



SAML V2.0 Text-Based Challenge/Response Token Authentication Context Class

Committee Specification 01, May 23, 2007

Document identifier:

sstc-saml-text-based-challenge-response-authn-context-class-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:

Sharon Boeyen (sharon.boeyen@entrust.com), Entrust

Thomas Wisniewski (thomas.wisniewski@entrust.com), Entrust

Contributors:

Abstract:

The current set of standardized SAML V2.0 authentication context definitions cover a subset of challenge/response schemes including those that are based on cryptographic functions and time-based tokens. The notion of text-based challenge/response tokens are not covered by any of the current authentication context definitions.

This document proposes an authentication context class to cover the general case of text-based challenge/response tokens to facilitate signaling their use in SAML. Such schemes include, for example, scratch tokens, numbered list tokens, grid tokens, etc. associated with a challenge/response authentication function. This document also proposes an extension that enables text-based challenge/response token parameters to be specified in relevant authentication contexts. This extension would be included in the <PrincipalAuthenticationMechanism> of such contexts.

Status:

This is a **Committee Specification** approved by the Security Services Technical Committee on 24 August 2009.

Committee members should submit comments and potential errata to the security-services@lists.oasis-open.org/committees/comments/form.php?wg_abbrev=security. The committee will publish on its web page (<http://www.oasis-open.org/committees/security>) a catalog of any changes made to this document as a result of comments.

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

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

Table of Contents

40	1 Introduction.....	3
41	Notation.....	3
42	2 Text-Based Challenge/Response Token Extension.....	4
43	Element <tcr:TextChallengeResponseToken>.....	4
44	Example.....	5
45	3 Text-Based Challenge/Response Authentication Context Class.....	6
46	4 References	7
47	Appendix A. Notices.....	8

48 1 Introduction

49 The current set of SAML V2.0 authentication context class definitions covers a subset of
50 challenge/response schemes, including those that are based on cryptographic functions and time-based
51 tokens. Authentication using text-based challenge/response tokens is not covered by any of the current
52 authentication context class specifications.

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

56 This specification defines an extension to the SAML V2.0 Authentication Context core schema
57 specification that can be optionally used to convey parameters associated with text-based
58 challenge/response tokens. This specification also introduces one new authentication context class for
59 use with text-based challenge/response tokens.

60 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 [RFC 2119].

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

<i>Prefix</i>	<i>XML Namespace</i>	<i>Comments</i>
saml:	urn:oasis:names:tc:SAML:2.0:assertion	This is the SAML V2.0 assertion namespace [SAMLCore].
ac:	urn:oasis:names:tc:SAML:2.0:ac	This is the SAML new core authentication context schema namespace for SAML V2.0 [SAMLAuthnCtx].
xs:	http://www.w3.org/2001/XMLSchema	This namespace is defined in the W3C XML Schema specification [SAMLCore].
tcr:	urn:oasis:names:tc:SAML:ac:ext:tcr	This is the text-based challenge/response token extension namespace developed herein and in the accompanying schema [TCR-xsd].

68

2 Text-Based Challenge/Response Token Extension

In some environments authentication is performed using text-based challenge/response tokens of various types such as scratch tokens, grid tokens and numbered list tokens. These tokens share a common set of parameters that are key to the assessment of the quality of the authentication performed.

This section defines an extension to the SAML V2.0 authentication context schema that can be used to express these parameters in an authentication context. The extension may optionally appear within the `<ac:PrincipalAuthenticationMechanismType>` element.

Element `<tcr:TextChallengeResponseToken>`

The `<tcr:TextChallengeResponseToken>` element is used to indicate the use of a text-based challenge/response token in authentication.

