



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

Committee Draft 01, 28 September 2006

Document identifier:

sstc-saml-text-based-challenge-response-authn-context-class-cd-01

Location:

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

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 Draft** approved by the Security Services Technical Committee on 26 September 2006.

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

Table of Contents

35	1 Introduction.....	3
36	Notation.....	3
37	2 Text-Based Challenge/Response Token Extension.....	4
38	Element <tcr:TextChallengeResponseToken>.....	4
39	Example.....	5
40	3 Text-Based Challenge/Response Authentication Context Class.....	6
41	4 References	7
42	Appendix A. Notices.....	8

43 1 Introduction

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

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

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

55 Notation

56 This specification uses normative text.

57 The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD
58 NOT", "RECOMMENDED", "MAY", AND "OPTIONAL" in this specification are to be interpreted as
59 described in [RFC 2119].

60 Conventional XML namespace prefixes are used throughout the listings in this specification to stand for
61 their respective namespaces as follows, whether or not a namespace declaration is present in the
62 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].

63

64 2 Text-Based Challenge/Response Token Extension

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

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

71 Element <tcr:TextChallengeResponseToken>

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

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

```
75 <xs:element name="TextBasedChallengeResponseToken"  
76 type="tcr:TextBasedChallengeResponseType"/>  
77 <xs:annotation>  
78 <xs:documentation>This element can only appear as an Extension in  
79 PrincipalAuthenticationMechanismType</xs:documentation>  
80 </xs:annotation>  
81 <xs:complexType name="TextBasedChallengeResponseType">  
82 <xs:annotation>  
83 <xs:documentation>Identifies the type of token and  
84 authentication</xs:documentation>  
85 </xs:annotation>  
86 <xs:sequence>  
87 <xs:element name="TokenDescription" type="xs:anyURI">  
88 <xs:annotation>  
89 <xs:documentation>A URI pointing to descriptive information  
90 about the type of text-based challenge response scheme supported by the  
91 token</xs:documentation>  
92 </xs:annotation>  
93 </xs:element>  
94 <xs:element name="TokenParameters" minOccurs="0">  
95 <xs:complexType>  
96 <xs:sequence>  
97 <xs:element name="NumberOfPossibleChallenges"  
98 type="xs:positiveInteger">  
99 <xs:annotation>  
100 <xs:documentation>The total number of possible  
101 challenges represented on the token</xs:documentation>  
102 </xs:annotation>  
103 </xs:element>  
104 <xs:element name="NumberOfPossibleValues"  
105 type="xs:positiveInteger">  
106 <xs:annotation>  
107 <xs:documentation>The total number of possible  
108 values for each response</xs:documentation>  
109 </xs:annotation>  
110 </xs:element>  
111 <xs:element name="NumberOfChallenges"  
112 type="xs:positiveInteger">  
113 <xs:annotation>  
114 <xs:documentation>The number of challenges used in  
115 an authentication operation</xs:documentation>  
116 </xs:annotation>  
117 </xs:element>  
118 </xs:sequence>  
119 </xs:complexType>  
120 </xs:element>  
121 <xs:element name="TokenAuthenticated" type="xs:boolean" minOccurs="0">  
122 <xs:annotation>  
123 <xs:documentation>An indication of whether the token identity  
124 (eg serial number) was checked</xs:documentation>
```

```
125         </xs:annotation>
126     </xs:element>
127 </xs:sequence>
128 </xs:complexType>
129 </xs:element>
```

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

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

143 Example

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

```
148
149 <ac:AuthenticationContextDeclaration>
150     <ac:AuthnMethod>
151         <ac:PrincipalAuthenticationMechanism>
152             <ac:Extension>
153                 <tcr:TextBasedChallengeResponseToken>
154                     <tcr:TokenDescription>
155                         http://www.examplechallengeresponsetoken.com
156                     </tcr:TokenDescription>
157
158                     <tcr:TokenParameters>
159                         <tcr:NumberOfPossibleChallenges>50</tcr:NumberOfPossibleChallenges>
160                         <tcr:NumberOfPossibleValues>150</tcr:NumberOfPossibleValues>
161                         <tcr:NumberOfChallenges>4</tcr:NumberOfChallenges>
162                     </tcr:TokenParameters>
163
164                     <tcr:TokenAuthenticated>true</tcr:TokenAuthenticated>
165                 </tcr:TextBasedChallengeResponseToken>
166             </ac:Extension>
167         </ac:PrincipalAuthenticationMechanism>
168     </ac:AuthnMethod>
169 </ac:AuthenticationContextDeclaration>
```

3 Text-Based Challenge/Response Authentication Context Class

172

173

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

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

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

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

234 **4 References**

235 **[RFC 2119]** S. Bradner. *Key words for use in RFCs to indicate requirement levels*. IETF RFC
236 2119, March 1997. <http://www.ietf.org/rfc/rfc2119.txt>.

237 **[SAMLAC-xsd]** J. Kemp et al. SAML authentication context schema. OASIS SSTC, March 2005.
238 See [http://docs.oasis-open.org/security/saml/v2.0/saml-schema-authn-context-](http://docs.oasis-open.org/security/saml/v2.0/saml-schema-authn-context-2.0.xsd)
239 [2.0.xsd](http://docs.oasis-open.org/security/saml/v2.0/saml-schema-authn-context-2.0.xsd).

240 **[SAMLAuthnCtx]** J. Kemp et al. *Authentication Context for the OASIS Security Assertion Markup*
241 *Language (SAML) V2.0*. OASIS SSTC, March 2005. Document ID saml-
242 authncontext-2.0-os. [http://docs.oasis-open.org/security/saml/v2.0/saml-authn-](http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf)
243 [context-2.0-os.pdf](http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf).

244 **[SAMLCore]** S. Cantor et al. *Assertions and Protocols for the OASIS Security Assertion Markup*
245 *Language (SAML) V2.0*. OASIS SSTC, March 2005. Document ID saml-core-2.0-os.
246 <http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf> .

247 **[TCR-xsd]** S. Boeyen and T. Wisniewski. *SAML Text-based Challenge/Response Token*
248 *Authentication Context extension schema*. OASIS SSTC, July 2006. Document ID
249 sstc-saml-authncontext-tcr.xsd. See [http://www.oasis-](http://www.oasis-open.org/committees/security/)
250 [open.org/committees/security/](http://www.oasis-open.org/committees/security/).

251 **[XMLSchema]** H.S. Thompson et al. *XML Schema Part 1: Structures*. World Wide Web Consortium
252 Recommendation, May 2001. See <http://www.w3.org/TR/xmlschema-1/>.

253 **Appendix A. Notices**

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

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

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

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

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

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