The Design of the Unified Identity Authentication System for IHEP

Qi Luo, luoq@ihep.ac.cn

Institute of High Energy Physics,

Chinese Academy of Science

2023-03

Outline

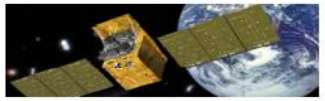
- User Identity Authentication platform @IHEP
- Identity Authentication Challenges for IHEP & Goals
- The Unified Identity Authentication System for HEPS
- Summary & Plant

IHEP-Institute of High Energy Physics

- IHEP is hosting or attending >15 experiments around the field of high energy physics
- Mass data (~PB/year) from multiple experiments
- IHEP localed in Beijing

BESIII (Beijing Spectrometer III at BECPII)

JUNO (Jiangmen Underground Neutrino Observatory)



HXMT(Hard X-Ray Moderate Telescope)

China Spallation Neutron Source

LHAASO (Large High Altitude Air Shower Observatory)

HEPS (High Energy Photon Source)

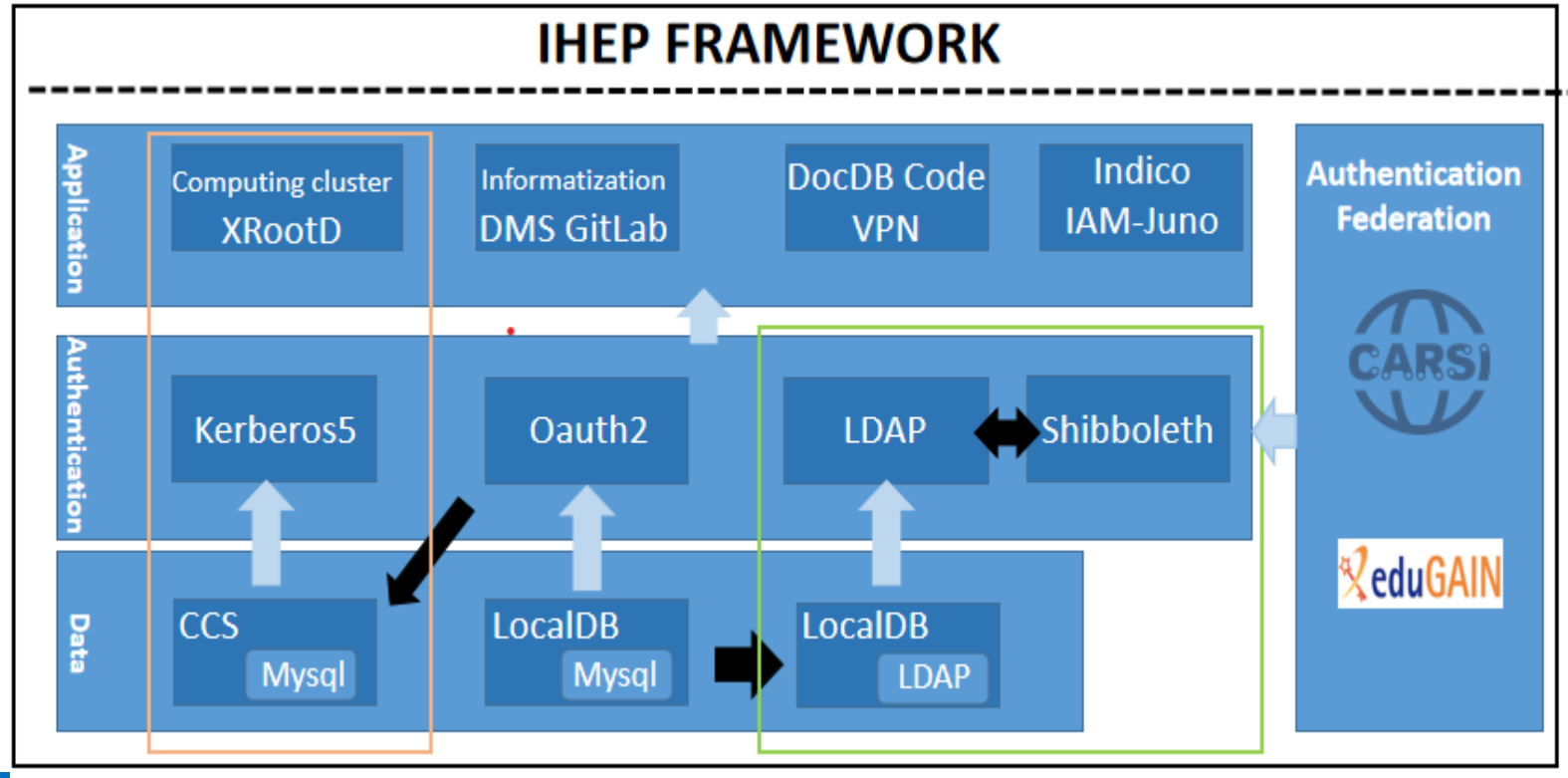
User Identity Authentication platform @IHEP

