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

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

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

1.1 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 :

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

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

```
Listings of XML schemas appear like this.
```

```
Example code listings appear like this.
```

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
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.

This specification uses the following typographical conventions in text: <SAMLElement>, <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>

<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>
```

```
</ac:AuthnContextDeclaration>
```

2.3 Processing Rules

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

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

A <sc:SharedCredential> element MUST NOT appear in any other <ac:Extension> element 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">
      <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" minOccurs="0"/>
            <xs:element ref="Authenticator"/>
            <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:element ref="Extension" minOccurs="1"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>
  </redefine>

</schema>
```

3.1.2 Unique Credential

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

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

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

```
<?xml version="1.0" encoding="UTF-8"?>
<schema targetNamespace="urn:oasis:names:tc:SAML:2.0:ac:classes:ext:sc:unique"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:oasis:names:tc:SAML:2.0:ac:classes:ext:sc:unique"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

 <redefine schemaLocation="sstc-saml-context-ext-sc.xsd">

  <xs:annotation>
    <xs:documentation>This class is defined by a fixed value of '0' for the
      SharedCredential extension, indicating that the credential was uniquely
      held.
    </xs:documentation>
  </xs:annotation>
  <complexType name="SharedCredentialType">
```

```
    <complexContent>
      <restriction base="SharedCredentialType">
         <simpleContent>
          <extension  base="xs:boolean" fixed="0"/>
         </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">
      <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" minOccurs="0"/>
            <xs:element ref="Authenticator"/>
            <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:element ref="Extension" minOccurs="1"/>
          </xs:sequence>
        </xs:restriction>
      </xs:complexContent>
    </xs:complexType>
  </redefine>

</schema>
```

4 References

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

4.1 Normative 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.

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

[SAMLAC-schema] *J. Kemp et al. SAML authentication context schema.*OASIS SSTC, March 2005. Document ID saml-authn-context-2.0-os.

[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. See http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf.

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

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

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

[Schema1] H. S. Thompson et al. *XML Schema Part 1: Structures.* World Wide Web Consortium Recommendation, May 2001. See http://www.w3.org/TR/2001/REC-xmlschema-1-20010502/.

[sc-xsd] P. Madsen & A. Patel. SAML Shared Credential Authentication Context extension schema. OASIS SSTC, September 2006. Document ID sstc-saml-context-ext-sc.xsd. See http://www.oasis-open.org/committees/security/.

Appendix A. Acknowledgements

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

- Hal Lockhart, BEA Systems, Inc.
- Steve Anderson, BMC Software
- Thomas Wisniewski, Entrust
- Ashish Patel, France Telecom
- Greg Whitehead, Hewlett-Packard
- Heather Hinton, IBM
- Anthony Nadalin, IBM
- Eric Tiffany, IEEE Industry Standards and Technology Org (IEEE-ISTO)
- Scott Cantor, Internet2
- Bob Morgan, Internet2
- Tom Scavo, National Center for Supercomputing Applications (NCSA)
- Peter Davis, Neustar, Inc.
- Jeff Hodges, Neustar, Inc.
- Frederick Hirsch, Nokia Corporation
- Abbie Barbir, Nortel Networks Limited
- Paul Madsen, NTT Corporation
- Ari Kermaier, Oracle Corporation
- Prateek Mishra, Oracle Corporation
- John Hughes, PA Consulting
- Brian Campbell, Ping Identity Corporation
- Rob Philpott, RSA Security
- Jahan Moreh, Sigaba Corp.
- Bhavna Bhatnagar, Sun Microsystems
- Eve Maler, Sun Microsystems
- Emily Xu, Sun Microsystems
- David Staggs, Veterans Health Administration

Appendix B. 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.