VT Assurance Testing

The document describes the results of Virginia Tech's testing related to InCommon Silver Assurance. We use CAS for our SSO environment, so the context for all our testing leveraged CAS for authentication and the RemoteUser login handler in the Shibboleth IDP. Instructions for configuring an environment similar to ours can be found at: https://wiki.jasig.org/display/CASUM/Shibboleth-CAS+Integration. All of this testing occurred with the help of the folks at CILogin using their test SP.

Use Case Testing

While the assurance use cases lay out several work flows, this document will concentrate on how the IDP functions. Ultimately the behavior of *requires* or *p refers* in those use cases is dictated entirely by the SP.

Note: *It's not possible at present for the SP to send multiple authnContext values in the request. A reasonable work around is for the SP to perform multiple round trips to get a preferred assurance and this is how the CILogin SP is configured.*

SP requests assurance using AuthnContext:

```
<?xml version="1.0" encoding="UTF-8"?>
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" AssertionConsumerServiceURL="
https://test.cilogon.org/Shibboleth.sso/SAML2/POST" Destination="https://shib-dev.middleware.vt.edu/idp/profile
/SAML2/Redirect/SSO" ID="_2686f9d7635d048070933e9354706ecb" IssueInstant="2012-02-07T15:24:57Z"
ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Version="2.0">
   <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://cilogon.org/shibboleth</saml:Issuer>
   <samlp:NameIDPolicy AllowCreate="1"/>
   <samlp:RequestedAuthnContext>
      <saml:AuthnContextClassRef xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">http://id.incommon.org
/assurance/silver-test</saml:AuthnContextClassRef>
   </samlp:RequestedAuthnContext>
</samlp:AuthnRequest>
```

User authenticates with silver credential

- SP receives silver assurance
- "Silver" access is reported at the SP.

This is what occurs on the IDP

IDP Sends:

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2p:Response xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol" Destination="https://test.cilogon.org
/Shibboleth.sso/SAML2/POST" ID="_5a5795b02e1da27a579f214e61205d7f" InResponseTo="
_cb9ac1df179f243c95d1b9f03802a3a7" IssueInstant="2012-02-07T15:54:07.632Z" Version="2.0" xmlns:xs="http://www.
w3.org/2001/XMLSchema">
   <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:entity">https://shib-dev.middleware.vt.edu</saml2:Issuer>
   <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:SignedInfo>
         <snip/>
      </ds:SignedInfo>
      <ds:SignatureValue><snip/></ds:SignatureValue>
      <ds:KeyInfo><snip/></ds:KeyInfo>
   </ds:Signature>
   <saml2p:Status>
      <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
   </saml2p:Status>
   <saml2:Assertion xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" ID="_f7eb1d1e14fbf4d2aee22bb85a3d62f3"
IssueInstant="2012-02-07T15:54:07.632Z" Version="2.0">
      <saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">https://shib-dev.middleware.vt.
edu</saml2:Issuer>
      <saml2:Subject>
         <saml2:EncryptedID>
            <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#" Id="
_a25862ac755ba6b0480924fe75722c1a" Type="http://www.w3.org/2001/04/xmlenc#Element">
               <snip/>
            </xenc:EncryptedData>
         </saml2:EncryptedID>
         <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
            <saml2:SubjectConfirmationData Address="128.173.13.118" InResponseTo="
_cb9ac1df179f243c95d1b9f03802a3a7" NotOnOrAfter="2012-02-07T15:59:07.632Z" Recipient="https://test.cilogon.org
/Shibboleth.sso/SAML2/POST"/>
         </saml2:SubjectConfirmation>
      </saml2:Subject>
      <saml2:Conditions NotBefore="2012-02-07T15:54:07.632Z" NotOnOrAfter="2012-02-07T15:59:07.632Z">
         <saml2:AudienceRestriction>
            <saml2:Audience>https://cilogon.org/shibboleth</saml2:Audience>
         </saml2:AudienceRestriction>
      </saml2:Conditions>
      <saml2:AuthnStatement AuthnInstant="2012-02-07T15:54:07.528Z" SessionIndex="
67e19f808736d8291f41189e14cd9fde5358f9103d4ba8ebe368ed84b87af639">
         <saml2:SubjectLocality Address="128.173.13.118"/>
         <saml2:AuthnContext>
            <saml2:AuthnContextClassRef>http://id.incommon.org/assurance/silver-test</saml2:
AuthnContextClassRef>
         </saml2:AuthnContext>
      </saml2:AuthnStatement>
      <saml2:AttributeStatement>
         <snip/>
      </saml2:AttributeStatement>
   </saml2:Assertion>
</saml2p:Response>
```

User authenticates with non-silver credential

- SP receives AuthnFailed
- SP requests unspecified
- IDP responds immediately due to SSO session with unspecified
- "Basic" access is reported at the SP.

This is what occurs on the IDP

IDP Logs:

```
DEBUG [org.jasig.cas.client.validation.Saml11TicketValidationFilter:137] - Successfully authenticated user:
serac
INFO [edu.vt.middleware.shib.cas.AssertionAttributeAuthenticationMethodFilter:110] - Setting authentication
method to urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified.
ERROR [edu.internet2.middleware.shibboleth.idp.authn.AuthenticationEngine:525] - Relying patry required an
authentication method of [http://id.incommon.org/assurance/silver-test] but the login handler performed urn:
oasis:names:tc:SAML:2.0:ac:classes:unspecified
ERROR [edu.internet2.middleware.shibboleth.idp.authn.AuthenticationEngine:555] - Authentication failed with the
error:
edu.internet2.middleware.shibboleth.idp.authn.AuthenticationException: Relying patry required an authentication
method of [http://id.incommon.org/assurance/silver-test] but the login handler performed urn:oasis:names:tc:
SAML:2.0:ac:classes:unspecified
```

IDP Sends:

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2p:Response xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol" Destination="https://test.cilogon.org
/Shibboleth.sso/SAML2/POST" ID="_dc922098c9f4739cf9baf9a682ddbf4c" InResponseTo="
_9587d8903988db70fe44a94f486e4f57" IssueInstant="2012-02-07T22:08:18.272Z" Version="2.0">
   <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:entity">https://shib-dev.middleware.vt.edu</saml2:Issuer>
   <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:SignedInfo>
         <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
         <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
         <ds:Reference URI="#_dc922098c9f4739cf9baf9a682ddbf4c">
            <ds:Transforms>
               <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
               <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <ds:DigestValue>zf8lGRuepz4jJmEFDIkEPYfO6Rs=</ds:DigestValue>
         </ds:Reference>
      </ds:SignedInfo>
      <ds:SignatureValue><snip/></ds:SignatureValue>
      <ds:KeyInfo><snip/></ds:KeyInfo>
   </ds:Signature>
   <saml2p:Status>
      <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Responder">
         <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:AuthnFailed"/>
      </saml2p:StatusCode>
   </saml2p:Status>
</saml2p:Response>
```

User cannot authenticate

It's worth mentioning that an IDP may deliver the user to an authentication web form that the user cannot supply credentials for. In this case the IDP should provide link(s) to additional authentication work flows in case the SP allows access for lower assurance credentials.

