Comments: Use of SAML to Retrieve Authorization Credentials

The specification [OGFSAML] profiles the following two use cases:

Case 1. The requester is the subject
Case 2. The requester is acting on behalf of the subject

In case 1, the following issues have been identified:

Issue 1a. Unable to bind the SAML token to a proxy certificate
Issue 1b. X.509 authentication is assumed
Issue 1c. Holder-of-key subject confirmation is not well defined

Likewise in case 2, the following issues have been identified:

Issue 2a. Unable to prove the presence of the subject
Issue 2b. The requester is an entity acting on behalf of the subject

We consider each of these issues below.

Issue 1a. Unable to bind the SAML token to a proxy certificate

The first SAML assertion listed in Appendix B has the following <saml:SubjectConfirmation> element:

```
<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>
```

This SAML assertion can not be bound to an X.509 proxy certificate since the subject of the assertion can not be confirmed. The value of the <ds:X509Certificate> element above is the user's X.509 end-entity certificate (EEC) but since the user authenticates with a proxy certificate, the user proves possession of the wrong private key. Thus the subject is not confirmed and the relying party SHOULD discard the enclosing assertion.

So that the assertion may be bound to an X.509 proxy certificate, the identity provider should bind the DN of the EEC to the <saml:SubjectConfirmation> element:

```
<saml:SubjectConfirmation
  Method="urn:oasis:names:tc:SAML:2.0:cm:holder-of-key">
  <saml:SubjectConfirmationData>
    <ds:KeyInfo>
      <ds:X509Data>
        <ds:X509SubjectName>
          CN=trscavo@uiuc.edu,OU=User,O=NCSA-TEST,C=US
        </ds:X509SubjectName>
      </ds:X509Data>
    </ds:KeyInfo>
  </saml:SubjectConfirmationData>
</saml:SubjectConfirmation>
```

Now, since the subject of the EEC is the same as the subject of the proxy certificate, authentication with the proxy certificate simultaneously confirms the SAML subject.

This suggests the following attribute query (which does not agree with the published specification):

```
<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">
    CN=trscavo@uiuc.edu,OU=User,O=NCSA-TEST,C=US
  </saml:Issuer>
  <saml:Subject>
    <saml:SubjectConfirmation
      Method="urn:oasis:names:tc:SAML:2.0:cm:holder-of-key">
      <saml:SubjectConfirmationData>
        <ds:KeyInfo>
          <ds:X509Data>
            <ds:X509SubjectName>
              CN=trscavo@uiuc.edu,OU=User,O=NCSA-TEST,C=US
            </ds:X509SubjectName>
          </ds:X509Data>
        </ds:KeyInfo>
      </saml:SubjectConfirmationData>
    </saml:SubjectConfirmation>
  </saml:Subject>
</samlp:AttributeQuery>
```

Note that the above query has a <saml:SubjectConfirmation> element but no <saml:NameID> element (which is the exact opposite of that specified in [SAMLX509Subject]).

Issue 1b. X.509 authentication is assumed

The profile [SAMLX509SelfQry] assumes that the user authenticates to the SAML Attribute Authority (AA) with an X.509 credential, which is too restrictive. The user should be able to authenticate with any type of credential, even a username/password, as long as the requirement for a holder-of-key assertion is satisfied.

To permit flexibility in the authentication token used to authenticate to the AA, the specification needs to separate the authentication step from the proof of possession. The following requirements achieve the required separation:

* The user MUST authenticate to the AA, but the means by which this authentication takes place are unspecified
* The user MUST present an X.509 certificate to the AA
* The user MUST prove possession of the private key corresponding to the public key bound to the certificate

If the user authenticates with a trusted X.509 certificate, all of these requirements are satisfied, but the above reformulation of the requirements permits other scenarios as well. For example, suppose that the user authenticates to the AA with a username/ password using HTTP basic auth or WS-Security Username Token Profile. Suppose further that the request is issued over SSL/TLS using an untrusted client certificate. This proves possession of the corresponding private key, but since the client certificate is untrusted, it does not authenticate the user. However, the client certificate still can (and should) be bound to the assertion by the AA.

