# User management and authorization

Assumptions (the system will be replicated in all DAC instances.):

1. User has been authenticated by logging in to  LSST, using identity management provided in NCSA
2. User has an account in LSST system

Related products:

- Resource management (NCSA)
- A+A (NCSA)

Question:

- I assume that the content for user workspace will not be duplicated at different DAC. Do we allow one user to have workspace at both US and Chile? If yes, how do we manage resources for the user?

Capabilities in User Management System:

- Identity mapping between the login-ID and LSST-ID

  CILogon service provides authentication service, allowing user to login with institute ID, Google ID, or GitHub credentials, just to name a few. After user authentication, LSST applications need to know the user's LSST-ID so the applications can access the authorization system for privileges for this user.

  When a user logs in with different credentials (GitHub, Google, institution ...),  the system should be able to map either one to the correct LSST-ID.

- Content of the user management system
  - contact information:
    - user name, address, phone number, email, institute
    - contact preferences (like subscribe to list of newsletter ...)
    - group information: group names the user belongs to
  - group information:
    - group name, admin for the group, users in the group
    - data access info for the group
  - information regarding data rights: right to search, to view, to download.
    - Table access granularity:  release level, table level or row level
    - File system access granularity: directory, file
    - when a user loses the data right at time A, but still has access to data produced/released before time A, the system needs to have capability to distinguish this.
  - Information related to resources:
    - User workspace: DAC,  root directory, disk usage and quota,
    - User database: name, database server, database usage and quota,
    - Computation: CPU usage and quota,
  - Alert subscription database:
  - Access control information:
    - Sharing with other users
    - Collaboration group sharing
  - User preference in Portal and Notebook
    - First question: Shall we save the user preference in the central user management system, or Portal/Notebook keeps its own?
    - For portal, some of the preferences are mainly meaningful in portal, but some could be shared with Notebook, like search history.
      - search history, ...
      - Table data display: table page size, selected columns, sorting (asc, desc) preference,
      - Image display: preferred stretch, distance unit, default zoom level, coordinate system and format for position readout, coordinate grid overlay on images, color preference for catalog overlay, ...
      - XY plot display: columns as X, Y axis,
    - For Notebook ....

Administration of the User Management System

Self service by users
- contact information update
- password retrieval/reset
- create a group and manage membership in the group
- grant permission to other user and/or group to access my workspace (read/write/execute)
- can a user merge two accounts created by accident? But more importantly, how do we prevent a user to create multiple accounts to get more resources?

API to access the user management system

- login API should take redirect URL after successful login
  Token granted after successful login:
    - Life duration of the token

Background information:

From LDM-542 2.2.7  Data Access Permissions and Quotas
"Users who had LSST data rights but have since lost them may be granted access to the data products available as of the time of loss but not newer ones."