xs:restriction base="PrincipalAuthenticationMechanismType">
228       <xs:sequence>
229         <xs:element ref="Extension" minOccurs="1"/>
230       </xs:sequence>
231     </xs:restriction>
232   </xs:complexContent>
233 </xs:complexType>
234 </redefine>
235
236 </schema>

```

237 3.1.2 Unique Credential

238 **URI:** urn:oasis:names:tc:SAML:2.0:ac:ext:classes:sc:unique

239 This URI reflects that the credential used to authenticate is known to be unique (or at least not known to
240 be shared) to the authenticating user..

241 This class can be composed with other authentication context class URIs.

```

242 <?xml version="1.0" encoding="UTF-8"?>
243 <schema
244 targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:ext:sc:unique"
245 xmlns:xs="http://www.w3.org/2001/XMLSchema"
246 xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:ext:sc:unique"
247 finalDefault="extension"
248 blockDefault="substitution"
249 version="2.0">
250
251 <redefine schemaLocation="sstc-saml-context-ext-sc.xsd">

```



```

252
253 <xs:annotation>
254   <xs:documentation>This class is defined by a fixed value of '0' for the
255     SharedCredential extension, indicating that the credential was uniquely
256     held.
257   </xs:documentation>
258 </xs:annotation>
259 <complexType name="SharedCredentialType">
260   <complexContent>
261     <restriction base="SharedCredentialType">
262       <simpleContent>
263         <extension base="xs:boolean" fixed="0"/>
264       </simpleContent>
265     </restriction>
266   </complexContent>
267 </complexType>
268 </redefine>
269
270 <redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">
271
272   <xs:annotation>
273     <xs:documentation>There MUST be an Extension element in the
274       PrincipalAuthenticationMechanism
275     </xs:documentation>
276   </xs:annotation>
277
278   <xs:complexType name="AuthnContextDeclarationBaseType">
279     <xs:complexContent>
280       <xs:restriction base="AuthnContextDeclarationBaseType">
281         <xs:sequence>
282           <xs:element ref="Identification" minOccurs="0"/>
283           <xs:element ref="TechnicalProtection" minOccurs="0"/>
284           <xs:element ref="OperationalProtection" minOccurs="0"/>
285           <xs:element ref="AuthnMethod"/>
286           <xs:element ref="GoverningAgreements" minOccurs="0"/>
287           <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
288         </xs:sequence>
289         <xs:attribute name="ID" type="xs:ID" use="optional"/>
290       </xs:restriction>
291     </xs:complexContent>
292   </xs:complexType>
293
294   <xs:complexType name="AuthnMethodBaseType">
295     <xs:complexContent>
296       <xs:restriction base="AuthnMethodBaseType">
297         <xs:sequence>
298           <xs:element ref="PrincipalAuthenticationMechanism"
299 minOccurs="0"/>
300           <xs:element ref="Authenticator"/>
301           <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
302           <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
303         </xs:sequence>
304       </xs:restriction>
305     </xs:complexContent>
306   </xs:complexType>
307

```

