Shared XACML Class – WMS, Annotation & DLR

The objective is to create a shared XACML class for WMS, DLR and Annotation Tool in R5.2. Note that the shared XACML class will not generate the XACML for licensed videos.

Scenario

1. Faculty Deposit (FD) and ETD embargo: A faculty member or a student has specified the embargo of a document. The ETD and FD software will capture the embargo period in the user input. Start date for FD is the date of the work submitted to WMS. Start date for ETD is the degree date. ETD and FD will calculate the end date by adding the embargo period to the start date. The xml for right event will show as below:

   ```
   <rulib:rightsEvent ID="2" authority="rulib">
   <rulib:type>Embargo</rulib:type>
   <rulib: dateTime encoding="w3cdtf" point="end" > yyyy-mm-dd </rulib: dateTime >
     <rulib:detail>Embargo period:  2 years</rulib:detail>
   </rulib:rightsEvent>
   ```

   The ETD and FD software will submit an object to WMS. When WMS sees an object with rightsEvent type=" embargo", WMS will call the shared XACML class by passing the end date and type of datastream to create a POLICY XML. The shared XACML class will generate the XACML. The XACML policy becomes a datastream in the object with ID equal to POLICY. All the presentation datastreams will be embargoed (i.e. PDF-1, JPEG-1, DJUV-1, XML-1, Audio, video) except Archive master. We will put a system restriction to the Archive master. (This procedure is outside the shared XACML. After the system XACML in place, we need to restart the fedora server.)
2. Annotations in unpublished stage: The Annotation application will check if an annotation is set to unpublished and pass the LDAP user id to the shared XACML class. The shared XACML class will create the XACML xml based on LDAP user id and return the POLICY xml to the Annotation application. A LDAP user id needs to be added to the fedora user xml file by calling dlr/EDIT script. (see note)
3. Jazz Oral History collection: The object with RightsMD: rightsMD / rightsEvent type="embargo" dateTime ="for ever", WMS will call the shared XACML class to generate the XACML xml to embargo all the datastreams. It will work for all the collections with rightsEvent type="embargo" set.

Shared XACML Class

Shared XACML will provide a general class to deal with these three scenarios above.

. 01/26/11 Jie

1. For FD and ETD embargo, WMS finds the item with Rights Event: embargo and detail is set, then call the shared XACML class to do the following to create the XACML.
   - When WMS see an object with rightsEvent type=”embargo” .
   - WMS will find the end date in <rulib: dateTime > and pass this information to shared class.
   - Shared XACML will create the POLICY XML based on the end date. It will convert the date to UTC date time and generate the XACML POLICY.
   - The POLICY will block all the datastreams to the public. (i.e. PDF-1, JPEG-1, DJUV-1, XML-1, Video, Audio etc..).

2. For annotations in unpublished stage, Annotations application will call shared XACML class to create the POLICY xml based on the LDAP user id.
   - Annotations application pass the LDAP user id to shared XACML class, shared XACML class generates the POLICY xml and returns the xml file to Annotations application.

3. WMS finds the Jazz object with ‘Rights Event type embargo’ and pass dateTime =”for ever” to shared XACML class, and to create the XACML. Shared XACML class will create the POLICY xml to not display the Audio datastreams to the public for ever.

WMS User Interface

There is no user interface for WMS in R5.2.

Note

- After object ingested, policy datastream will be viewable for Fedora admin user.
- An object has been ingested into Fedora without POLICY and needs one; DLR should call the Shared XACML class to add POLICY datastream to this object.
- If there is any changes to policy XACML datastream after ingested, policy datastream will be edited though dlr/EDIT. (At some point, WMS needs to be able to edit the datastream).
- For annotations in unpublished stage, LDAP user id needs to be added to the fedora user xml file by calling dlr/EDIT script (Jeffery will provide script that will automatically add the user ids to the user xml file). The shared XACML class will call the script to all LDAP user id to the fedora user xml file.
- If the creator changes the annotations status from unpublished stage to publish, Annotation application will call shared XACML class to delete XACML POLICY xml in fedora by giving the fedora id.
- WMS will provide user interface in next release

. 01/26/11 Jie