IHEP SSO capacity

- Support for multiple authentication protocols, Kerberos5、OAuth2 and Shibboleth
- Support for multiple databases, mysql and LDAP
- Support OAuth2、LDAP and Shibboleth applications :260~

Current Status

- Total users : 24700~
- VPN groups: 27~
- Cooperations : 160~
- Computing cluster users: 4100~
- Computing cluster groups: 130~



Identity Authentication Challenges for IHEP

IHEP remote multi-site multi-source authentication

- IHEP hosts many remote scientific equipment and facilities
- A large number of cross-disciplinary experiment needs
- More and more scientists will joining in

Dynamic authority management

- Deep intersection of disciplines
- Multidisciplinary experimental needs of scientists
- Different experiments need different operation permissions

Accounts & Data security

- Generate massive data per year
- Various identities of scientists
- Remote operate experiments

Goals

IHEP remote multi-site multi-source authentication

- Interworking between different sites
- Multiple devices using one account
- Unite CARSI and EduGAIN

Dynamic authorization management

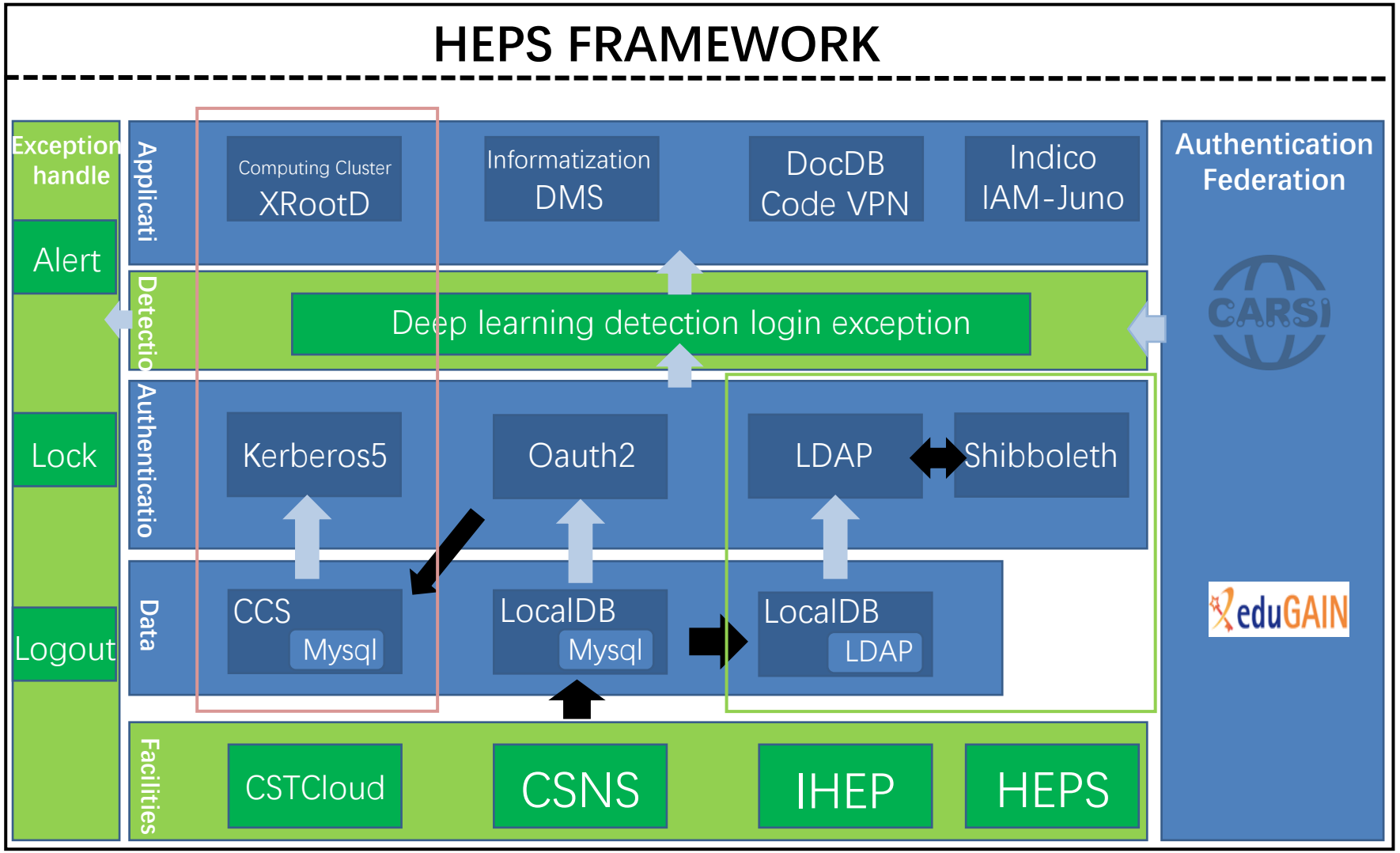
- Apply for permission changes at any time
- Users from inside and outside IHEP have different apply processes
- Users from different experiments have different permissions