The following schema fragment defines the `<tcr:TextChallengeResponseToken>` element:

```
<xs:element name="TextBasedChallengeResponseToken"
  type="tcr:TextBasedChallengeResponseType"/>
  <xs:annotation>
    <xs:documentation>This element can only appear as an Extension in
PrincipalAuthenticationMechanismType</xs:documentation>
  </xs:annotation>
  <xs:complexType name="TextBasedChallengeResponseType">
    <xs:annotation>
      <xs:documentation>Identifies the type of token and
authentication</xs:documentation>
    </xs:annotation>
    <xs:sequence>
      <xs:element name="TokenDescription" type="xs:anyURI">
        <xs:annotation>
          <xs:documentation>A URI pointing to descriptive information
about the type of text-based challenge response scheme supported by the
token</xs:documentation>
        </xs:annotation>
      </xs:element>
      <xs:element name="TokenParameters" minOccurs="0">
        <xs:complexType>
          <xs:sequence>
            <xs:element name="NumberOfPossibleChallenges"
type="xs:positiveInteger">
              <xs:annotation>
                <xs:documentation>The total number of possible
challenges represented on the token</xs:documentation>
              </xs:annotation>
            </xs:element>
            <xs:element name="NumberOfPossibleValues"
type="xs:positiveInteger">
              <xs:annotation>
                <xs:documentation>The total number of possible
values for each response</xs:documentation>
              </xs:annotation>
            </xs:element>
            <xs:element name="NumberOfChallenges"
type="xs:positiveInteger">
              <xs:annotation>
                <xs:documentation>The number of challenges used in
an authentication operation</xs:documentation>
              </xs:annotation>
            </xs:element>
          </xs:sequence>
        </xs:complexType>
      </xs:element>
      <xs:element name="TokenAuthenticated" type="xs:boolean" minOccurs="0">
        <xs:annotation>
          <xs:documentation>An indication of whether the token identity
(eg serial number) was checked</xs:documentation>
        </xs:annotation>
      </xs:element>
    </xs:sequence>
  </xs:complexType>

```

```
130         </xs:annotation>
131     </xs:element>
132 </xs:sequence>
133 </xs:complexType>
134 </xs:element>
```

135 An overview of the the sub-elements contained within this element is provided below:

- 136 ● `<tcr:TokenDescription>`: This element is mandatory and contains a URI that points to a
137 description of the type of text-based challenge/response mechanism used in conjunction with
138 the token (for example, scratch, grid, etc.).
- 139 ● `<tcr:TokenParameters>`: If present, this element provides the necessary information
140 about an authentication to enable a determination of the quality of that authentication. These
141 parameters include an indication of the number of possible challenges (e.g., number of
142 scratch boxes on a scratch token, number of cells on a grid token, etc.), an indication of the
143 number of possible values for each challenge (e.g., the total number of possible images that
144 could be contained in each box on a scratch card) and the number of challenges conducted as
145 part of a specific authentication instance.
- 146 ● `<tcr:TokenAuthenticated>`: If present, this element indicates whether a check is
147 conducted to ensure the proper token was used (e.g., a serial number check was conducted).

148 Example

149 Following is an example of an Authentication Context declaration in which a scratch card
150 challenge/response token was used. In this example, there are 50 spaces on the scratch card, of which 4
151 were challenged. There are 150 values that could appear in each space. Also, in this example, the
152 identity of the scratch card was verified.

```
154 <ac:AuthenticationContextDeclaration>
155   <ac:AuthnMethod>
156     <ac:PrincipalAuthenticationMechanism>
157       <ac:Extension>
158         <tcr:TextBasedChallengeResponseToken>
159           <tcr:TokenDescription>
160             http://www.examplechallengeresponsetoken.com
161           </tcr:TokenDescription>
162
163           <tcr:TokenParameters>
164             <tcr:NumberOfPossibleChallenges>50</tcr:NumberOfPossibleChallenges>
165             <tcr:NumberOfPossibleValues>150</tcr:NumberOfPossibleValues>
166             <tcr:NumberOfChallenges>4</tcr:NumberOfChallenges>
167           </tcr:TokenParameters>
168
169           <tcr:TokenAuthenticated>true</tcr:TokenAuthenticated>
170         </tcr:TextBasedChallengeResponseToken>
171       </ac:Extension>
172     </ac:PrincipalAuthenticationMechanism>
173   </ac:AuthnMethod>
174 </ac:AuthenticationContextDeclaration>
```

3 Text-Based Challenge/Response Authentication Context Class

177

178

179 The following Authentication Context class is defined to represent authentication using text-based
180 challenge/response tokens and makes use of the text-based challenge/response token extension.

