User Management and Access Controls Challenge Area

Current Status

We have created a Contributor Project around this problem area. For up to date information on this work, go to the Improved Fedora Security Layer (FSL) project page.

Required Features for first release

Vocabulary

- Simple, intuitive, well documented vocabulary for controlling Read, Create, Edit and Delete for Collections, Objects, and Datastreams
- Assign permissions by User or by Group, regardless of where user attributes are coming from (ie. LDAP, Shibboleth, OpenId, CAS, etc.)
- One vocabulary covers all equivalent methods in SOAP and REST APIs (ie. policies decide at a higher level who can edit a datastream, rather than saying who can call the modifyDatastream SOAP method)

Authentication (AuthN)

- Support *surrogate authentication* and document how to do it
- Support LDAP and Tomcat-Users
- Use servlet filters to enforce access controls on all inbound requests

Policy Manager / Authorization (AuthZ)

- Allow repository managers to find out what policies apply to a given Object, Datastream, or Collection
- Enforce policies at Datastream, Object and Collection level. (Rely on either RELS-EXT or Fedora's bundled RIsearch for evaluating collection memberships.)

General

- Keep the implementation stable & current
- Bundle solution with Fedora and include it in the installer
- Audit the Implementation for potential security flaws
- Support community innovation & allow people to completely replace the whole thing if they wish

Desirable Features (not required for first release)

- Support Shibboleth
- Support OpenID & OpenAuth
- Support Single Sign-on (SSO) - must be pluggable/overridable
- Allow for Custom AuthN