NanoHUBTestbed

nanoHUB Testbed

A nanoHUB testbed is being developed to explore various deployment scenarios based on GridShib technology. Specifically, GridShib for Globus Toolkit and the GridShib SAML Tools have been deployed by nanoHUB (see NanoHUBDeploymentNotes for deployment details).

The GridShib SAML Tools, which are new, include:

- *SAML Assertion Issuer Tool*
- *SAML Attribute Query Client*
- *SAML X.509 Binding Tool*
- *Globus SAML Library*

Note that the SAML Assertion Issuer Tool and the SAML Attribute Query Client replace previously released software components called the GridShib Authentication Assertion Client and Shibboleth IdP Tester, respectively.

The current version of the GridShib SAML Tools (v0.1) supports attribute pull and a limited form of attribute push. The next version of the GridShib SAML Tools (v0.2), working in conjunction with a forthcoming version of GridShib for Globus Toolkit, will support unlimited attribute push. The GridShib SAML Tools v0.2 will leverage the full power of the Shibboleth Attribute Resolver.

Attribute Pull

This deployment scenario is realized with current nanoHUB infrastructure, GridShib SAML Tools v0.1 and GridShib for Globus Toolkit v0.5.

1. An unauthenticated browser user requests a Grid Resource via the nanoHUB portal.
2. The nanoHUB portal authenticates the user (via LDAP), which initiates the following subsequence of events:
    a. The portal writes a dynamic config file (including one or more attributes) to disk.
    b. The portal passes the principal name and the authentication context (authentication method, authentication instant, and IP address) to the SAML Assertion Issuer Tool, which reads the config file created at the previous step.
    c. Using the nanoHUB community credential, the SAML Assertion Issuer Tool issues a SAML assertion and binds this assertion to a proxy certificate, which is written to disk.
    d. The portal invokes the Grid Client.
3. Using the proxy certificate issued by the SAML Assertion Issuer Tool at step 2c above, the Grid Client authenticates to the Grid SP.
4. The Grid SP parses the SAML assertion in the proxy certificate and issues an attribute query to the Attribute Authority (AA) at the nanoHUB IdP.
5. The AA issues an attribute assertion and returns a response to the Grid SP.
6. The Grid SP parses the attribute assertion in the response, makes an access control decision, and returns a response to the Grid Client.
7. The Grid Client returns a response to the portal.
8. The portal returns a response to the browser client.

With the exception of the dynamic config file at step 2a and the authentication context at step 2b, all of this infrastructure is deployed today.

Example

Here is an example of a SAML assertion bound to an X.509 proxy certificate in the case of attribute pull:

```
<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"
  AssertionID="_26de37af523834ef42c110ec23097ebc"
  IssueInstant="2007-01-24T01:31:09.327Z"
  Issuer="O=Grid, OU=GlobusTest, OU=simpleCA-gatekeeper.rcac.purdue.edu, OU=rcac.purdue.edu, CN=VMware"
  MajorVersion="1" MinorVersion="1">
  <saml:AuthenticationStatement
    AuthenticationInstant="2007-01-24T01:31:08.837Z"
    AuthenticationMethod="urn:oasis:names:tc:SAML:1.0:am:password">
    <saml:Subject>
      <saml:NameIdentifier
        Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"
        NameQualifier="urn:mace:inqueue:shadow120.punch.purdue.edu">
        wlee
      </saml:NameIdentifier>
    </saml:Subject>
    <saml:SubjectLocality IPAddress="192.168.1.102"/>
  </saml:AuthenticationStatement>
  <saml:AttributeStatement>
    <saml:Subject>
      <saml:NameIdentifier
        Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"
        NameQualifier="urn:mace:inqueue:shadow120.punch.purdue.edu">
        wlee
      </saml:NameIdentifier>
    </saml:Subject>
    <!-- FriendlyName="countryName" -->
    <saml:Attribute
      AttributeName="https://gridshib.globus.org/names/attribute/countryName"
      AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri">
      <saml:AttributeValue xsi:type="xsd:string">US</saml:AttributeValue>
    </saml:Attribute>
    <!-- FriendlyName="isMemberOf" -->
    <saml:Attribute
      AttributeName="urn:oid:1.3.6.1.4.1.5923.1.5.1.1"
      AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri">
      <saml:AttributeValue xsi:type="xsd:string">
        http://www.nanohub.org
      </saml:AttributeValue>
    </saml:Attribute>
  </saml:AttributeStatement>
</saml:Assertion>
```

