Authentication/Access of objects and datastreams

As agreed upon in the teleconference 11/12/07 we are focusing on two particular objectives with regards to access management.

1) Locking down particular objects in VITAL based on authentication and possibly IP Range

2) Locking down individual datastreams in VITAL based on authentication and possibly IP Range

VTLS has instructions on how to restrict access to the Access API and the management API of Fedora, this is done using XACML policies. These instructions can be found in the VITAL System management and Configuration Guide on page 35.

Furthermore Fedora is able to lock down individual datastreams only allowing access to specific users. This is done using XACML policies also. In order for this to work the individual datastreams that you wish to lock down will need to have unique metadata properties such as the FormatURI. The contents of the FormatURI is used by to differentiate between objects eg. Items that are locked down and Items that are not.

The above example of Fedora locking down records has two possible issues:

Firstly, locking down these items in Fedora does not change the way that VITAL displays or hides data, it is purely the end user communicating with Fedora based on XACML policies.

Secondly, So far there is no automated way to add unique metadata (FormatURI) to each item, so for example, the FormatURI will have to be added by hand to each object/datastream.

VITAL looks set to release access management in Version 4, at this stage we are unclear what the functionality and capabilities of this access management will be.