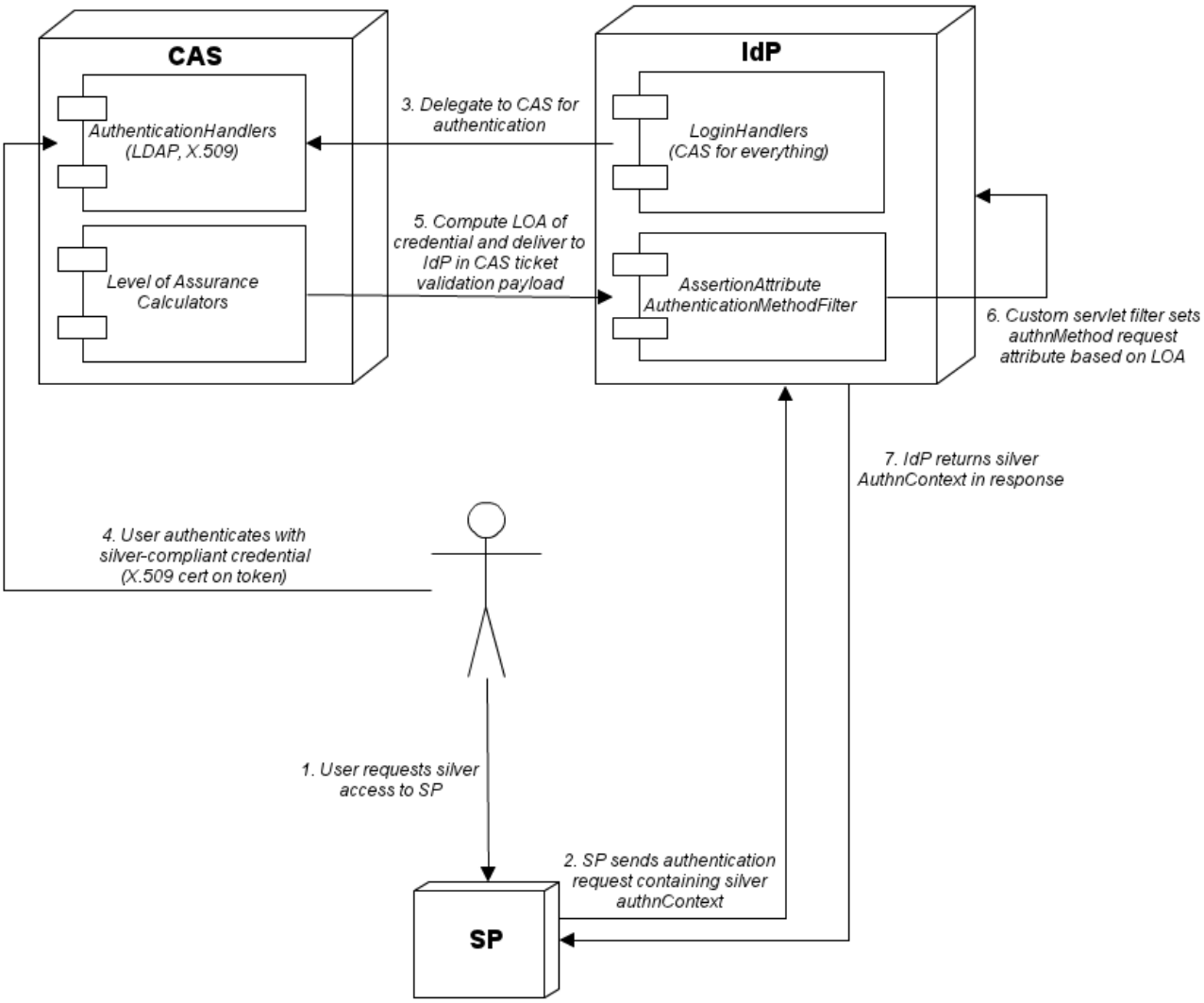
Lessons Learned

The authnMethod request attribute **must** be set on the Shibboleth IDP for **all** requests. Failure to do so will result in incorrect assertions apparently due to advertising silver in the response authnContext.

Configuration

We present some important configuration considerations relating to the above testing. It's important to note that leveraging our existing CAS SSO infrastructure is a vital aspect of our approach to assurance, and many of the following considerations are specific to our architecture. We hope that by sharing some important specific configuration matters, some general concerns may be distilled for other IDM architectures.

IDM Architecture for Assurance



IdP Configuration

CAS is the authentication provider for our IdP, so all authentication methods map to a single login handler. We use the IdP's delegated authentication handler, i.e. RemoteUser, to integrate with CAS.

IdP Login Handler Configuration (handler.xml)

```
<!-- Remote User handler for CAS support -->
<LoginHandler xsi:type="RemoteUser">
  <AuthenticationMethod>
    urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified
  </AuthenticationMethod>
  <AuthenticationMethod>
    urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
  </AuthenticationMethod>
  <AuthenticationMethod>
    http://id.incommon.org/assurance/bronze-test
  </AuthenticationMethod>
  <AuthenticationMethod>
    http://id.incommon.org/assurance/silver-test
  </AuthenticationMethod>
</LoginHandler>
```

The order of advertised authentication methods within the handler is apparently irrelevant, yet we list them in order of increasing strength.

The key component of CAS-IdP integration from the perspective of InCommon Assurance is a custom servlet filter that maps a SAML AuthenticationMethod attribute sent by CAS into an AuthnContext to be asserted by the IdP. The source for this component, `AssertionAttributeAuthenticationMethodFilter`, is available for review.

Servlet Configuration for AssertionAttributeAuthenticationMethodFilter (web.xml)

```
<filter>
  <filter-name>AssertionAttributeAuthenticationMethodFilter</filter-name>
  <filter-class>
    edu.vt.middleware.shib.cas.AssertionAttributeAuthenticationMethodFilter
  </filter-class>
  <init-param>
    <param-name>authMethodAttribute</param-name>
    <param-value>samlAuthenticationStatement::authMethod</param-value>
  </init-param>
</filter>
<filter-mapping>
  <filter-name>AssertionAttributeAuthenticationMethodFilter</filter-name>
  <url-pattern>/Authn/RemoteUser</url-pattern>
</filter-mapping>
```

The key integration configuration item between CAS and Shib is the value of the `authMethodAttribute` parameter. The particular value we have chosen, `samlAuthenticationStatement::authMethod`, corresponds to the value that the CAS components use for the SAML 1.1 AuthenticationMethod attribute. It's important to note that corresponding configuration is required in CAS to set the AuthenticationMethod appropriately so it can be consumed by the IdP.