Here is an example of a SAML assertion received from the nanoHUB Attribute Authority:

```
<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"
  AssertionID="..."
  IssueInstant="2007-01-24T01:31:13.000Z"
  Issuer="urn:mace:inqueue:shadow120.punch.purdue.edu"
  MajorVersion="1" MinorVersion="1">
  <saml:AttributeStatement>
    <saml:Subject>
      <saml:NameIdentifier
        Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"
        NameQualifier="urn:mace:inqueue:shadow120.punch.purdue.edu">
        wlee
      </saml:NameIdentifier>
    </saml:Subject>
    <!-- many nanoHUB attributes, too numerous to mention -->
  </saml:AttributeStatement>
</saml:Assertion>
```

Note that one or more attributes are pushed to the Grid SP despite the fact that GridShib for Globus Toolkit v0.5 can not consume them. This is mainly done as a proof of concept, in preparation for the push deployment scenario below.

Attribute Push

This deployment scenario requires GridShib SAML Tools v0.2 and GridShib for Globus Toolkit v0.6 (both of which are on the GridShib Online Roadmap). In this scenario, the functionality of the nanoHUB AA has been incorporated into the GridShib SAML Tools v0.2.

1. An unauthenticated browser user requests a Grid Resource via the nanoHUB portal.
2. The nanoHUB portal authenticates the user (via LDAP), which initiates the following subsequence of events:
    a. The portal passes the principal name and the authentication context (authentication method, authentication instant, and IP address) to the SAML Assertion Issuer Tool.
    b. The SAML Assertion Issuer Tool resolves attributes from the nanoHUB LDAP.
    c. Using the nanoHUB community credential, the SAML Assertion Issuer Tool issues a SAML assertion and binds this assertion to a proxy certificate, which is written to disk.
    d. The portal invokes the Grid Client.
3. Using the proxy certificate issued by the SAML Assertion Issuer Tool at step 2c above, the Grid Client authenticates to the Grid SP.
4. The Grid SP parses the SAML assertion in the proxy certificate, makes an access control decision, and returns a response to the Grid Client.
5. The Grid Client returns a response to the portal.
6. The portal returns a response to the browser client.

Note that the SAML Assertion Issuer Tool can resolve attributes from multiple attribute stores. In this case, attributes are resolved from nanoHUB LDAP.

Example

Here is an example of a SAML assertion bound to an X.509 proxy certificate in the case of attribute push:

```
<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"
  AssertionID="_26de37af523834ef42c110ec23097ebc"
  IssueInstant="2007-01-24T01:31:09.327Z"
  Issuer="O=Grid, OU=GlobusTest, OU=simpleCA-gatekeeper.rcac.purdue.edu, OU=rcac.purdue.edu, CN=VMware"
  MajorVersion="1" MinorVersion="1">
  <saml:AuthenticationStatement
    AuthenticationInstant="2007-01-24T01:31:08.837Z"
    AuthenticationMethod="urn:oasis:names:tc:SAML:1.0:am:password">
    <saml:Subject>
      <saml:NameIdentifier
        Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">
        wlee
      </saml:NameIdentifier>
    </saml:Subject>
    <saml:SubjectLocality IPAddress="192.168.1.102"/>
  </saml:AuthenticationStatement>
  <saml:AttributeStatement>
    <saml:Subject>
      <saml:NameIdentifier
        Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">
        wlee
      </saml:NameIdentifier>
    </saml:Subject>
    <!-- FriendlyName="countryName" -->
    <saml:Attribute
      AttributeName="https://gridshib.globus.org/names/attribute/countryName"
      AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri">
      <saml:AttributeValue xsi:type="xsd:string">US</saml:AttributeValue>
    </saml:Attribute>
    <!-- FriendlyName="isMemberOf" -->
    <saml:Attribute
      AttributeName="urn:oid:1.3.6.1.4.1.5923.1.5.1.1"
      AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri">
      <saml:AttributeValue xsi:type="xsd:string">
        http://www.nanohub.org
      </saml:AttributeValue>
    </saml:Attribute>
    <!-- many nanoHUB attributes, too numerous to mention -->
  </saml:AttributeStatement>
</saml:Assertion>
```

