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

1 Introduction

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

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

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

Notation

This specification uses normative text.

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

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

Prefix	***XML Namespace***	***Comments***
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].

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:TextBasedChallengeResponseTokenType"/>
    <xs:annotation>
        <xs:documentation>This element can only appear as an Extension in
PrincipalAuthenticationMechanismType</xs:documentation>
    </xs:annotation>
    <xs:complexType name="TextBasedChallengeResponseTokenType">
        <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>
</xs:element>
```

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

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

Example

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

```
<ac:AuthenticationContextDeclaration>
    <ac:AuthnMethod>
        <ac:PrincipalAuthenticationMechanism>
            <ac:Extension>
                <tcr:TextBasedChallengeResponseToken>
                    <tcr:TokenDescription>
                    http://www.examplechallengeresponsetoken.com
                    </tcr:TokenDescription>

                        <tcr:TokenParameters>
              <tcr:NumberOfPossibleChallenges>50</tcr:NumberOfPossibleChallenges>
              <tcr:NumberOfPossibleValues>150</tcr:NumberOfPossibleValues>
              <tcr:NumberOfChallenges>4</tcr:NumberOfChallenges>
                        </tcr:TokenParameters>

                       <tcr:TokenAuthenticated>true</tcr:TokenAuthenticated>

                </tcr:TextBasedChallengeResponseToken>
            </ac:Extension>
        </ac:PrincipalAuthenticationMechanism>
    </ac:AuthnMethod>
</ac:AuthenticationContextDeclaration>
```

3 Text-Based Challenge/Response Authentication Context Class

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

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

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

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
    targetNamespace=
"urn:oasis:names:tc:SAML:2.0:ac:classes:TextBasedChallengeResponse"
    xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:TextBasedChallengeResponse"
    xmlns:xs="http://www.w3.org/2001/XMLSchema" blockDefault="substitution"
finalDefault="extension" version="2.0">
    <xs:redefine
        schemaLocation=
"http://docs.oasis-open.org/security/saml/v2.0/saml-schema-authn-context-types-
2.0.xsd">
        <xs:complexType name="AuthnContextDeclarationBaseType">
            <xs: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:element ref="GoverningAgreements" minOccurs="0"/>
                        <xs:element ref="Extension" minOccurs="0”
maxOccurs="unbounded"/>
                    </xs:sequence>
                    <xs:attribute name="ID" type="xs:ID" use="optional"/>
                </xs:restriction>
            </xs:complexContent>
        </xs:complexType>
        <xs:complexType name="AuthnMethodBaseType">
            <xs:complexContent>
                <xs:restriction base="AuthnMethodBaseType">
                    <xs:sequence>
                        <xs:element ref="PrincipalAuthenticationMechanism"/>
                        <xs:element ref="Authenticator" minOccurs="0"/>
                        <xs:element ref="AuthenticatorTransportProtocol"
minOccurs="0"/>
                        <xs:element ref="Extension" minOccurs="0"
maxOccurs="unbounded"/>
                    </xs:sequence>
                </xs:restriction>
            </xs:complexContent>
        </xs:complexType>
        <xs:complexType name="PrincipalAuthenticationMechanismType">
            <xs:complexContent>
                <xs:restriction base="PrincipalAuthenticationMechanismType">
                    <xs:sequence>
                        <xs:annotation>
                            <xs:documentation>The only element that can appear in
Extension is tcr:TextChallengeResponseToken</xs:documentation>
                        </xs:annotation>
                        <xs:element ref="Extension"/>
                    </xs:sequence>
                </xs:restriction>
            </xs:complexContent>
        </xs:complexType>
    </xs:redefine>
</xs:schema>
```

4 References

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

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

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

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

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

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

Appendix A. Notices

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

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