Accounts & Data security

- Collect login logs for all the accounts
- Abnormal login detection
- Handle login exceptions automatically

Design of the Unified Identity Authentication System for HEPS

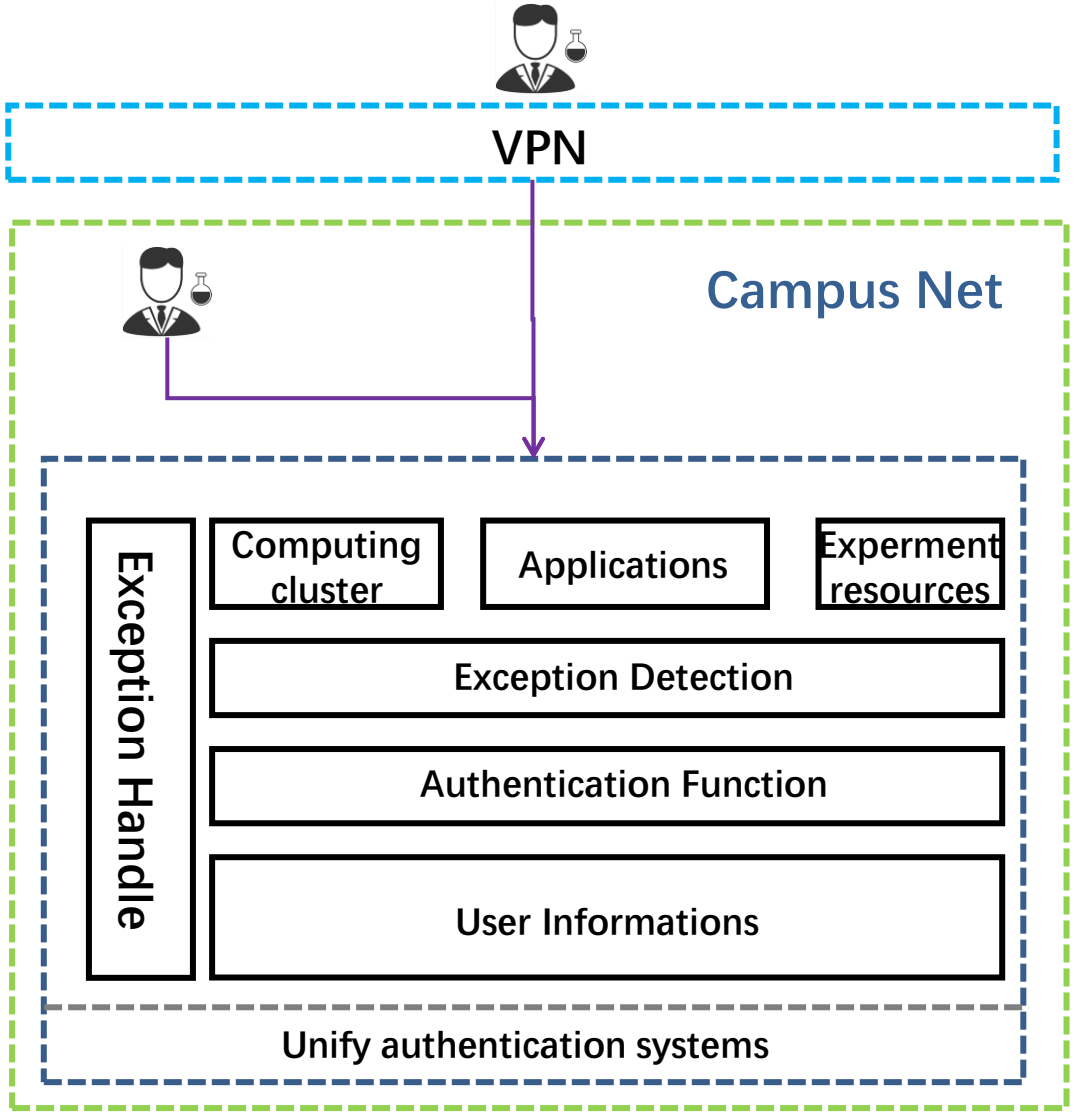
- Hihg Energy Photon Source(HEPS)
- New Features:
  - Forming four large device authentication alliances
  - Illegal login detection by deep learning