Note that the `NameIdentifier` element has no `NameQualifier` attribute in this case since the Grid SP need not query the AA. (In fact, using the `NameQualifier` attribute for IdP Discovery—as in the attribute pull deployment scenario—is flawed. A subsequent version of the SAML X.509 Binding Tool will bind the IdP `entityID` to the Subject Information Access (SIA) extension of the X.509 proxy certificate. If the Grid SP needs to query, it first looks to the SIA extension for the `entityID`. If it doesn't find the `entityID` there, it inspects nested assertions in the `Advice` element. See, for example, the attribute push with cross-domain SSO deployment scenario below)

Attribute Push with Local SSO

This deployment scenario assumes the nanoHUB portal is Shib-protected. The IdP depicted in the diagram is a fully configured nanoHUB IdP.

There is no IdP Discovery issue since the nanoHUB IdP is the only trusted IdP. Thus in the flow diagram above (and the discussion below), the flow begins with an authentication request at the nanoHUB IdP for simplicy of presentation.

1. An unauthenticated browser user issues a SAML authentication request to the nanoHUB IdP.
2. The SSO Service at the IdP authenticates the user (if necessary) and returns an authentication response (including attributes) to the browser.
3. The browser user transmits the authentication response to the nanoHUB portal.
4. The Shib-protected nanoHUB portal consumes the authentication response and initiates the following subsequence of events:
    a. The portal passes the Shib-issued SSO assertion (which includes the authentication context as well as nanoHUB attributes) to the SAML Assertion Issuer Tool.
    b. The SAML Assertion Issuer Tool binds the SSO assertion to a locally-issued SAML assertion (in the `Advice` element).
    c. Using the nanoHUB community credential, the SAML Assertion Issuer Tool binds this nested assertion to a proxy certificate, which is written to disk.
    d. The portal invokes the Grid Client.
5. Using the proxy certificate issued by the SAML Assertion Issuer Tool at step 4c above, the Grid Client authenticates to the Grid SP.
6. The Grid SP parses the SAML assertion in the proxy certificate, makes an access control decision, and returns a response to the Grid Client.
7. The Grid Client returns a response to the portal.
8. The portal returns a response to the browser client.

