



SAML 2.0 Protocol Extension for Requested Authentication Context

Committee Draft 03, 11 September 2006

Document identifier:

draft-sstc-saml-protocol-ext-rac-cd-03

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 a protocol extension to SAML 2.0 specification that facilitates a more flexible model for expressing Authentication Context than that currently supported. The extension allows service providers to express combinations of Authentication Context classes in their requests for authentication assertions. The expectation is that the extension, when its additional functionality was necessary, would be used in replacement of the existing Authentication Context mechanisms in the authentication request message. Readers should be familiar with before reading this document.

Status

This is a **Committee Draft** approved by the Security Services Technical Committee on 11 September 2006.

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 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 SAML Protocol Extension for Requested Authentication Context..... 4

40 2.1 Element <rac:RequestedACCombination>..... 4

41 2.1.1 RACComparison attribute..... 5

42 2.2 Example..... 5

43 2.3 Processing Rules..... 6

44 2.4 Metadata Considerations..... 6

45 2.4.1 Metadata Example..... 7

46 3 References..... 8

47 3.1 Normative References..... 8

48 Appendix A. Acknowledgements..... 9

49 Appendix B. Notices..... 10

50

51 1 Introduction

52 SAML protocol extensions consist of elements defined for inclusion in the `<samlp:Extensions>`
53 element that modify the behavior of SAML requesters and responders when processing such extended
54 messages.

55 This specification defines an extension to the SAML 2.0 protocol specification that can be optionally
56 used to replace the existing mechanisms for Authentication Context `#saml_ac` in authentication requests.
57 The extension provides a more flexible structure for expressing combinations of Authentication Context
58 classes than do existing mechanisms.

59 1.1 Notation

60 This specification uses normative text.

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

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

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

69 Listings of XML schemas appear like this.

70 Example code listings appear like this.

72 Conventional XML namespace prefixes are used throughout the listings in this specification to stand for
73 their respective namespaces as follows, whether or not a namespace declaration is present in the
74 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
rac:	urn:oasis:names:tc:SAML:protocol:ext:rac	This is the SAML V2.0 protocol extension namespace, defined by this document and its accompanying schema RAC-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.

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

2 SAML Protocol Extension for Requested Authentication Context

This specification defines an extension to the SAML 2.0 protocol specification that can be optionally used to replace the existing mechanisms within requests for Authentication Context [SAMLAC](#) with a more flexible structure for expressing combinations of Authentication Context classes.

Existing structures for indicating authentication context in authentication request messages are limited in their ability to express combinations of authentication contexts – the assumption is that the full context can be expressed through a single declaration, declaration reference, or a class reference.

Consequently, were an SP or IDP to wish to express such a logical combination (or the SSTC to define classes to enable this), it would necessarily imply the creation of a new class URI to represent such a combination.

As a concrete example, 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. Because no existing SAML AC classes support this distinction (nor the schema as it stands), to allow an SP to make this distinction in its `<AuthnRequest>` implies that new AC classes would need to be defined to add the shared/unique distinction to each (relevant) existing AC class. For just this single initially unforeseen aspect of authentication context, we face the possibility of a combinatorial explosion of AC class URIs. Should other such aspects emerge in the future, the problem would be exacerbated.

More scalable would be to allow the SP to compose its Authentication Context requirements through the listing of multiple AC classes, and to allow the SP to control how those multiple classes are to be logically combined. Unfortunately, the existing `<saml:RequestedAuthnContext>` mechanism does not provide this flexibility.

This extension is intended to override existing mechanisms for requesting authentication contexts with a more flexible model – thereby meeting the immediate requirements of the above telco use cases, as well as providing a scalable solution for dealing with similar currently unforeseen AC aspects should they arise.

Unless specifically noted, nothing in this document should be taken to conflict with the SAML 2.0 protocol specification [SAMLCore](#). Readers are advised to familiarize themselves with that specification first.

2.1 Element `<rac:RequestedACCombination>`

The `<rac:RequestedACCombination>` element is used to carry the individual requested Authentication Contexts and to specify the logical operator defining how they should be combined.

The following schema fragment defines the `<rac:RequestedACCombination>` element:

```
<element name="RequestedACCombination" type="RequestedACCombinationType"/>
<complexType name="RequestedAuthnContextType">
  <choice>
    <element ref="RequestedACCombination" maxOccurs="unbounded"/>
    <element ref="saml:AuthnContextClassRef" maxOccurs="unbounded"/>
  </choice>
  <attribute name="RACComparison" type="anyURI" use="optional"/>
</complexType>
```

123 The <rac:RequestedACCombination> element can be nested to allow the SP to define combinations
124 of Authentication Contexts. There SHOULD NOT be more than one level of such nesting.

