

SAML 2.0 Shared Credentials Authentication Context Extension and Related Classes

Committee Specification 01

23 May 2007

Document identifier:

draft-sstc-saml-context-ext-sc-cs-01

Location:

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

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.

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

Status

This is a **Committee Specification** approved by the Security Services Technical Committee on 23 May 2007.

Committee members should submit comments and potential errata to the security-services@lists.oasis-open.org list. Others should submit them by filling out the web form located 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

34
35

Intellectual Property Rights web page for the Security Services TC (<http://www.oasis-open.org/committees/security/ipr.php>).

36 **Table of Contents**

37 1 Introduction.....3

38 1.1 Notation.....3

39 2 Shared Credential SAML Authentication Context Extension.....5

40 2.1 Element <sc:SharedCredential>.....5

41 2.2 Example.....5

42 2.3 Processing Rules.....6

43 3 Authentication Context Shared Credential Classes.....7

44 3.1.1 Shared Credential7

45 3.1.2 Unique Credential.....8

46 4 References.....10

47 4.1 Normative References.....10

48 Appendix A. Acknowledgements.....11

49 Appendix B. Notices.....12

50

51 1 Introduction

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

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

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

60 1.1 Notation

61 This specification uses normative text.

62 The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD
63 NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this specification are to be interpreted as
64 described in :

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

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

70 Listings of XML schemas appear like this.

71 Example code listings appear like this.

73 Conventional XML namespace prefixes are used throughout the listings in this specification to stand for
74 their respective namespaces as follows, whether or not a namespace declaration is present in the
75 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.

76 This specification uses the following typographical conventions in text: <SAMLElement>,
77 <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:AuthenticatorTransportProtocol/>
  </ac:AuthnMethod>
```

127 `</ac:AuthnContextDeclaration>`

128

129 **2.3 Processing Rules**

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

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

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

3 Authentication Context Shared Credential Classes

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

3.1.1 Shared Credential

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

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

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

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema targetNamespace="urn:oasis:names:tc:SAML:
2.0:ac:ext:classes:sc:shared"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:ext:classes:sc:shared"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">
  <xs:redefine schemaLocation=" sstc-saml-context-ext-sc.xsd">
    <xs:annotation>
      <xs:documentation>
        This class is defined by a fixed value of '1' for the
        SharedCredential extension, indicating that the credential was shared
      </xs:documentation>
    </xs:annotation>
    <complexType name="SharedCredentialType">
      <complexContent>
        <restriction base="SharedCredentialType">
          <simpleContent>
            <extension base="xs:boolean" fixed="1"/>
          </simpleContent>
        </restriction>
      </complexContent>
    </complexType>
  </redefine>
  <redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">
    <xs:annotation>
      <xs:documentation>There MUST be an Extension element in the
        PrincipalAuthenticationMechanism
      </xs:documentation>
    </xs:annotation>
    <xs:complexType name="AuthnContextDeclarationBaseType">
      <complexContent>
        <xs:restriction base="AuthnContextDeclarationBaseType">
          <xs:sequence>
            <xs:element ref="Identification" minOccurs="0"/>
            <xs:element ref="TechnicalProtection" minOccurs="0"/>
            <xs:element ref="OperationalProtection" minOccurs="0"/>
            <xs:element ref="AuthnMethod"/>
          </xs:sequence>
        </xs:restriction>
      </complexContent>
    </xs:complexType>
  </redefine>
</xs:schema>
```

```

191     <xs:element ref="GoverningAgreements" minOccurs="0"/>
192     <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
193   </xs:sequence>
194   <xs:attribute name="ID" type="xs:ID" use="optional"/>
195 </xs:restriction>
196 </xs:complexContent>
197 </xs:complexType>
198
199 <xs:complexType name="AuthnMethodBaseType">
200   <xs:complexContent>
201     <xs:restriction base="AuthnMethodBaseType">
202       <xs:sequence>
203         <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
204         <xs:element ref="Authenticator"/>
205         <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
206         <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
207       </xs:sequence>
208     </xs:restriction>
209   </xs:complexContent>
210 </xs:complexType>
211
212 <xs:complexType name="PrincipalAuthenticationMechanismType">
213   <xs:complexContent>
214     <xs:restriction base="PrincipalAuthenticationMechanismType">
215       <xs:sequence>
216         <xs:element ref="Extension" minOccurs="1"/>
217       </xs:sequence>
218     </xs:restriction>
219   </xs:complexContent>
220 </xs:complexType>
221 </redefine>
222
223 </schema>

```

224 3.1.2 Unique Credential

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

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

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

```

229 <?xml version="1.0" encoding="UTF-8"?>
230 <schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:ext:sc:unique"
231   xmlns:xs="http://www.w3.org/2001/XMLSchema"
232   xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:ext:sc:unique"
233   finalDefault="extension"
234   blockDefault="substitution"
235   version="2.0">
236
237   <redefine schemaLocation="sstc-saml-context-ext-sc.xsd">
238
239     <xs:annotation>
240       <xs:documentation>This class is defined by a fixed value of '0' for the
241         SharedCredential extension, indicating that the credential was uniquely
242         held.
243       </xs:documentation>
244     </xs:annotation>
245     <complexType name="SharedCredentialType">