Issue 1c. Holder-of-key subject confirmation is not well defined

The issuing and processing of holder-of-key SAML assertions is not well defined in [SAMLX509]. Moreover, such requirements are not specified in SAML Core, so there is nothing to rely on. (The OASIS SSTC is considering this issue [SAMLHoK] at this time.)

Issue 2a. Unable to prove the presence of the subject

Since the profile [SAMLX509] specifies that the name identifier in the query is a DN, there is no way to prove user presence at the Grid SP. Without proof of user presence, an SP could phish for attributes using the globally unique, persistent DN.

Note that this issue does not exist for the self-query (of which traditional VOMS is an example), rather the problem involves a query where the requester is acting on behalf of the subject. In that case, the subject must pass some piece of information to the Grid SP that the SP can forward to the AA.

I'm convinced we've specified the name identifier in the query (DN) incorrectly. The requester has to prove user presence and it seems clear that more than a DN is needed. Since the user is authenticating to the Grid SP with an X.509 certificate, the obvious conclusion is that 1) there is some piece of info in the certificate that proves user presence, and 2) the SP passes the complete cert (not just the DN) to the AA.

I'll propose the following "patch" to our profile:

Instead of requiring a DN, the name identifier in the query should be generalized to accommodate the entire certificate (without excluding the possibility of a naked DN in those situations where it is warranted). This can be done using <ds:KeyInfo>,

something like this:

```
<saml:Subject>
 <saml:BaseID xsi:type="KeyIdentifierType">
  <ds:KeyInfo>...</ds:KeyInfo>
 </saml:BaseID>
</saml:Subject>
```

where KeyIdentifierType is defined as follows:

```
<complexType name="KeyIdentifierType">
 <complexContent>
 <extension base="saml:BaseIDAbstractType">
   <sequence>
     <element ref="ds:KeyInfo"/>
   </sequence>
 </extension>
 </complexContent>
</complexType>
```

This new name identifier type accommodates either a DN or a certificate. In addition to proving user presence at the Grid SP, using a certificate in this way has the extra added benefit that it avoids potential DN string matching at the AA, which in and of itself is almost sufficient reason to pass a certificate instead of a DN.

Issue 2b. The requester is an entity acting on behalf of the subject

In Fig 2 of [OGFSAML], it is assumed that the requester is the SAML subject (i.e., the end user). What if the requester is not the subject, but rather an entity acting on behalf of the subject? How does the Grid SP know if the requester is the subject or an entity acting on behalf of the subject?

Consider the following use case. In TeraGrid, a science gateway is issued a community credential. Individual users authenticate to the gateway with an ordinary username/ password, after which the gateway turns around and requests grid resources on the user's behalf, authenticating to the resource provider with the community credential (or rather a proxy signed by the community credential). In this case, the subject DN in the request is that of the gateway, not the end user.

In TeraGrid, a science gateway identifies the end user to the resource provider by embedding a SAML assertion in the community proxy, but in general, the question remains: How does the Grid SP know if the requester is the subject or an entity acting on behalf of the subject?

References

[OGFSAML] V. Venturi, T. Scavo, D. Chadwick. Use of SAML to retrieve Authorization Credentials. See http://www.ogf.org/Public_Comment_Docs/Documents/2008-07/ Attributes_Exchange_Profilev1.4.pdf

[SAMLX509] T. Scavo. SAML V2.0 Deployment Profiles for X.509 Subjects. OASIS Committee Specification, 27 March 2008. Document ID sstc-saml2-x509-profiles-deploy-cs-01. See http://wiki.oasis-open.org/security/SstcSaml2X509ProfilesDeploy

[SAMLX509Subject] X.509 SAML Subject Profile. See section 2 of [SAMLX509]

[SAMLX509Query] SAML Attribute Query Deployment Profile for X.509 Subjects. See section 3 of [SAMLX509]

[SAMLX509SelfQry] SAML Attribute Self-Query Deployment Profile for X.509 Subjects. See section 4 of [SAMLX509]

[SAMLHoK] SAML V2.0 Holder-of-Key Assertion Profile. See http://wiki.oasis-open.org/security/SAMLHoKSubjectConfirmation