125 2.1.1 RACComparison attribute

126 An SP uses the RACComparison attribute of the <rac:RequestedACCombination> element to
127 specify the logical comparison or combination to be performed on the listed Authentication Context
128 classes by the IDP in order to determine the appropriate combined context for any issued statement.

129 This specification defines the following value(s) for the RACComparison attribute. Other additional
130 values MAY be defined.

131 **URI:** urn:oasis:names:tc:SAML:protocol:ext:rac:all

132 Indicates that the authentication context of any resultant statement MUST
133 satisfy the requirements of all the listed
134 <samlp:RequestedAuthenticationContext> elements. This is the default value.

135 **URI:** urn:oasis:names:tc:SAML:protocol:ext:rac:exact

136 Indicates that the authentication context of any resultant statement MUST
137 be the exact match of one of the listed AC classes.

138 **URI:** urn:oasis:names:tc:SAML:protocol:ext:rac:minimum

139 Indicates that the authentication context of any resultant statement MUST
140 be at least as strong (as deemed by the responder) as one of the
141 authentication contexts specified

142 **URI:** urn:oasis:names:tc:SAML:protocol:ext:rac:maximum

143 Indicates that the authentication context of any resultant statement MUST
144 be as strong as possible (as deemed by the responder) without exceeding the strength of at least one of the
145 authentication contexts specified.

146 **URI:** urn:oasis:names:tc:SAML:protocol:ext:rac:better

147 Indicates that the authentication context of any resultant statement MUST
148 be stronger (as deemed by the responder) than any one of the
149 authentication contexts specified.

150 2.2 Example

151 The following is an example of a <rac:RequestedACCombination> element in which the SP is
152 expressing that it desires the resultant <AuthnStatement> to have an Authentication Context that:

- 153 1. represents an authentication event characterized by a mechanism at least as strong as
154 'password' AND
- 155 2. represents an authentication event characterized by an authentication credential that is not
156 shared by multiple users.
- 157 3.

```
158 <rac:RequestedACCombination RACComparison="all">  
159   <rac:RequestedACCombination RACComparison="minimum">  
160     <saml:AuthnContextClassRef>  
161       urn:oasis:names:tc:SAML:2.0:ac:classes:password
```

```
162     </saml:AuthnContextClassRef>
163   </rac:RequestedACCombination>
164   <rac:RequestedACCombination RACComparison="exact">
165     <saml:AuthnContextClassRef>
166       urn:oasis:names:tc:SAML:2.0:ac:ext:classes:sc:unique
167     </saml:AuthnContextClassRef>
168   </rac:RequestedACCombination>
169 </RequestedACCombination>
```

170

171 2.3 Processing Rules

172 This extension is included in a protocol request message by placing it in the optional
173 `<samlp:Extensions>` element. Due to existing processing requirements, all extensions are explicitly
174 deemed optional. Therefore, senders SHOULD only include this extension when they can be reasonably
175 confident that the extension will be understood by the recipient.

176 This extension element MUST NOT be used in conjunction with any protocol message element whose
177 complex type is not derived from the **samlp:RequestAbstractType** complex types.

178 A sender MUST NOT include more than one `<rac:RequestedACCombination>` element in a given
179 request message unless additional elements occur as nested children of the top-most extension,

180 The `<rac:RequestedACCombination>` extension element MUST NOT be used in a message in which
181 there exists a `<samlp:RequestedAuthnContext>` element.

182 A sender MAY specify the logical combination it desires by providing the appropriate URI in the
183 `RACComparison` attribute. If not specified, it is logically equivalent to the `RACComparison` attribute
184 being present with a value of `urn:oasis:names:tc:SAML:protocol:ext:rac:all`.

185 If a `<AuthnRequest>` message's `<samlp:Extensions>` element contains a
186 `<rac:RequestedACCombination>` element, then a responder that understands the extension MUST fulfill
187 the request (if it does so at all) by issuing a `<Response>` containing an assertion with at least one
188 `<AuthnStatement>` element containing an `<AuthnContext>` element that satisfies the specified
189 Authentication Context in the `<rac:RequestedACCombination>` extension.

190 If the responder is unable to satisfy the specified Authentication Context then the responder MUST return
191 a `<Response>` message with a second-level `<StatusCode>` of
192 `urn:oasis:names:tc:SAML:2.0:protocol:NoAuthnContext`.

193 2.4 Metadata Considerations

194 SAML metadata MAY be used to indicate support for this protocol extension at particular protocol
195 endpoints, using the extension capabilities of the metadata schema.