  - Automatically handle exceptions



Unify authentication systems of funtion

HEPS Unify authentication systems of funtion

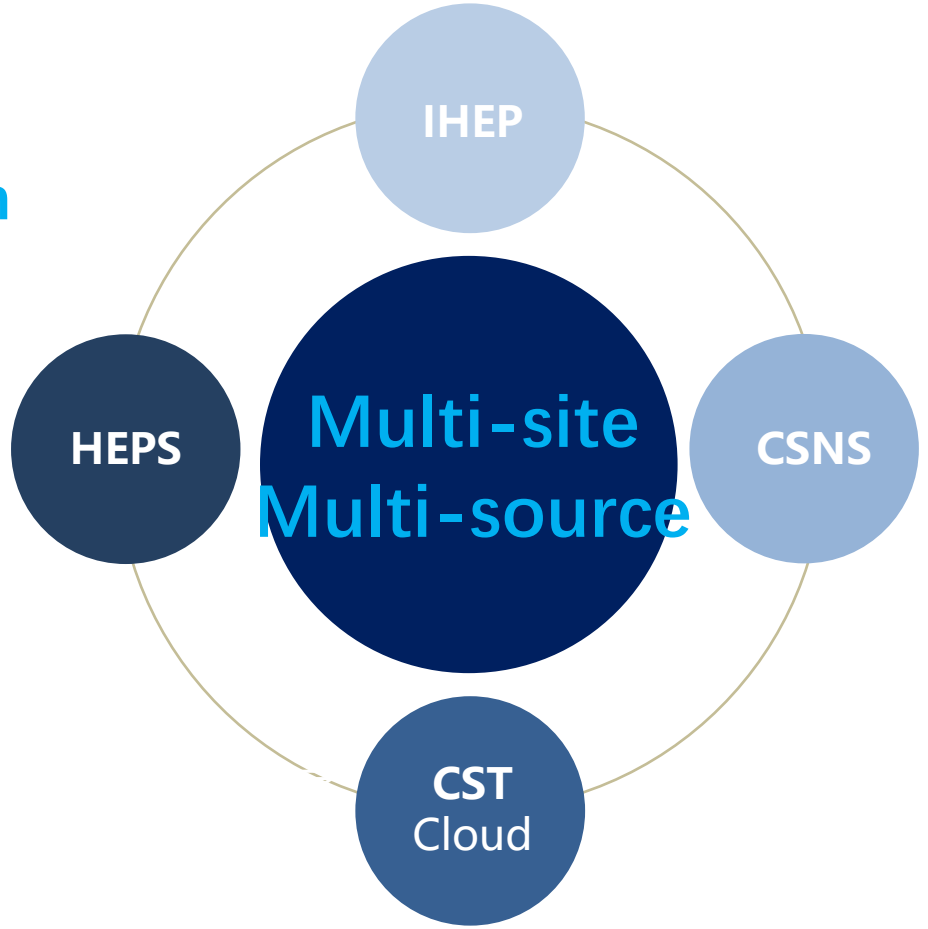
- VPN for External scientist to access resourcs
- Exception Detection collect all informations when user use resours
- Collect personnel information of the four site
- Handle login exceptions automatically



