GWD-R-P
OGSA Authorization Working Group

Valerio Venturi, INFN
Tom Scavo, NCSA
David Chadwick, University of Kent
7 April 2008

Use of SAML to retrieve Authorization Credentials

Status of This Document

This document provides information to the Grid community about a proposed standards track protocol. Distribution is unlimited.

Abstract

This document presents a specification for an authorization credential retrieval protocol based on the use of the Security Assertion Markup Language (SAML) and protocol as a format for requesting and retrieving attribute assertions.

ogsa-authz-wg@ogf.org

Venturi, Scavo, Chadwick

7 April 2008

Contents

Joel Replogle 7/31/08 5:10 PM
Deleted: 1. Introduction 3
2. Notational Conventions 3
3. SAML Protocols and Bindings Usage 4
4. SAML Element Usage 4
4.1 Attribute Element 4
5. Security Consideration 4
6. Contributors 4
7. Intellectual Property Statement 4
8. Disclaimer 5
9. Full Copyright Notice 5
10. References 5

1. Introduction

This document presents a specification for an authorization credential retrieval protocol in which a client requests attribute assertions about a subject (the Access Requestor) from a Credential Issuing Service (CIS), as shown in Figures 1 and 2. The client may be the subject itself (as in Figure 1) or may be a component of the grid service provider (i.e. the Credential Validation Service, as shown in Figure 2).

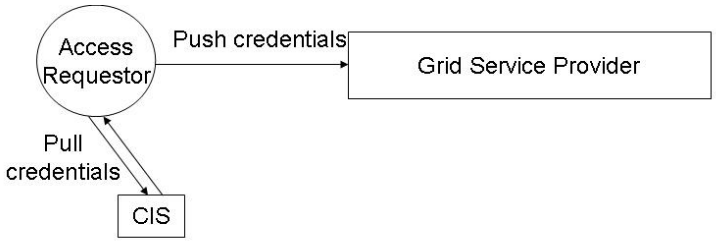

Fig 1 Self Query Mode of Operation

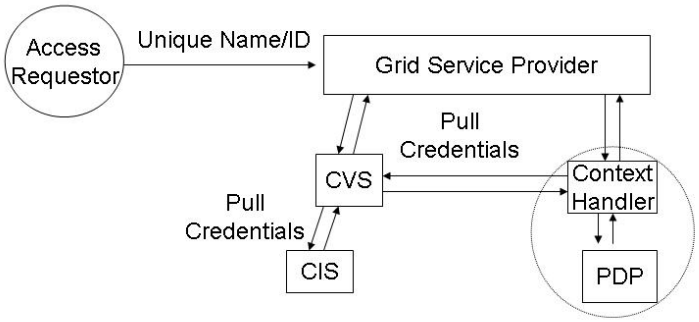

Fig 2 Third Party Query Mode of Operation

This specification is based on the OASIS Security Assertion Markup Language (SAML) V2.0 request-response protocol for requesting and expressing attribute assertions. SAML, developed by the Security Services Technical Committee (TC) of OASIS,[1] is an XML-based framework for communicating user authentication, attribute, and authorization decision information. It allows entities to make assertions regarding the identity, attributes and authorization decisions of a subject to other entities. In particular, SAML is used to enable attribute-based access control, where one entity communicates attributes about a subject in support of access control decisions made by another entity.

The core SAML specification is the *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0* [SAMLCore], which defines the XML format used to express assertions and the protocol messages used to request assertions from a SAML authority. Of special interest is the Assertion Query and Request Protocol [SAMLCore] used to formulate an attribute query. The companion specification *Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0* [SAMLBind] defines bindings that map the protocols defined in [SAMLCore] onto standard message or communication protocols. For example, the SAML SOAP Binding [SAMLBind] is used in conjunction with the Assertion Query and Request Protocol to

[1] http://www.oasis-open.org/committees/security/

profile an attribute exchange. Finally, the *Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0* [SAMLProf] specifies certain combinations of protocols and bindings. In particular, the Assertion Query/Request Profile is a basic profile underlying the exchange of attribute assertions, including the credential issuing protocol specified in this document.

