R5.2 Requirements for Linking Rights Events to Administrative Documents

From a CISC review, the following clarification regarding object relationships has resulted. A compound object is one with many simple objects (e.g. documents, video, audio, etc) where the simple objects have an intellectual relationship to the compound object itself or to each other. These relationships will be represented architecturally using ontologies and Fedora's relationship services. ETDs with supplemental files, data objects, and annotations of resources are examples of objects that might require this type of relationship. Another class of relationships arises when a resource is related to an administrative document (e.g., a license document). In cases like this, the administrative document will be a separate object and the resource object will reference the administrative document via the 'reference' element under rightsEvent and the associatedObject block of metadata. The reference to the administrative document will be via the persistent URL (PID). The remainder of these requirements refer only to administrative documents.

Assumptions

1. In general, only the collection manager (CM), or those so designated by the CM, will need to view the administrative document.
2. It is assumed that there can be multiple restricted documents that apply to a single resource object.
3. It is also assumed that linking from metadata is needed in only one direction, i.e. it is only necessary to link from the resource object to the restricted document; linking in the reverse direction is not needed.
4. The administrative documents are in a separate collection

The Administrative Documents Collection

Collections of administrative documents will not be accessible to the public and thus will not be attached to any public node. These collections can be indexed as deemed appropriate, but will not show on any public portal. There can be many of these types of collections (and sub-collections) and the collection manager will need to determine the structure for the collection of restricted documents. As For example, with the NJVid project, one could imagine setting up a collection of license documents for the various vendors, FMG, Global Media, etc. For the Jazz Oral History collection, a license document collection could be set up that holds the unique licenses for each oral history.

Process and Event Metadata

The basic approach would be to insert the PID (Handle) of the license document into the event metadata of the resource object. Assuming that the administrative document has been ingested, the

PID can then be inserted at the time the resource object itself is ingested. Otherwise, a WMS edit procedure might be used to insert the PID after the administrative document has been ingested.

Access and Access Restrictions

After review in the software architecture group, the following approach was decided upon. Given that rights event data is typically displayed in the full record, the PID of the administration document will be visible to public users. Therefore, access to this document will need to be authorized. The basic approach involves the following:

1. On ingest of the administrative document, an XACML policy will be inserted into the object. Note, that WMS will need to provide the capability for selecting the appropriate policy during the metadata creation and ingest process. The policy will allow access to administrative documents by those who are identified in an appropriate authorization database. There will be relatively few of these people and repository managers will need to provide administrative support for this database. (Note that our current Shibboleth/LDAP/XACML approach does not work very well for several reasons. First, we cannot identify these special roles in LDAP, and second, collection managers may not necessarily be associated with an institution that is running a directory database).
2. On display of the administrative document record, either in the full record or in showfed, a message would indicate that "sign-in" is required. At this point, we would redirect to a new process (rather than Shibboleth) in which we would authenticate and authorize the user. Upon success, the user would be able to view the administrative document. It should be noted that it is not necessary to restrict the administrative document to a PDF, although it is unlikely that other formats will be used.

Implementation in R5.2

In addition to the WMS changes above, it is assumed that required changes would affect the private portal capability, public record display, and showfed. The approach described above is relatively straight-forward to implement and is planned for RUcore R5.2 (targeted for mid-Winter 2010). We think that this approach might be useful in other applications with the following criteria: a) a relatively small number of users who need to be authenticated/authorized; and b) where the users might not all be members of an institution that has a directory and therefore do not have netid's.

rcj/jat/cmm – 06/21/2010