```
308 <xs:complexType name="PrincipalAuthenticationMechanismType">
309   <xs:complexContent>
310     <xs:restriction base="PrincipalAuthenticationMechanismType">
311       <xs:sequence>
312         <xs:element ref="Extension" minOccurs="1"/>
313       </xs:sequence>
314     </xs:restriction>
315   </xs:complexContent>
316 </xs:complexType>
317 </redefine>
318
319 </schema>
```

320 4 References

321 The following works are referenced in the body of this specification.

322 4.1 Normative References

323

- 324 **[RFC 2119]** S. Bradner. *Key words for use in RFCs to Indicate Requirement Levels*. IETF
325 RFC 2119, March 1997. <http://www.ietf.org/rfc/rfc2119.txt>.
- 326 **[SAMLAuthnCxt]** J. Kemp et al. *Authentication Context for the OASIS Security Assertion Markup
327 Language (SAML) V2.0*. OASIS SSTC, March 2005. Document ID saml-authn-
328 context-2.0-os. See [http://docs.oasis-open.org/security/saml/v2.0/saml-authn-
context-2.0-os.pdf](http://docs.oasis-open.org/security/saml/v2.0/saml-authn-
329 context-2.0-os.pdf).
- 330 **[SAMLAC-schema]** J. Kemp et al. *SAML authentication context schema*. OASIS SSTC, March
331 2005. Document ID saml-authn-context-2.0-os.
- 332 **[SAMLCore]** S. Cantor et al. *Assertions and Protocols for the OASIS Security Assertion
333 Markup Language (SAML) V2.0*. OASIS SSTC, March 2005. Document ID saml-
334 core-2.0-os. See [http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-
os.pdf](http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-
335 os.pdf).
- 336 **[SAMLBind]** S. Cantor et al. *Bindings for the OASIS Security Assertion Markup Language
337 (SAML) V2.0*. OASIS SSTC, March 2005. Document ID saml-bindings-2.0-os.
338 See <http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf>.
- 339 **[SAMLMeta]** S. Cantor et al. *Metadata for the OASIS Security Assertion Markup Language
340 (SAML) V2.0*. OASIS SSTC, March 2005. Document ID saml-metadata-2.0-os.
341 See <http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf>.
- 342 **[SAMLProf]** S. Cantor et al. *Profiles for the OASIS Security Assertion Markup Language
343 (SAML) V2.0*. OASIS SSTC, March 2005. Document ID saml-profiles-2.0-os. See
344 <http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf>.
- 345 **[Schema1]** H. S. Thompson et al. *XML Schema Part 1: Structures*. World Wide Web
346 Consortium Recommendation, May 2001. See [http://www.w3.org/TR/2001/REC-
xmlschema-1-20010502/](http://www.w3.org/TR/2001/REC-
347 xmlschema-1-20010502/).
- 348 **[sc-xsd]** P. Madsen & A. Patel. *SAML Shared Credential Authentication Context
349 extension schema*. OASIS SSTC, September 2006. Document ID sstc-saml-
350 context-ext-sc.xsd. See <http://www.oasis-open.org/committees/security/>.
- 351

352 **Appendix A. Acknowledgements**

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

- 355 • Hal Lockhart, BEA Systems, Inc.
- 356 • Steve Anderson, BMC Software
- 357 • Thomas Wisniewski, Entrust
- 358 • Ashish Patel, France Telecom
- 359 • Greg Whitehead, Hewlett-Packard
- 360 • Heather Hinton, IBM
- 361 • Anthony Nadalin, IBM
- 362 • Eric Tiffany, IEEE Industry Standards and Technology Org (IEEE-ISTO)
- 363 • Scott Cantor, Internet2
- 364 • Bob Morgan, Internet2
- 365 • Tom Scavo, National Center for Supercomputing Applications (NCSA)
- 366 • Peter Davis, Neustar, Inc.
- 367 • Jeff Hodges, Neustar, Inc.
- 368 • Frederick Hirsch, Nokia Corporation
- 369 • Abbie Barbir, Nortel Networks Limited
- 370 • Paul Madsen, NTT Corporation
- 371 • Ari Kermaier, Oracle Corporation
- 372 • Prateek Mishra, Oracle Corporation
- 373 • John Hughes, PA Consulting
- 374 • Brian Campbell, Ping Identity Corporation
- 375 • Rob Philpott, RSA Security
- 376 • Jahan Moreh, Sigaba Corp.
- 377 • Bhavna Bhatnagar, Sun Microsystems
- 378 • Eve Maler, Sun Microsystems
- 379 • Emily Xu, Sun Microsystems
- 380 • David Staggs, Veterans Health Administration

381 **Appendix B. Notices**

382 OASIS takes no position regarding the validity or scope of any intellectual property or other rights that
383 might be claimed to pertain to the implementation or use of the technology described in this document or
384 the extent to which any license under such rights might or might not be available; neither does it
385 represent that it has made any effort to identify any such rights. Information on OASIS's procedures with
386 respect to rights in OASIS specifications can be found at the OASIS website. Copies of claims of rights
387 made available for publication and any assurances of licenses to be made available, or the result of an
388 attempt made to obtain a general license or permission for the use of such proprietary rights by
389 implementors or users of this specification, can be obtained from the OASIS Executive Director.

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

393 **Copyright © OASIS Open 2006. All Rights Reserved.**

394 This document and translations of it may be copied and furnished to others, and derivative works that
395 comment on or otherwise explain it or assist in its implementation may be prepared, copied, published
396 and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice
397 and this paragraph are included on all such copies and derivative works. However, this document itself
398 may not be modified in any way, such as by removing the copyright notice or references to OASIS, except
399 as needed for the purpose of developing OASIS specifications, in which case the procedures for
400 copyrights defined in the OASIS Intellectual Property Rights document must be followed, or as required to
401 translate it into languages other than English.

402 The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors
403 or assigns.

404 This document and the information contained herein is provided on an "AS IS" basis and OASIS
405 DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY
406 WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR
407 ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.