GridShibBetaAttributePull

GridShib Beta Attribute Exchange Profile

Preconditions

- The Grid User and the Grid Service Provider (Grid SP) each possess an X.509 credential.
- The Grid Client application has access to the Grid User's X.509 credential.
- The Grid User has an account with a Shibboleth Identity Provider (!IdP).
- The !IdP is able to map the Grid User's X.509 Subject DN to one and only one user in its security domain.
- The Grid SP and the !IdP each have been assigned a unique identifier called a *providerId*.
- The Grid SP and the !IdP rely on the same metadata format and exchange this metadata out-of-band.
- The Grid SP and the !IdP are collocated in the same security domain.

Protocol Flow

Overview

This GridShib profile consists of four (4) steps:

1. The Grid Client requests a service at the Grid SP.
2. The Grid SP authenticates the Client and queries the Attribute Authority (AA) at the !IdP.
3. The AA returns an attribute assertion to the Grid SP.
4. The Grid SP parses the attribute assertion, performs the requested service, and returns a response to the Grid Client.

Description

Step 1 is the beginning of a normal grid request/response cycle. At step 1, the Grid Client presents an ordinary X.509 proxy certificate to the Grid SP. (See the Issues section, however.)

The Grid SP authenticates the Client and queries the AA at the !IdP at step 2. **The `Subject` of the query is the DN from the proxy.** For example, the Grid SP might POST a SAML SOAP request similar to the following:

```
POST /shibboleth/AA HTTP/1.1
Host: gridshib.uchicago.edu
Content-Type: text/xml
Content-Length: nnn
SOAPAction: http://www.oasis-open.org/committees/security

<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope
  xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Header/>
  <SOAP-ENV:Body>
         <samlp:Request
                xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
                xmlns:samlp="urn:oasis:names:tc:SAML:1.0:protocol"
                MajorVersion="1" MinorVersion="1"
                IssueInstant="2004-12-05T09:22:04Z"
                RequestID="aaf23196-1773-2113-474a-fe114412ab72">
                <samlp:AttributeQuery
                  Resource="https://globus.org/gridshib">  <!-- Grid SP providerId -->
                  <saml:Subject>
                         <saml:NameIdentifier
                                Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName"
                                NameQualifier="https://idp.uchicago.edu/shibboleth">  <!-- IdP providerId -->
                                <!-- insert X.509 Subject DN here -->
                         </saml:NameIdentifier>
                  </saml:Subject>
                  <!-- the requested attributes are for illustration only -->
                  <saml:AttributeDesignator
                         AttributeName="urn:mace:dir:attribute-def:eduPersonAffiliation"
                         AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri"/>
                  <saml:AttributeDesignator
                         AttributeName="urn:mace:dir:attribute-def:eduPersonPrincipalName"
                         AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri"/>
                </samlp:AttributeQuery>
         </samlp:Request>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

At step 3, the AA authenticates the requester, maps the DN to a local principal name, formulates an attribute assertion, and returns the assertion to the Grid SP:

```
HTTP/1.1 200 OK
Content-Type: text/xml
Content-Length: nnnn

<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope
  xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Header/>
  <SOAP-ENV:Body>
         <samlp:Response
                xmlns:samlp="urn:oasis:names:tc:SAML:1.0:protocol"
                InResponseTo="aaf23196-1773-2113-474a-fe114412ab72"
                IssueInstant="2004-12-05T09:22:05Z"
                MajorVersion="1" MinorVersion="1"
                ResponseID="b07b804c-7c29-ea16-7300-4f3d6f7928ac">
                <samlp:Status>
                  <samlp:StatusCode Value="samlp:Success"/>
                </samlp:Status>
                <saml:Assertion
                  xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
                  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                  MajorVersion="1" MinorVersion="1"
                  AssertionID="a144e8f3-adad-594a-9649-924517abe933"
                  IssueInstant="2004-12-05T09:22:05Z"
                  Issuer="https://idp.uchicago.edu/shibboleth">  <!-- IdP providerId -->
                  <saml:Conditions
                         NotBefore="2004-12-05T09:17:05Z"
                         NotOnOrAfter="2004-12-05T09:52:05Z">
                         <saml:AudienceRestrictionCondition>
                                <!-- Grid Service providerId -->
                                <saml:Audience>https://globus.org/gridshib</saml:Audience>
                         </saml:AudienceRestrictionCondition>
                  </saml:Conditions>
                  <saml:AttributeStatement>
                         <saml:Subject>
                                <saml:NameIdentifier
                                  Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName"
                                  NameQualifier="https://idp.uchicago.edu/shibboleth">  <!-- IdP providerId -->
                                  <!-- insert X.509 Subject DN here -->
                                </saml:NameIdentifier>
                         </saml:Subject>
                         <saml:Attribute
                                AttributeName="urn:mace:dir:attribute-def:eduPersonAffiliation"
                                AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri">
                                <saml:AttributeValue>
                                  member
                                </saml:AttributeValue>
                         </saml:Attribute>
                         <saml:Attribute
                                AttributeName="urn:mace:dir:attribute-def:eduPersonPrincipalName"
                                AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri">
                                <saml:AttributeValue Scope="uchicago.edu">
                                  gridshib
                                </saml:AttributeValue>
                         </saml:Attribute>
                  </saml:AttributeStatement>
                </saml:Assertion>
         </samlp:Response>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Finally, at step 4, the Grid SP parses the attribute assertion, caches the attributes, makes an access control decision, and returns a response to the Grid Client.

Both the !IdP and the Grid SP rely on SAML 2.0 metadata. GridShib for Shibboleth supports a framework for consuming Grid SP metadata whereby the metadata file includes an `EntityDescriptor` element for each Grid SP that the !IdP trusts. SAML 2.0 does not define a role for Grid SPs, however, so an extended role of type **AttributeRequesterDescriptorType** has been specified for use with this profile. The defined role of each such entity is basically that of a standalone attribute requester.

Illustrative metadata examples from Globus CVS:

- gridshib-sp-metadata.xml
- gridshib-sp-metadata-template.xml
- gridshib-idp-metadata-template.xml

Requirements

The following requirements must be satisfied:

Attribute Query

- The value of the `AttributeQuery/@Resource` attribute is the providerId of the Grid SP.
- The value of the `NameIdentifier/@Format` attribute is the standard SAML URI "urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName".
- The value of the `NameIdentifier/@NameQualifier` attribute is the providerId of the Grid User's !IdP.
- The value of the `Subject` element is the X.509 Subject DN (suitably encoded) from the proxy certificate presented by the Grid Client at step 1.
- The query SHOULD NOT have a `Subject/SubjectConfirmation` element.

Attribute Response

- The Grid SP SHOULD ignore any non-attribute statements in the response.
- The Subject of each attribute statement in the response SHOULD **strongly match** the Subject of the query. Any attribute statement with a Subject that does not **strongly match** the Subject of the query should be discarded.
- If there are one or more `AudienceRestrictionCondition/Audience` elements in the response, the Grid SP SHOULD verify that it is a member of at least one audience. [Is this a SAML requirement?]
- In processing the attribute response, the Grid SP collapses the value of the `AttributeValue/@Scope` attribute into the value of `Attribute/AttributeValue` by appending "@" followed by the `Scope` value to the `AttributeValue` .

!IdP Metadata

- The value of the `EntityDescriptor/@entityID` attribute is the providerId of the !IdP.
- The value of the `AttributeService/@Binding` attribute is "urn:oasis:names:tc:SAML:1.0:bindings:SOAP-binding".
- The value of the `AttributeService/@Location` attribute is used at step 2 of the profile.
- There must be one `NameIDFormat` element whose value is "urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName". Other identifiers may be supported by the !IdP, that is, other `NameIDFormat` elements may be called out in metadata.

Grid SP Metadata

- The value of the `EntityDescriptor/@entityID` attribute is the providerId of the Grid SP.
- The value of the `EntityDescriptor/RoleDescriptor/NameIDFormat` element is "urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName". No other `NameIDFormat` elements are allowed.

Security and Privacy Considerations

TBD

Issues

- To satisfy the precondition that the !IdP be able to map the DN to one and only one local principal name, the current implementation relies on a name mapping file at the !IdP. This creates a maintenance problem, so this and other name mapping issues need to be considered.
- To relax the precondition that the !IdP and the Grid SP be collocated in the same security domain, we must solve the IdP Discovery problem.
- The production, distribution, and consumption of SAML 2.0 metadata is an ongoing issue.