Unify authentication systems of multi-sites

HEPS remote multi-site multi-source authentication

- Build Internal authentication Alliance
- Make The Institute of High Energy Physics of the Chinese Academy of Sciences (IHEP)、China Spallation Neutron Source(CSNS)、High Energy Photon Source(HEPS) and Chinese Academy of Sciences(CSTCloud) accouts data synchronization
- One account is accessible



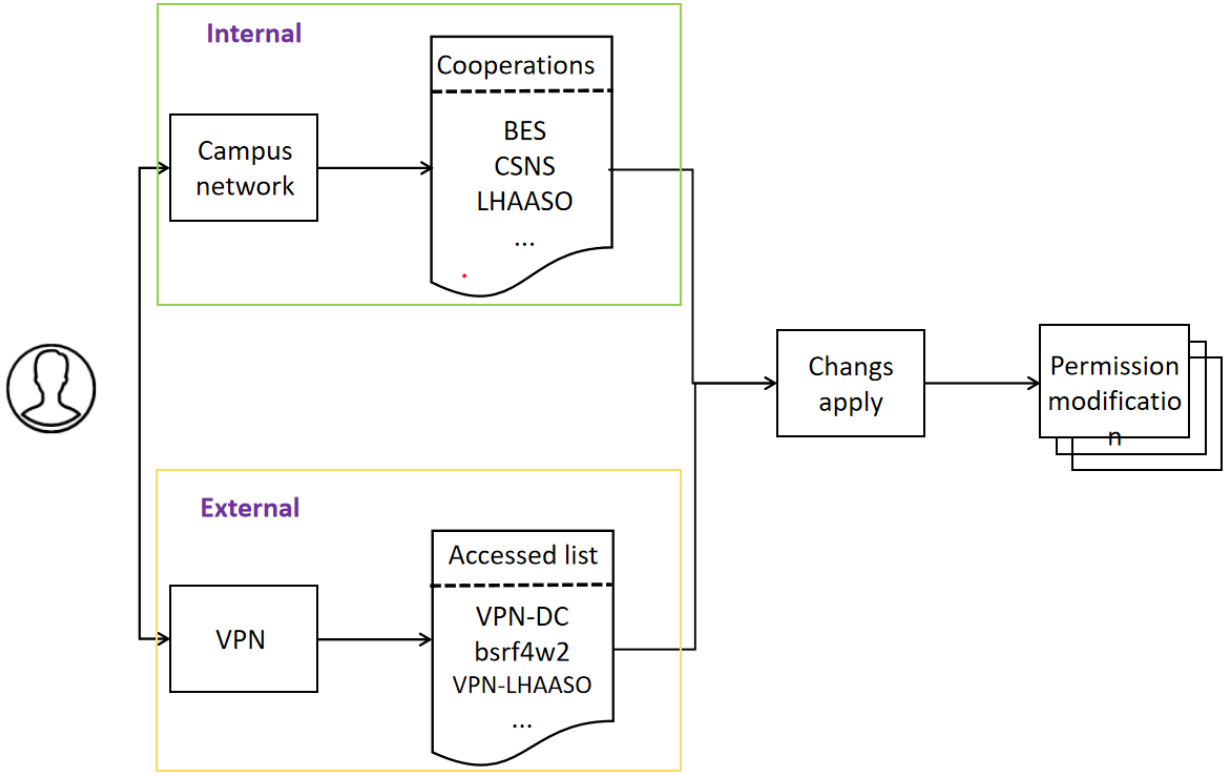
Dynamic Authorization Management

For IHEP Internal User

- Experiment using campus network access
- Each experiment corresponds to a Cooperation group