Example

Here is an example of a SAML assertion bound to an X.509 proxy certificate in the case of attribute push with local SSO:

```
<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"
  AssertionID="_26de37af523834ef42c110ec23097ebc"
  IssueInstant="2007-01-24T01:31:09.327Z"
  Issuer="O=Grid, OU=GlobusTest, OU=simpleCA-gatekeeper.rcac.purdue.edu, OU=rcac.purdue.edu, CN=VMware"
  MajorVersion="1" MinorVersion="1">
  <saml:Advice>
    <!-- assertion obtained from the nanoHUB IdP -->
    <saml:Assertion ...>
      ...
      <saml:AuthenticationStatement>
        <saml:Subject>
          <saml:NameIdentifier
            Format="urn:mace:shibboleth:1.0:nameIdentifier"
            NameQualifier="urn:mace:inqueue:shadow120.punch.purdue.edu">
            3f7b3dcf-1674-4ecd-92c8-1544f346baf8
          </saml:NameIdentifier>
          <saml:SubjectConfirmation>
            <saml:ConfirmationMethod>
              urn:oasis:names:tc:SAML:1.0:cm:bearer
            </saml:ConfirmationMethod>
          </saml:SubjectConfirmation>
        </saml:Subject>
      </saml:AuthenticationStatement>
      <saml:AttributeStatement>
        <saml:Subject>
          <saml:NameIdentifier
            Format="urn:mace:shibboleth:1.0:nameIdentifier"
            NameQualifier="urn:mace:inqueue:shadow120.punch.purdue.edu">
            3f7b3dcf-1674-4ecd-92c8-1544f346baf8
          </saml:NameIdentifier>
        </saml:Subject>
        <saml:Attribute
          AttributeName="urn:mace:dir:attribute-def:eduPersonPrincipalName"
          AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri">
          <saml:AttributeValue Scope="example.org">
            wlee
          </saml:AttributeValue>
        </saml:Attribute>
      </saml:AttributeStatement>
    </saml:Assertion>
  </saml:Advice>
  <saml:AttributeStatement>
    <saml:Subject>
      <saml:NameIdentifier
        Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">
        wlee
      </saml:NameIdentifier>
    </saml:Subject>
    <!-- FriendlyName="countryName" -->
    <saml:Attribute
      AttributeName="https://gridshib.globus.org/names/attribute/countryName"
      AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri">
      <saml:AttributeValue xsi:type="xsd:string">US</saml:AttributeValue>
    </saml:Attribute>
    <!-- FriendlyName="isMemberOf" -->
    <saml:Attribute
      AttributeName="urn:oid:1.3.6.1.4.1.5923.1.5.1.1"
      AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri">
      <saml:AttributeValue xsi:type="xsd:string">
        http://www.nanohub.org
      </saml:AttributeValue>
    </saml:Attribute>
    <!-- many nanoHUB attributes, too numerous to mention -->
  </saml:AttributeStatement>
</saml:Assertion>
```

Attribute Push with Cross-domain SSO

This deployment scenario supports cross-domain SSO. The IdP depicted in the diagram is any IdP trusted by nanoHUB.

In the flow diagram above (and the discussion below), we ignore the problem of IdP Discovery for simplicity of presentation. Thus the flow begins with an authentication request at the IdP.

1. An unauthenticated browser user issues a SAML authentication request to a Shibboleth IdP.
2. The SSO Service at the IdP authenticates the user (if necessary) and returns an authentication response to the browser. We assume the IdP supports attribute push and that the authentication response includes attributes.
3. The browser user transmits the authentication response to the nanoHUB portal.
4. The Shib-protected nanoHUB portal consumes the authentication response and initiates the following subsequence of events:
    a. The portal passes the Shib-issued SSO assertion (which includes the authentication context as well as campus attributes) to the SAML Assertion Issuer Tool.
    b. The SAML Assertion Issuer Tool binds the SSO assertion to a locally-issued SAML assertion (in the `Advice` element).
    c. Using the nanoHUB community credential, the SAML Assertion Issuer Tool binds this nested assertion to a proxy certificate, which is written to disk.
    d. The portal invokes the Grid Client.
5. Using the proxy certificate issued by the SAML Assertion Issuer Tool at step 4c above, the Grid Client authenticates to the Grid SP.
6. The Grid SP parses the SAML assertion in the proxy certificate, makes an access control decision, and returns a response to the Grid Client.
7. The Grid Client returns a response to the portal.
8. The portal returns a response to the browser client.

Note that between steps 5 and 6 the Grid SP may decide to query the AA at the IdP. There is sufficient information in the nested assertion (namely, the IdP `entityID` and SAML Subject) to perform such a query.