The *SAML V2.0 Deployment Profile for X.509 Subjects* [SAMLX509] is an extension of the Assertion Query/Request Profile that describes how a subject that possesses an X.509 public key certificate is represented as a SAML Subject, how an attribute assertion regarding such a subject is produced and consumed, and how two entities exchange attribute assertions about such a subject. The *Use of SAML to retrieve authorization credentials* is an extension of the SAML V2.0 Deployment Profile for X.509 Subjects, and therefore the former assumes an environment that relies on X.509 subject authentication.

Section 2 describes the conventions and namespaces used in this document. Section 3 is normative and defines how to use SAML protocols and bindings when requesting, asserting, and consuming attribute assertions. Section 4 is normative and defines how SAML elements should be used when formulating requests and responses. This document concludes with security considerations, author affiliations and contact information, copyright and intellectual property statements, and references. Appendix A presents a non-normative WSDL that can be used to build a conformant service.

2. Notational Conventions

The key words ‘MUST,” “MUST NOT,” “REQUIRED,” “SHALL,” “SHALL NOT,” “SHOULD,” “SHOULD NOT,” “RECOMMENDED,” “MAY,” and “OPTIONAL” are to be interpreted as described in RFC 2119 [RFC2119].

This specification uses namespace prefixes throughout. These prefixes are listed in Table 1. Note that the choice of any namespace prefix is arbitrary and not semantically significant.

Table 1: Namespace prefixes used in this specification

Prefix	Namespace
`saml`	`urn:oasis:names:tc:SAML:2.0:assertion`
`samlp`	`urn:oasis:names:tc:SAML:2.0:protocol`

3. SAML Protocols and Bindings Usage

This section is normative and describes how to use SAML protocols and bindings when retrieving authorization credentials.

A client implementation of this specification is called a conforming *Extended Mode X.509 Attribute Query/Requester* or a conforming *Extended Mode X.509 Attribute Self-Query/Requester* as described in section 5 of [SAMLX509]. On the server side, an implementation of this specification is called a conforming *Extended Mode X.509 Attribute Query/Responder* or a conforming *Extended Mode X.509 Attribute Self-Query/Responder*, respectively.

4. SAML Element Usage

This section is normative, and describes how to use SAML elements when requesting attribute assertions from a conforming credential issuing service and when responding to requests.

Unless stated otherwise, SAML elements MUST be conformant to [SAMLX509].

4.1 Attribute Element

Attributes in a SAML attribute assertion may be used when requesting an authorization decision

according to the eXtensible Access Control Markup Language (XACML) [XACML] specification and OGF profile [XACMLProf]. Since the SAML and XACML attribute formats differ, an XACML Attribute Profile is defined in [SAMLProf] to facilitate mapping between the two formats.

The SAML Attribute elements MUST conform to the XACML Attribute Profile. Since a SAML Attribute may satisfy multiple attribute profiles simultaneously, an Attribute that satisfies this profile MAY satisfy other profiles in addition to the XACML Attribute Profile. For example, a conforming SAML Attribute MAY satisfy both the XACML Attribute Profile and the X.500/LDAP Attribute Profile (see the last example in section 8 of [SAMLProf] for instance).

4.2 <saml:Subject> Usage

The <saml:NameID> option SHOULD be used. The <saml:EncryptedID> element should not be used. Confidentiality MUST be provided by the underlying SSL/TLS connection (see Section 5).

5. Security Consideration

This specification profiles a SAML attribute query/response that returns attribute assertions that relying parties can use to derive authorization decisions. Implementers of this specification need to be aware that errors in implementation could lead to improper granting of services to unauthorized users. Furthermore sniffing of the communications could reveal sensitive information about the subject.

For these reasons mutual authentication and confidentiality MUST be provided by SSLv 3.0 [SSL] or TLS v1.0 [RFC2246] and a strong cipher (of at least 128 bits) MUST be selected. In addition, the <samlp:AttributeQuery>, <saml:Assertion> and <samlp:Response> elements MAY be signed.

> Note that SAML does not provide a means for encrypting (confidentially protecting) entire request messages, except via the underlying transport layer security, although it does allow SAML subject IDs to be encrypted in the request and entire assertions to be encrypted in the response. For these reasons this profile mandates the use of SSL/TLS encryption.