- Owning multiple collaboration groups at your authority
- Permission can be modified only after administrator's acceptation

For IHEP External User

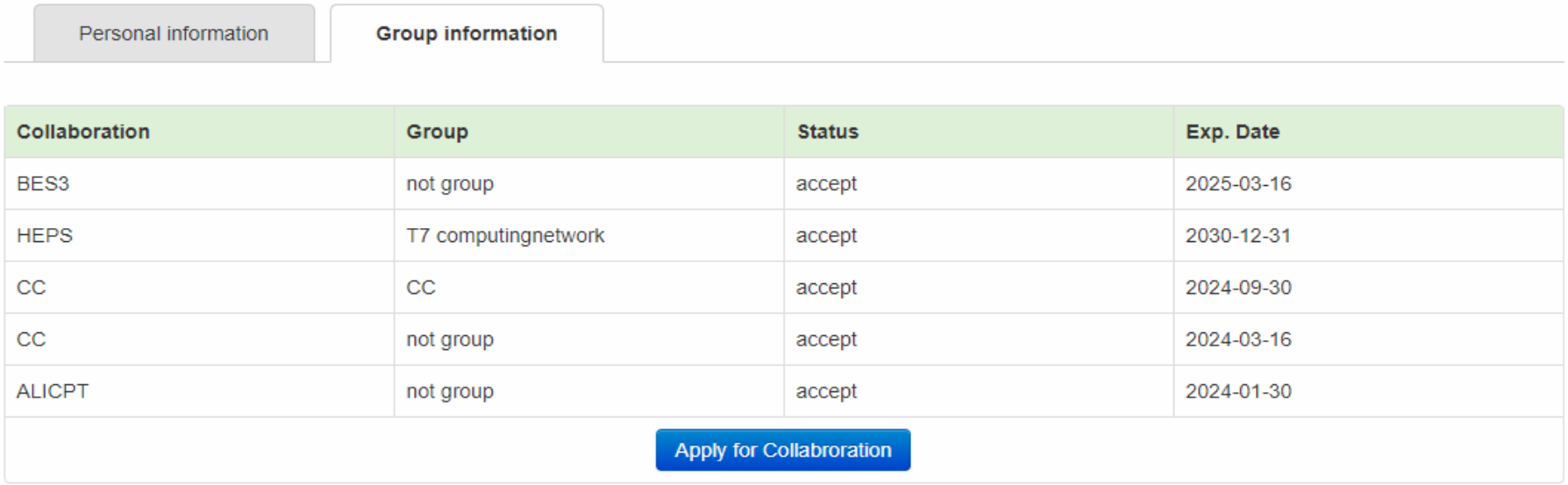
- Use VPN to connect experiment net
- VPN has accessed list to different authorization
- Permission can be modified after administrator's acceptation



Dynamic Authorization Management-- for internal user

IHEP Internal user

- Can choose your collaboration
- Automatically send apply mail to collaborate administrators
- Can have multiple cooperation group permissions at the same time



