Design and Implementation of Unified Authentication Management System of IHEP

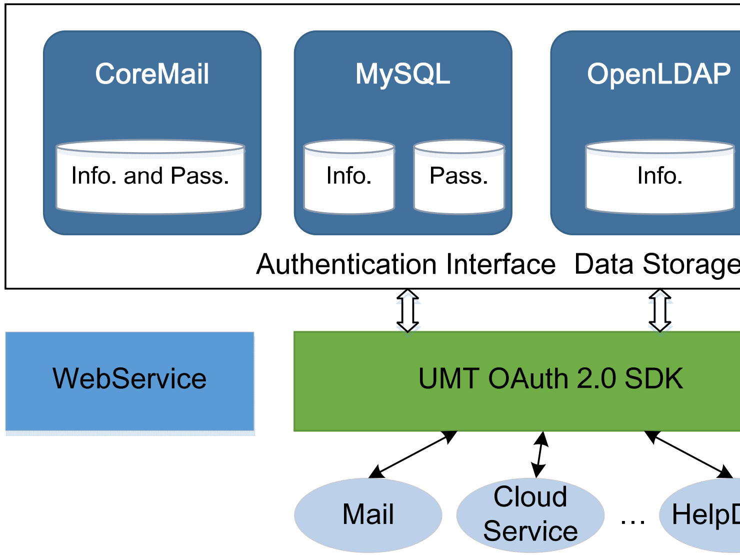
Li Wang, Zhihui Sun, Fazhi Qi

Institute of High Energy Physics, 19B Yuquan Road, Beijing, 100049 China

System Architecture

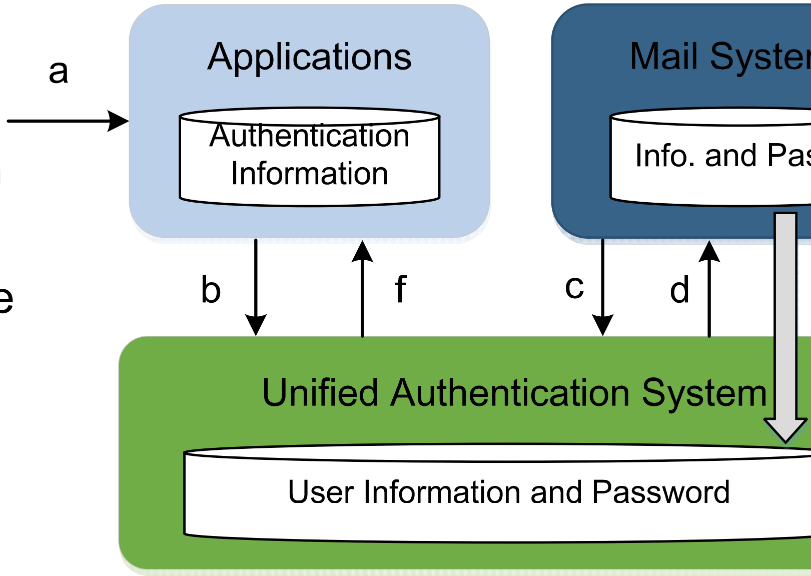
- The identity data integration and sharing of the LDAP directory service has a secure authorization and authentication mechanism and fine-grained access control. LDAP directory services and OAuth2 protocol allow efficient and simple integration with existing authentication mechanisms to make user information easy to manage and quick data access.

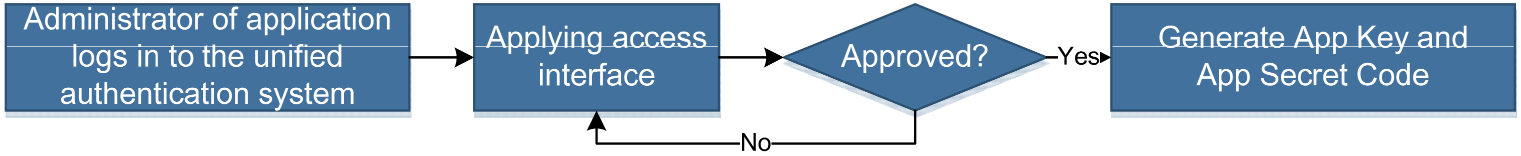
- The proposed architecture allows users to single sign-on and authenticate. After authentication, users can directly access a variety of information systems and resource services, such as the mail system, personal cloud storage services, HelpDesk, managed by the unified LDAP directory service.



Data Flow and Workflow

- Data Flow
  - The data flow of IHEP unified authentication management system (Figure 3) is described as follows:
  - a. One user initiates a login request to a target application;
  - b. The application redirect the request to unified authentication management system;
  - c. The unified authentication management system sends the user's information and password to the mail system to continue the authentication;
  - d. If the authentication does not pass, then use the local database for authentication; if one of the two authentication methods is passed, then go ahead with the next step;
  - e. Sync the user's personal information from the mail system into the unified authentication database;
  - f. Return the user's authentication information for further operation of the target application system.


a
Applications
Authentication Information
Mail Syster
Info. and Pas
b
f
c
d
Unified Authentication System
User Information and Password


Administrator of application logs in to the unified authentication system
Applying access interface
Approved?
Yes
No
Generate App Key and App Secret Code

Workflow