181 **URI:** urn:oasis:names:tc:SAML:2.0:ac:classes:TextBasedChallengeResponse

182 This class defines a text-based challenge/response token used in authentication.

```
183 <?xml version="1.0" encoding="UTF-8"?>
184 <xs:schema
185   targetNamespace=
186   "urn:oasis:names:tc:SAML:2.0:ac:classes:TextBasedChallengeResponse"
187   xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:TextBasedChallengeResponse"
188   xmlns:xs="http://www.w3.org/2001/XMLSchema" blockDefault="substitution"
189   finalDefault="extension" version="2.0">
190   <xs:redefine
191     schemaLocation=
192     "http://docs.oasis-open.org/security/saml/v2.0/saml-schema-authn-context-types-
193     2.0.xsd">
194     <xs:complexType name="AuthnContextDeclarationBaseType">
195       <xs:complexContent>
196         <xs:restriction base="AuthnContextDeclarationBaseType">
197           <xs:sequence>
198             <xs:element ref="Identification" minOccurs="0"/>
199             <xs:element ref="TechnicalProtection" minOccurs="0"/>
200             <xs:element ref="OperationalProtection" minOccurs="0"/>
201             <xs:element ref="AuthnMethod"/>
202             <xs:element ref="GoverningAgreements" minOccurs="0"/>
203             <xs:element ref="Extension" minOccurs="0"
204             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     <xs:complexType name="AuthnMethodBaseType">
211       <xs:complexContent>
212         <xs:restriction base="AuthnMethodBaseType">
213           <xs:sequence>
214             <xs:element ref="PrincipalAuthenticationMechanism"/>
215             <xs:element ref="Authenticator" minOccurs="0"/>
216             <xs:element ref="AuthenticatorTransportProtocol"
217             minOccurs="0"/>
218             <xs:element ref="Extension" minOccurs="0"
219             maxOccurs="unbounded"/>
220           </xs:sequence>
221         </xs:restriction>
222       </xs:complexContent>
223     </xs:complexType>
224     <xs:complexType name="PrincipalAuthenticationMechanismType">
225       <xs:complexContent>
226         <xs:restriction base="PrincipalAuthenticationMechanismType">
227           <xs:sequence>
228             <xs:annotation>
229               <xs:documentation>The only element that can appear in
230               Extension is tcr:TextChallengeResponseToken</xs:documentation>
231             </xs:annotation>
232             <xs:element ref="Extension"/>
233           </xs:sequence>
234         </xs:restriction>
235       </xs:complexContent>
236     </xs:complexType>
237   </xs:redefine>
238 </xs:schema>
```

239 4 References

- 240 **[RFC 2119]** S. Bradner. *Key words for use in RFCs to indicate requirement levels*. IETF RFC
241 2119, March 1997. <http://www.ietf.org/rfc/rfc2119.txt>.
- 242 **[SAMLAC-xsd]** J. Kemp et al. SAML authentication context schema. OASIS SSTC, March 2005.
243 See [http://docs.oasis-open.org/security/saml/v2.0/saml-schema-authn-context-
244 2.0.xsd](http://docs.oasis-open.org/security/saml/v2.0/saml-schema-authn-context-2.0.xsd).
- 245 **[SAMLAuthnCtx]** J. Kemp et al. *Authentication Context for the OASIS Security Assertion Markup
246 Language (SAML) V2.0*. OASIS SSTC, March 2005. Document ID saml-
247 authncontext-2.0-os. [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-
248 context-2.0-os.pdf).
- 249 **[SAMLCore]** S. Cantor et al. *Assertions and Protocols for the OASIS Security Assertion Markup
250 Language (SAML) V2.0*. OASIS SSTC, March 2005. Document ID saml-core-2.0-os.
251 <http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf> .
- 252 **[TCR-xsd]** S. Boeyen and T. Wisniewski. *SAML Text-based Challenge/Response Token
253 Authentication Context extension schema*. OASIS SSTC, July 2006. Document ID
254 sstc-saml-authncontext-tcr.xsd. See [http://www.oasis-
open.org/committees/security/](http://www.oasis-
255 open.org/committees/security/).
- 256 **[XMLSchema]** H.S. Thompson et al. *XML Schema Part 1: Structures*. World Wide Web Consortium
257 Recommendation, May 2001. See <http://www.w3.org/TR/xmlschema-1/>.

258 **Appendix A. Notices**

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

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

270 **Copyright © OASIS Open 2009. All Rights Reserved.**

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

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

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