ExtendingClassicGridShib

Extending Classic GridShib

The classic GridShib Attribute Pull Profile (called *Classic !GridShib*) is an initial attempt to provide interoperability between Globus Toolkit and Shibboleth. The next round of implementations will refine Classic !GridShib, decompose the profile (for reusability), and address attribute push in addition to attribute pull.

Why are we extending Classic !GridShib?

1. To serve as a model for future revisions of the OASIS SAML V2.0 Attribute Sharing Profile (an important work-in-progress)
2. To provide a specification to drive this round of GridShib implementations (which addresses the needs of caBIG, among others)
3. To facilitate the GGF ShibGrid Birds-of-a-Feather interoperability testbed (to be discussed at GGF18)
4. To provide reusable building blocks for subsequent profiles (including an emerging X.509 Binding Profile for SAML Assertions)

How are we extending Classic !GridShib?

Specific work items include the following:

- [GridShib for GT] Modify the Shibboleth Attribute Requester PIP to send the Issuer DN in the `NameQualifier` attribute.
- [GridShib for Shib] Modify the `GridShibNameMapper` plugin to process the Issuer DN in the `NameQualifier` attribute.
- [GridShib for Shib] Refactor the GridShib `NameMap` interface (and everything that depends on it) to map an ordered pair of the form `(subjectDN, issuerDN)` to a local principal name.
- [GridShib for Shib] Implement a modified query protocol handler (similar to !LionShare) that handles the case where the requester is the subject of the query (i.e., self-queries). If the DN of the query matches the DN of the requester (from TLS client authn) and the !IdP trusts the issuer of the client cert, then the AA bypasses the ARPs and returns all attributes pertaining to the subject. (See below for a sample assertion.)
- [GridShib Client] Extend the SAML Assertion Client to query a Shib AA (similar to !LionShare) and embed the resulting assertion in a non-critical X.509 extension. In the query, the name identifier format is `X509SubjectName` and the value of the `NameIdentifier` is the Subject DN of the client certificate. The `NameQualifier` attribute is the Issuer DN of the client certificate.
- [GridShib for GT] Extend the SAML Assertion Consumer PIP to consume the assertion in the extension as follows: If the assertion contains an `AttributeStatement` , the attributes are parsed and the Shibboleth Attribute Requester PIP is bypassed. If, on the other hand, there is only an `AuthenticationStatement` in the assertion, the Shibboleth Attribute Requester PIP is invoked. Note: The assertion MUST contain an `AuthenticationStatement` and it MAY contain an `AttributeStatement` .
- [GridShib for GT] Modify the SAML Assertion Consumer PIP to validate the signature on an assertion (if one exists).
- [GridShib for GT] Modify the SAML Assertion Consumer PIP to perform holder-of-key subject confirmation (if necessary). Note: An assertion with holder-of-key subject confirmation MUST be signed.
- [GridShib for Shib] Define a new role at the !IdP that calls out support for this profile.
- [GridShib for GT] Extend the metadata handler to check for profile support at the !IdP.

Future extensions to Classic !GridShib:

- [GridShib Client] Extend the SAML Assertion Client to issue a SOAP request with a SAML assertion in the SOAP header (according to the WSS SAML Token Profile).
- [GridShib for GT] Extend the SAML Assertion Consumer PIP to handle assertions in SOAP request headers (according to the WSS SAML Token Profile).

Example:

```
<Assertion
  xmlns="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";
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#";
  AssertionID="_33776a319493ad607b7ab3e689482e45"
  IssueInstant="2006-05-11T16:21:24.575Z"
  Issuer="https://idp.example.org/shibboleth";
  MajorVersion="1" MinorVersion="1">
  <!-- NotBefore and NotOnOrAfter mirror the lifetime of the authn credential -->
  <Conditions
         NotBefore="2006-05-11T16:21:24.575Z"
         NotOnOrAfter="2006-05-12T00:21:24.575Z"/>
  <AuthenticationStatement
         AuthenticationInstant="2006-05-11T16:21:24.575Z"
         AuthenticationMethod="urn:ietf:rfc:2246">
         <Subject>
                <NameIdentifier
                  Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName"
                  NameQualifier="C=US, O=NCSA-TEST, OU=GridShib, CN=GridShib-CA">
                  C=US, O=NCSA-TEST, OU=User, CN=trscavo@xxxxxxxx
                </NameIdentifier>
                <SubjectConfirmation>
                  <ConfirmationMethod>
```

```
                        urn:oasis:names:tc:SAML:1.0:cm:holder-of-key
                  </ConfirmationMethod>
                  <SubjectConfirmationData>
                        <ds:KeyInfo>
                              <ds:X509Data>
                                <ds:X509Certificate>...</ds:X509Certificate>
                              </ds:X509Data>
                        </ds:KeyInfo>
                  </SubjectConfirmationData>
                </SubjectConfirmation>
          </Subject>
    </AuthenticationStatement>
    <AttributeStatement>
          <Subject>
                <NameIdentifier
                  Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName"
                  NameQualifier="C=US, O=NCSA-TEST, OU=GridShib, CN=GridShib-CA">
                  C=US, O=NCSA-TEST, OU=User, CN=trscavo@uiuc.edu
                </NameIdentifier>
                <SubjectConfirmation>
                  <ConfirmationMethod>
                        urn:oasis:names:tc:SAML:1.0:cm:holder-of-key
                  </ConfirmationMethod>
                  <SubjectConfirmationData>
                        <ds:KeyInfo>
                              <ds:X509Data>
                                <ds:X509Certificate>...</ds:X509Certificate>
                              </ds:X509Data>
                        </ds:KeyInfo>
                  </SubjectConfirmationData>
                </SubjectConfirmation>
          </Subject>
          <Attribute
                AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri"
                AttributeName="urn:mace:dir:attribute-def:eduPersonPrincipalName">
                <AttributeValue Scope="uiuc.edu">trscavo</AttributeValue>
          </Attribute>
          <Attribute
                AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri"
                AttributeName="urn:mace:dir:attribute-def:givenName">
                <AttributeValue xsi:type="xsd:string">Tom</AttributeValue>
          </Attribute>
          <Attribute
                AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri"
                AttributeName="urn:mace:dir:attribute-def:sn">
                <AttributeValue xsi:type="xsd:string">Scavo</AttributeValue>
          </Attribute>
          <Attribute
                AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri"
                AttributeName="urn:mace:dir:attribute-def:mail">
                <AttributeValue xsi:type="xsd:string">trscavo@xxxxxxxxx</AttributeValue>
          </Attribute>
    </AttributeStatement>
    <ds:Signature>...</ds:Signature>
</Assertion>
```