6. Contributors

Valerio Venturi
INFN
valerio.venturi@cnaf.infn.it

Tom Scavo
National Center for Supercomputing Applications
tscavo@ncsa.uiuc.edu

David W. Chadwick
The Computing Laboratory
University of Kent
D.W.Chadwick@kent.ac.uk

7. Intellectual Property Statement

The OGF 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. 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 implementers or users of this specification can be obtained from the OGF Secretariat.

The OGF 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 practice this recommendation. Please address the information to the OGF Executive Director.

8. Disclaimer

This document and the information contained herein is provided on an “As Is” basis and the OGF disclaims all warranties, express or implied, including but not limited to any warranty that the use of the information herein will not infringe any rights or any implied warranties of merchantability or fitness for a particular purpose.

9. Full Copyright Notice

10. References

[RFC2119] S. Bradner. *Key Words for Use in RFCs to Indicate Requirement Levels*, RFC 2119. March 1997. http://www.ietf.org/rfc/rfc2119.txt

[RFC2246] Dierks, T., Allen, C. "The TLS Protocol Version 1.0", RFC 2246, January 1999.

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

[SAMLProf] S. Cantor et al. *Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS Standard, March 2005. http://docs.oasis-

open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf

[SAMLX509] T. Scavo. *SAML V2.0 Deployment Profiles for X.509 Subjects*. OASIS Committee Draft, August 2007. Document ID sstc-saml2-profiles-deploy-x509-cd-02. http://wiki.oasis-open.org/security/SstcSaml2X509ProfilesDeploy

[SSL] Frier, A., Karlton, P., Kocher, P. (1996). 'The SSL 3.0 Protocol', Netscape Communications Corp., Nov 18, 1996.

[XACML] T. Moses. *eXtensible Access Control Markup Language (XACML) Version 2.0*. OASIS Standard, February 2005. http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf

[XACMLProf] David W Chadwick, Linying Su, Romain Laborde "Use of XACML Request Context to Obtain an Authorisation Decision". OGF Authz WG Draft, 31 March 2008

Appendix A. WSDL

This section is non-normative and presents a WSDL document that describes a service conformant to section 3. This WSDL is inspired by the one published by the OASIS Security Service TC (http://www.oasis-open.org/committees/download.php/23975/saml-2.0.wsdl).

```
<?xml version="1.0" encoding="UTF-8"?>
<definitions

    targetNamespace=”http://schemas.ggf.org/authz/2007/12/aep"
   xmlns:tns="urn:oasis:names:tc:SAML:2.0:protocol:wsdl"
    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
    xmlns="http://schemas.xmlsoap.org/wsdl/">

  <import namespace="urn:oasis:names:tc:SAML:2.0:protocol"
        location="saml-schema-protocol-2.0.xsd"/>

  <message name="AttributeQueryMessage">
    <part name="body" element="samlp:AttributeQuery"/>
  </message>

  <message name="ResponseMessage">
    <part name="body" element="samlp:Response"/>
  </message>

  <portType name="AttributeServicePortType">
    <operation name="AttributeQuery">
      <input message="tns:AttributeQueryMessage"/>
      <output message="tns:ResponseMessage"/>
    </operation>
  </portType>

  <binding name="AttributeServiceSoapBinding"
    type="tns:AttributeServicePortType">
    <soap:binding style="document"
       transport="http://schemas.xmlsoap.org/soap/http"/>
    <operation name="AttributeQuery">
      <soap:operation
soapAction="http://http://schemas.ggf.org/authz/2007schemas.ggf.org/authz/2007/12/aep/Attri
buteServicePortType/AttributeQuery"/>
      <input>
        <soap:body use="literal"/>
      </input>
      <output>
        <soap:body use="literal"/
      </output>
    </operation>
  </binding>

</definitions>
```

Valerio Venturi
Comment: Change name, targetNamespace, and action.

Appendix B. Examples

This section is non normative and provides examples.