CAS Configuration

We had already invested a significant amount of engineering effort on supporting multiple credentials in our CAS SSO solution prior to the InCommon Assurance program. We leveraged this existing assurance infrastructure to bridge our internal credential LOA values onto InCommon Assurance identifiers. The SAML 1.1 support in CAS provided a convenient mechanism to indicate authentication method to clients, in this case the IdP. It was simply a matter of specifying how InCommon Assurance identifiers map onto particular authentication credentials. The following configuration snippet demonstrates this:

CAS Deployer Configuration (deployerConfigContext.xml)

```
<bean id="authenticationManager" class="org.jasig.cas.authentication.AuthenticationManagerImpl">
<snip/>
  <!--
  Populates the Authentication object with data about the authenticated
  principal or other circumstances of the authentication event.
  The Authentication object is an attribute or the TGT, so data in the
  Authentication can be provided to CAS clients at service ticket validation
```

```
    time.
    -->
    <property name="authenticationMetaDataPopulators">
      <list>
        <bean id="nistLevelPopulator"
              class="edu.vt.middleware.cas.authentication.metadata.LevelOfAssuranceMetaDataPopulator"
              p:attributeName="LOA">
          <property name="calculators">
            <list>
              <ref bean="usernameNistLevelCalculator"/>
              <ref bean="pdcNistLevelCalculator"/>
            </list>
          </property>
        </bean>
        <bean id="eduPersonAssurancePopulator"
              class="edu.vt.middleware.cas.authentication.metadata.LevelOfAssuranceMetaDataPopulator"
              p:attributeName="samlAuthenticationStatementAuthMethod">
          <property name="calculators">
            <list>
              <ref bean="usernameEduPersonAssuranceCalculator"/>
              <ref bean="pdcEduPersonAssuranceCalculator"/>
            </list>
            </property>
        </bean>
      </list>
    </property>
  <snip/>
  </bean>

  <!--
    URNs taken from
    http://www.oasis-open.org/committees/download.php/28706/sstc-saml-loa-authncontext-profile-draft-01.pdf
  -->
  <bean id="usernameNistLevelCalculator"
        class="edu.vt.middleware.cas.authentication.metadata.AuthIdLevelOfAssuranceCalculator"
        p:guestAccountLevel="urn:oasis:names:tc:SAML:2.0:post:ac:classes:nist-800-63:v1-0-2:1"
        p:pidAccountLevel="urn:oasis:names:tc:SAML:2.0:post:ac:classes:nist-800-63:v1-0-2:2" />

  <bean id="pdcNistLevelCalculator"
        class="edu.vt.middleware.cas.authentication.metadata.PDCLevelOfAssuranceCalculator"
        p:defaultLevel="urn:oasis:names:tc:SAML:2.0:post:ac:classes:nist-800-63:v1-0-2:1">
    <property name="oidLevelMap">
      <!-- Must list in order of descending value -->
      <map>
        <!-- Medium Silver -->
        <entry key="1.3.6.1.4.1.6760.5.2.2.5.1" value="urn:oasis:names:tc:SAML:2.0:post:ac:classes:nist-800-63:
v1-0-2:4" />

        <!-- Medium Bronze -->
        <entry key="1.3.6.1.4.1.6760.5.2.2.4.1" value="urn:oasis:names:tc:SAML:2.0:post:ac:classes:nist-800-63:
v1-0-2:4" />

        <!-- Basic -->
        <entry key="1.3.6.1.4.1.6760.5.2.2.3.1" value="urn:oasis:names:tc:SAML:2.0:post:ac:classes:nist-800-63:
v1-0-2:2" />
      </map>
    </property>
  </bean>

  <bean id="usernameEduPersonAssuranceCalculator"
        class="edu.vt.middleware.cas.authentication.metadata.AuthIdLevelOfAssuranceCalculator"
        p:guestAccountLevel="urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport"
        p:pidAccountLevel="urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport" />

  <bean id="pdcEduPersonAssuranceCalculator"
        class="edu.vt.middleware.cas.authentication.metadata.PDCLevelOfAssuranceCalculator"
        p:defaultLevel="urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified">
    <property name="oidLevelMap">
      <!-- Must list in order of descending value -->
      <map>
        <!-- Medium Silver -->
```

```
      <entry key="1.3.6.1.4.1.6760.5.2.2.5.1" value="http://id.incommon.org/assurance/silver" />

      <!-- Medium Bronze -->
      <entry key="1.3.6.1.4.1.6760.5.2.2.4.1" value="http://id.incommon.org/assurance/bronze" />
    </map>
  </property>
</bean>

<snip/>
```

The `*Calculator` components encapsulate the details of examining credentials, which in the case of X.509 certificates issued by the VT PKI is substantial, and computing an LOA value. We release NIST-like LOA values for internal use and InCommon Assurance identifiers for IdP integration. The e `duPersonAssurancePopulator` bean, in particular, is responsible for communicating that value to CAS clients such as the IdP via the SAML protocol AuthenticationMethod attribute.