196 Support for this extension is expressed in SAML 2.0 metadata by adding a boolean-typed XML attribute
197 to an element of or derived from the **md:EndpointType** complex type, indicating that SAML request
198 messages sent to that endpoint MAY include this extension.

199 The following schema fragment defines the `rac:supportsRequestedACComb` attribute:

200

```
201 <attribute name="supportsRequestedACComb" type="boolean"/>
```

202 2.4.1 Metadata Example

203 The example below shows a fragmentary `<md:SingleSignOnService>` element that advertises
204 support for the `<rac:RequestedACCombination>` extension. The namespace declaration must be in
205 scope, but the prefix is of course arbitrary.

206

```
207 <md:SingleSignOnService  
208   xmlns:rac="urn:oasis:names:tc:SAML:protocol:ext:rac"  
209   rac:supportsRequestedACComb="1" .../>
```

210 3 References

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

212 3.1 Normative References

- 213 **[RFC 2119]** S. Bradner. *Key words for use in RFCs to Indicate Requirement Levels*. IETF
214 RFC 2119, March 1997. <http://www.ietf.org/rfc/rfc2119.txt>.
- 215 **[SAMLAuthnCxt]** J. Kemp et al. *Authentication Context for the OASIS Security Assertion Markup
216 Language (SAML) V2.0*. OASIS SSTC, March 2005. Document ID saml-authn-
217 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-
218 context-2.0-os.pdf).
- 219 **[SAMLCore]** S. Cantor et al. *Assertions and Protocols for the OASIS Security Assertion
220 Markup Language (SAML) V2.0*. OASIS SSTC, March 2005. Document ID saml-
221 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-
222 os.pdf).
- 223 **[SAMLBind]** S. Cantor et al. *Bindings for the OASIS Security Assertion Markup Language
224 (SAML) V2.0*. OASIS SSTC, March 2005. Document ID saml-bindings-2.0-os.
225 See <http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf>.
- 226 **[SAMLMeta]** S. Cantor et al. *Metadata for the OASIS Security Assertion Markup Language
227 (SAML) V2.0*. OASIS SSTC, March 2005. Document ID saml-metadata-2.0-os.
228 See <http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf>.
- 229 **[SAMLProf]** S. Cantor et al. *Profiles for the OASIS Security Assertion Markup Language
230 (SAML) V2.0*. OASIS SSTC, March 2005. Document ID saml-profiles-2.0-os.
231 See <http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf>.
- 232 **[Schema1]** H. S. Thompson et al. *XML Schema Part 1: Structures*. World Wide Web
233 Consortium Recommendation, May 2001. See [http://www.w3.org/TR/2001/REC-
xmlschema-1-20010502/](http://www.w3.org/TR/2001/REC-
234 xmlschema-1-20010502/).
- 235 **[rac-xsd]** P. Madsen & A. Patel. SAML Requested Authentication Context protocol
236 extension schema. OASIS SSTC, September 2006. Document ID sstc-saml-
237 protocol-ext-rac.xsd. See <http://www.oasis-open.org/committees/security/>.
- 238
- 239

240 **Appendix A. Acknowledgements**

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

- 243 • Hal Lockhart, BEA Systems, Inc.
- 244 • Steve Anderson, BMC Software
- 245 • Thomas Wisniewski, Entrust
- 246 • Ashish Patel, France Telecom
- 247 • Greg Whitehead, Hewlett-Packard
- 248 • Heather Hinton, IBM
- 249 • Anthony Nadalin, IBM
- 250 • Eric Tiffany, IEEE Industry Standards and Technology Org (IEEE-ISTO)
- 251 • Scott Cantor, Internet2
- 252 • Bob Morgan, Internet2
- 253 • Tom Scavo, National Center for Supercomputing Applications (NCSA)
- 254 • Peter Davis, Neustar, Inc.
- 255 • Jeff Hodges, Neustar, Inc.
- 256 • Frederick Hirsch, Nokia Corporation
- 257 • Abbie Barbir, Nortel Networks Limited
- 258 • Paul Madsen, NTT Corporation
- 259 • Ari Kermaier, Oracle Corporation
- 260 • Prateek Mishra, Oracle Corporation
- 261 • John Hughes, PA Consulting
- 262 • Brian Campbell, Ping Identity Corporation
- 263 • Rob Philpott, RSA Security
- 264 • Jahan Moreh, Sigaba Corp.
- 265 • Bhavna Bhatnagar, Sun Microsystems
- 266 • Eve Maler, Sun Microsystems
- 267 • Emily Xu, Sun Microsystems
- 268 • David Staggs, Veterans Health Administration

269 **Appendix B. Notices**

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

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

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

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

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

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