The following is an AttributeQuery issued by the subject in the case of the *SAML Attribute Self-Query Deployment Profile for X.509 Subjects*.

```
<samlp:AttributeQuery
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  ID="aaf23196-1773-2113-474a-fe114412ab72"
  Version="2.0"
  IssueInstant="2006-07-17T20:31:40Z">
  <saml:Issuer
    Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
    C=US, O=NCSA-TEST, OU=User, CN=trscavo@uiuc.edu
  </saml:Issuer>
  <saml:Subject>
    <saml:NameID
      Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
      C=US, O=NCSA-TEST, OU=User, CN=trscavo@uiuc.edu
    </saml:NameID>
  </saml:Subject>
  <saml:Attribute
    xmlns:xacmlprof="urn:oasis:names:tc:SAML:2.0:profiles:attribute:XACML"
    xmlns:ldapprof="urn:oasis:names:tc:SAML:2.0:profiles:attribute:LDAP"
    xacmlprof:DataType="http://www.w3.org/2001/XMLSchema#string"
    ldapprof:Encoding="LDAP"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
    Name="urn:oid:2.5.4.42" FriendlyName="givenName">
  </saml:Attribute>
</samlp:AttributeQuery>
```

In response to the previous query, a responder will return the following SAML Assertion (where the containing SAML Response has been omitted for clarity).

```
<saml:Assertion
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
  ID="_33776a319493ad607b7ab3e689482e45"
  Version="2.0"
  IssueInstant="2006-07-17T20:31:41Z">
  <saml:Issuer>https://idp.example.org/saml</saml:Issuer>
  <ds:Signature>...</ds:Signature>
  <saml:Subject>
    <saml:NameID
      Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
      C=US, O=NCSA-TEST, OU=User, CN=trscavo@uiuc.edu
    </saml:NameID>
    <saml:SubjectConfirmation
      Method="urn:oasis:names:tc:SAML:2.0:cm:holder-of-key">
      <saml:SubjectConfirmationData>
        <ds:KeyInfo>
          <ds:X509Data>
            <!-- principal's X.509 cert -->
            <ds:X509Certificate>
MIICiDCCAXACCQDE+9eiWrm62jANBgkqhkiG9w0BAQQFADBFMQswCQYDVQQGEwJV
UzESMBAGA1UEChMJTkNTQS1URVNUMQ0wCwYDVQQLEwRVc2VyMRMwEQYDVQQDEwpT
UC1TZXJ2aWNlMB4XDTA2MDcxNzIwMjE0MVoXDTA2MDcxODIwMjE0MVowSzELMAkG
```

```
A1UEBhMCVVMxEjAQBgNVBAoTCU5DU0EtVEVTVDENMAsGA1UECxMEVXNlcjEZMBcG
A1UEAwwQdHJzY2F2b0B1aXVjLmVkdTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkC
gYEAv9QMe4lRl3XbWPcflbCjGK9gty6zBJmp+tsaJINM0VaBaZ3t+tSXknelYife
nCc2O3yaX76aq53QMXy+5wKQYe8Rzdw28Nv3a73wfjXJXoUhGkvERcscs9EfIWcC
g2bHOg8uSh+Fbv3lHih4lBJ5MCS2buJfsR7dlr/xsadU2RcCAwEAATANBgkqhkiG
9w0BAQQFAAOCAQEAdyIcMTob7TVkelfJ7+I1j0LO24UlKvbLzd2OPvcFTCv6fVHx
Ejk0QxaZXJhreZ6+rIdiMXrEzlRdJEsNMxtDW8++sVp6avoB5EX1y3ez+CEAIL4g
cjvKZUR4dMryWshWIBHKFFul+r7urUgvWI12KbMeE9KP+kiiiiTskLcKgFzngw1J
selmHhTcTCrcDocn5yO2+d3dog52vSOtVFDBsBuvDixO2hv679JR6Hlqjtk4GExp
E9iVI0wdPE038uQIJJTXlhsMMLvUGVh/c0ReJBn92Vj4dI/yy6PtY/8ncYLYNkjg
oVN0J/ymOktn9lTlFyTiuY4OuJsZRO1+zWLy9g==
          </ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </saml:SubjectConfirmationData>
  </saml:SubjectConfirmation>
</saml:Subject>
<!-- assertion lifetime constrained by principal's X.509 cert -->
<saml:Conditions
  NotBefore="2006-07-17T20:31:41Z"
  NotOnOrAfter="2006-07-18T20:21:41Z">
</saml:Conditions>
<saml:AuthnStatement
  AuthnInstant="2006-07-17T20:31:41Z">
  <saml:AuthnContext>
    <saml:AuthnContextClassRef>
        urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient
    </saml:AuthnContextClassRef>
  </saml:AuthnContext>
</saml:AuthnStatement>
<saml:AttributeStatement>
  <saml:Attribute
    xmlns:xacmlprof="urn:oasis:names:tc:SAML:2.0:profiles:attribute:XACML"
    xmlns:ldapprof="urn:oasis:names:tc:SAML:2.0:profiles:attribute:LDAP"
    xacmlprof:DataType="http://www.w3.org/2001/XMLSchema#string"
    ldapprof:Encoding="LDAP"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
    Name="urn:oid:2.5.4.42" FriendlyName="givenName">
    <saml:AttributeValue xsi:type="xs:string">Tom</saml:AttributeValue>
  </saml:Attribute>
</saml:AttributeStatement>
</saml:Assertion>
```