Example

Here is an example of a SAML assertion bound to an X.509 proxy certificate in the case of attribute push with cross-domain SSO:

```
<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"
  AssertionID="_26de37af523834ef42c110ec23097ebc"
  IssueInstant="2007-01-24T01:31:09.327Z"
  Issuer="O=Grid, OU=GlobusTest, OU=simpleCA-gatekeeper.rcac.purdue.edu, OU=rcac.purdue.edu, CN=VMware"
  MajorVersion="1" MinorVersion="1">
  <saml:Advice>
    <!-- assertion issued by campus Shib IdP -->
    <saml:Assertion ...>
      ...
      <saml:AuthenticationStatement
        AuthenticationInstant="2007-01-24T01:31:08.837Z"
```

```
        AuthenticationMethod="urn:oasis:names:tc:SAML:1.0:am:password">
        <saml:Subject>
          <saml:NameIdentifier
            Format="urn:mace:shibboleth:1.0:nameIdentifier"
            NameQualifier="https://idp.example.org/shibboleth">
            3f7b3dcf-1674-4ecd-92c8-1544f346baf8
          </saml:NameIdentifier>
          <saml:SubjectConfirmation>
            <saml:ConfirmationMethod>
              urn:oasis:names:tc:SAML:1.0:cm:bearer
            </saml:ConfirmationMethod>
          </saml:SubjectConfirmation>
        </saml:Subject>
        <saml:SubjectLocality IPAddress="192.168.1.102"/>
      </saml:AuthenticationStatement>
      <saml:AttributeStatement>
        <saml:Subject>
          <saml:NameIdentifier
            Format="urn:mace:shibboleth:1.0:nameIdentifier"
            NameQualifier="https://idp.example.org/shibboleth">
            3f7b3dcf-1674-4ecd-92c8-1544f346baf8
          </saml:NameIdentifier>
        </saml:Subject>
        <saml:Attribute
          AttributeName="urn:mace:dir:attribute-def:eduPersonPrincipalName"
          AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri">
          <saml:AttributeValue Scope="example.org">
            wlee
          </saml:AttributeValue>
        </saml:Attribute>
        <saml:Attribute
          AttributeName="urn:mace:dir:attribute-def:eduPersonScopedAffiliation"
          AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri">
          <saml:AttributeValue Scope="example.org">
            member
          </saml:AttributeValue>
          <saml:AttributeValue Scope="example.org">
            faculty
          </saml:AttributeValue>
        </saml:Attribute>
      </saml:AttributeStatement>
    </saml:Assertion>
  </saml:Advice>
  <saml:AttributeStatement>
    <saml:Subject>
      <saml:NameIdentifier
        Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">
        wlee
      </saml:NameIdentifier>
    </saml:Subject>
    <!-- FriendlyName="countryName" -->
    <saml:Attribute
      AttributeName="https://gridshib.globus.org/names/attribute/countryName"
      AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri">
      <saml:AttributeValue xsi:type="xsd:string">US</saml:AttributeValue>
    </saml:Attribute>
    <!-- FriendlyName="isMemberOf" -->
    <saml:Attribute
      AttributeName="urn:oid:1.3.6.1.4.1.5923.1.5.1.1"
      AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri">
      <saml:AttributeValue xsi:type="xsd:string">
        http://www.nanohub.org
      </saml:AttributeValue>
    </saml:Attribute>
    <!-- many nanoHUB attributes, too numerous to mention -->
  </saml:AttributeStatement>
</saml:Assertion>
```

SAML Name Identifier

The SAML Assertion Issuer Tool can be configured to produce any SAML `NameIdentifier` whatsoever. The choice of `NameIdentifier`, however, depends on the requirements of both the portal and the Grid SP.

Attribute Pull

In the case of attribute pull, today's Grid SP uses the SAML `Subject` in the bound assertion to formulate the attribute query (but this is subject to change in a future version of GridShib for GT). Thus the portal's choice of format must reflect the particular `NameIdentifier` format(s) the IdP supports. If there are multiple IdP partners (i.e., cross-domain SSO), each with its own format requirements, the problem is intensified.