```



```

246     <complexContent>
247       <restriction base="SharedCredentialType">
248         <simpleContent>
249           <extension base="xs:boolean" fixed="0"/>
250         </simpleContent>
251       </restriction>
252     </complexContent>
253 </complexType>
254 </redefine>
255
256 <redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">
257
258   <xs:annotation>
259     <xs:documentation>There MUST be an Extension element in the
260     PrincipalAuthenticationMechanism
261   </xs:documentation>
262 </xs:annotation>
263
264   <xs:complexType name="AuthnContextDeclarationBaseType">
265     <xs:complexContent>
266       <xs:restriction base="AuthnContextDeclarationBaseType">
267         <xs:sequence>
268           <xs:element ref="Identification" minOccurs="0"/>
269           <xs:element ref="TechnicalProtection" minOccurs="0"/>
270           <xs:element ref="OperationalProtection" minOccurs="0"/>
271           <xs:element ref="AuthnMethod"/>
272           <xs:element ref="GoverningAgreements" minOccurs="0"/>
273           <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
274         </xs:sequence>
275         <xs:attribute name="ID" type="xs:ID" use="optional"/>
276       </xs:restriction>
277     </xs:complexContent>
278   </xs:complexType>
279
280   <xs:complexType name="AuthnMethodBaseType">
281     <xs:complexContent>
282       <xs:restriction base="AuthnMethodBaseType">
283         <xs:sequence>
284           <xs:element ref="PrincipalAuthenticationMechanism" minOccurs="0"/>
285           <xs:element ref="Authenticator"/>
286           <xs:element ref="AuthenticatorTransportProtocol" minOccurs="0"/>
287           <xs:element ref="Extension" minOccurs="0" maxOccurs="unbounded"/>
288         </xs:sequence>
289       </xs:restriction>
290     </xs:complexContent>
291   </xs:complexType>
292
293   <xs:complexType name="PrincipalAuthenticationMechanismType">
294     <xs:complexContent>
295       <xs:restriction base="PrincipalAuthenticationMechanismType">
296         <xs:sequence>
297           <xs:element ref="Extension" minOccurs="1"/>
298         </xs:sequence>
299       </xs:restriction>
300     </xs:complexContent>
301   </xs:complexType>
302 </redefine>
303
304 </schema>

```

305 4 References

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

307 4.1 Normative References

308

- 309 **[RFC 2119]** S. Bradner. *Key words for use in RFCs to Indicate Requirement Levels*. IETF
310 RFC 2119, March 1997. <http://www.ietf.org/rfc/rfc2119.txt>.
- 311 **[SAMLAuthnCxt]** J. Kemp et al. *Authentication Context for the OASIS Security Assertion Markup
312 Language (SAML) V2.0*. OASIS SSTC, March 2005. Document ID saml-authn-
313 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-
314 context-2.0-os.pdf).
- 315 **[SAMLAC-schema]** J. Kemp et al. *SAML authentication context schema*. OASIS SSTC, March 2005.
316 Document ID saml-authn-context-2.0-os.
- 317 **[SAMLCore]** S. Cantor et al. *Assertions and Protocols for the OASIS Security Assertion
318 Markup Language (SAML) V2.0*. OASIS SSTC, March 2005. Document ID saml-
319 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-
320 os.pdf).
- 321 **[SAMLBind]** S. Cantor et al. *Bindings for the OASIS Security Assertion Markup Language
322 (SAML) V2.0*. OASIS SSTC, March 2005. Document ID saml-bindings-2.0-os.
323 See <http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf>.
- 324 **[SAMLMeta]** S. Cantor et al. *Metadata for the OASIS Security Assertion Markup Language
325 (SAML) V2.0*. OASIS SSTC, March 2005. Document ID saml-metadata-2.0-os.
326 See <http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf>.
- 327 **[SAMLProf]** S. Cantor et al. *Profiles for the OASIS Security Assertion Markup Language
328 (SAML) V2.0*. OASIS SSTC, March 2005. Document ID saml-profiles-2.0-os. See
329 <http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf>.
- 330 **[Schema1]** H. S. Thompson et al. *XML Schema Part 1: Structures*. World Wide Web
331 Consortium Recommendation, May 2001. See [http://www.w3.org/TR/2001/REC-
xmlschema-1-20010502/](http://www.w3.org/TR/2001/REC-
332 xmlschema-1-20010502/).
- 333 **[sc-xsd]** P. Madsen & A. Patel. *SAML Shared Credential Authentication Context
334 extension schema*. OASIS SSTC, September 2006. Document ID sstc-saml-
335 context-ext-sc.xsd. See <http://www.oasis-open.org/committees/security/>.
336

337 **Appendix A. Acknowledgements**

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

- 340 • Hal Lockhart, BEA Systems, Inc.
- 341 • Steve Anderson, BMC Software
- 342 • Thomas Wisniewski, Entrust
- 343 • Ashish Patel, France Telecom
- 344 • Greg Whitehead, Hewlett-Packard
- 345 • Heather Hinton, IBM
- 346 • Anthony Nadalin, IBM
- 347 • Eric Tiffany, IEEE Industry Standards and Technology Org (IEEE-ISTO)
- 348 • Scott Cantor, Internet2
- 349 • Bob Morgan, Internet2
- 350 • Tom Scavo, National Center for Supercomputing Applications (NCSA)
- 351 • Peter Davis, Neustar, Inc.
- 352 • Jeff Hodges, Neustar, Inc.
- 353 • Frederick Hirsch, Nokia Corporation
- 354 • Abbie Barbir, Nortel Networks Limited
- 355 • Paul Madsen, NTT Corporation
- 356 • Ari Kermaier, Oracle Corporation
- 357 • Prateek Mishra, Oracle Corporation
- 358 • John Hughes, PA Consulting
- 359 • Brian Campbell, Ping Identity Corporation
- 360 • Rob Philpott, RSA Security
- 361 • Jahan Moreh, Sigaba Corp.
- 362 • Bhavna Bhatnagar, Sun Microsystems
- 363 • Eve Maler, Sun Microsystems
- 364 • Emily Xu, Sun Microsystems
- 365 • David Staggs, Veterans Health Administration

366 **Appendix B. Notices**

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

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

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

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

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

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