The following is an AttributeQuery issued by an entity on behalf of the subject in the case of the *SAML Attribute Query Deployment Profile for X.509 Subjects*.

```
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  ID="aaf23196-1773-2113-474a-fe114412ab72"
  Version="2.0"
  IssueInstant="2006-07-17T22:26:40Z">
  <saml:Issuer>https://sp.example.org/saml</saml:Issuer>
  <saml:Subject>
    <saml:NameID
      Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
      C=US, O=NCSA-TEST, OU=User, CN=trscavo@uiuc.edu
    </saml:NameID>
  </saml:Subject>
  <saml:Attribute
    xmlns:xacmlprof="urn:oasis:names:tc:SAML:2.0:profiles:attribute:XACML"
```

```
    xmlns:ldapprof="urn:oasis:names:tc:SAML:2.0:profiles:attribute:LDAP"
    xacmlprof:DataType="http://www.w3.org/2001/XMLSchema#string"
    ldapprof:Encoding="LDAP"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
    Name="urn:oid:2.5.4.42" FriendlyName="givenName">
  </saml:Attribute>
</samlp:AttributeQuery>
```

Following the previous request, a responder will return the following Response.

```
<samlp:Response
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  InResponseTo="aaf23196-1773-2113-474a-fe114412ab72"
  ID="b07b804c-7c29-ea16-7300-4f3d6f7928ac"
  Version="2.0"
  IssueInstant="2006-07-17T22:26:41Z">
  <saml:Issuer>https://idp.example.org/saml</saml:Issuer>
  <samlp:Status>
    <samlp:StatusCode
      Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
  </samlp:Status>
  <saml:Assertion
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    ID="a144e8f3-adad-594a-9649-924517abe933"
    Version="2.0"
    IssueInstant="2006-07-17T22:26:41Z">
    <saml:Issuer>https://idp.example.org/saml</saml:Issuer>
    <saml:Subject>
      <saml:NameID
        Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
        C=US, O=NCSA-TEST, OU=User, CN=trscavo@uiuc.edu
      </saml:NameID>
    </saml:Subject>
    <!-- assertion lifetime constrained by principal's X.509 cert -->
    <saml:Conditions
      NotBefore="2006-07-17T22:21:41Z"
      NotOnOrAfter="2006-07-17T22:51:41Z">
      <saml:AudienceRestriction>
        <saml:Audience>https://sp.example.org/saml</saml:Audience>
      </saml:AudienceRestriction>
    </saml:Conditions>
    <saml:AttributeStatement>
      <saml:Attribute
        xmlns:xacmlprof="urn:oasis:names:tc:SAML:2.0:profiles:attribute:XACML"
        xmlns:ldapprof="urn:oasis:names:tc:SAML:2.0:profiles:attribute:LDAP"
        xacmlprof:DataType="http://www.w3.org/2001/XMLSchema#string"
        ldapprof:Encoding="LDAP"
        NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
        Name="urn:oid:2.5.4.42" FriendlyName="givenName">
        <saml:AttributeValue xsi:type="xs:string">Tom</saml:AttributeValue>
      </saml:Attribute>
    </saml:AttributeStatement>
  </saml:Assertion>
</samlp:Response>
```

All the previous examples illustrate attributes that conform to the XACML Attribute Profile [SAMLProf] as required by this Attribute Exchange Profile. Note the attributes also satisfy the X.500/LDAP Attribute Profile, which is not required but may prove to be useful in some deployment scenarios.