Attribute Push

In the case of attribute push, the portal need only satisfy the requirements of the Grid SP, so the SAML Assertion Issuer Tool must be able to produce a `NameIdentifier` on an SP-by-SP basis. GridShib SAML Tools v0.1 supports multiple SPs through dynamically generated config files, while GridShib SAML Tools v0.2 leverages the advanced configuration capabilities of the Shibboleth IdP.

SAML Authentication Context

The term *authentication context* refers to specific details of the authentication act, such as

- the authentication method
- the authentication instant
- the IP address of the authenticated client

If the nanoHUB portal is not Shib-protected, these pieces of information are passed from the portal to the SAML Assertion Issuer Tool so that the latter can include them in the SAML `AuthenticationStatement`. GridShib for Globus Toolkit may take the authentication context into account when making its access control decision.

In the case where the nanoHUB portal is Shib-protected, the authentication context is captured in the assertion issued by the Shibboleth SSO Service. This SSO assertion is nested in the assertion issued by the SAML Assertion Issuer Tool. This nesting of the SSO assertion signifies to the Grid SP that 1) the portal has validated the SSO assertion, and 2) the portal trusts the IdP that issued the SSO assertion. Thus it is up to the Grid SP to trust the provided authentication context and any included attributes.

SAML Attributes

In the case of GridShib SAML Tools v0.1, VO attributes are written (dynamically) into the config file. In v0.2, the Tools leverage an embedded Shibboleth IdP to resolve attributes "just in time." In either case, GridShib for GT v0.6 is able to render an access control decision based on pushed attributes.

Attribute countryName

The `countryName` LDAP attribute, sometimes referred to as the c attribute (RFC4519) has the following SAML V1.1 representation on the wire:

```
<saml:Attribute
  xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
  AttributeName="urn:oid:2.5.4.6"
  AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri">
  <saml:AttributeValue xsi:type="xsd:string">US</saml:AttributeValue>
</saml:Attribute>
```

Note that the attribute name (`"urn:oid:2.5.4.6"`) conforms to the MACE-Dir SAML Attribute Profiles.

The above attribute does not have the required semantics, however, so we define a new attribute with name

```
https://gridshib.globus.org/names/attribute/countryName
```

that is the complement to the following SAML attribute

```
AuthenticationStatement/SubjectLocality/@IPAddress
```

In the GridShib SAML Tools v0.1, a portal script maps the `IPAddress` to a GridShib `countryName`, and both are included in the assertion. In the GridShib SAML Tools v0.2, the Shibboleth Attribute Resolver is used to compute the `countryName` based on the IP address of the authenticated client.

Attribute isMemberOf

The OID of the `isMemberOf` attribute is specified in a document entitled LDAP representations of membership in groups.

On the wire, the `isMemberOf` attribute appears as

```
<saml:Attribute
  xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
  AttributeName="urn:oid:1.3.6.1.4.1.5923.1.5.1.1"
  AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri">
  <saml:AttributeValue
    xsi:type="xsd:string">http://www.nanohub.org</saml:AttributeValue>
</saml:Attribute>
```

In the above example, the value of the `isMemberOf` attribute is the base URI of the nanoHUB web (although any globally unique value will do).

eduCourse Attributes

We can configure Shibboleth to assert eduCourse attributes:

```
<saml:Attribute
  xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
  AttributeName="urn:oid:1.3.6.1.4.1.5923.1.6.1.1"
  AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri">
  <saml:AttributeValue xsi:type="xsd:anyURI">
    urn:mace:purdue.edu:classes:spring2007:cs44100.001
  </saml:AttributeValue>
</saml:Attribute>
```

Exactly where such attributes come from, and how they might be used, is still very much an open question.