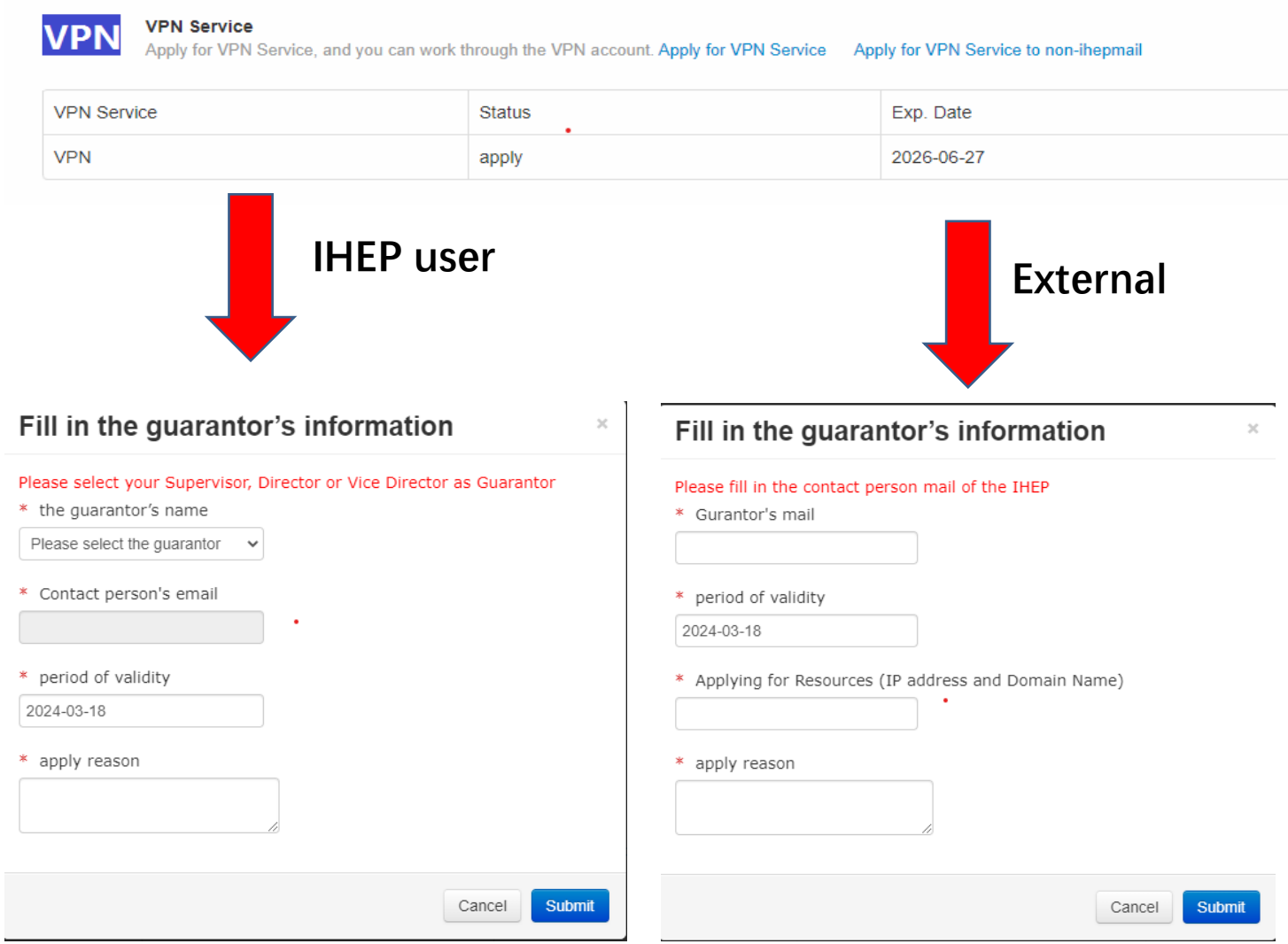
Dynamic Authorization Management-- for external user

VPN IHEP user

- Choose your Guarantor
- Automatically fill in the Guarantor's email
- Fill in your apply reason
- It will send a mail to your Guarantor

VPN External

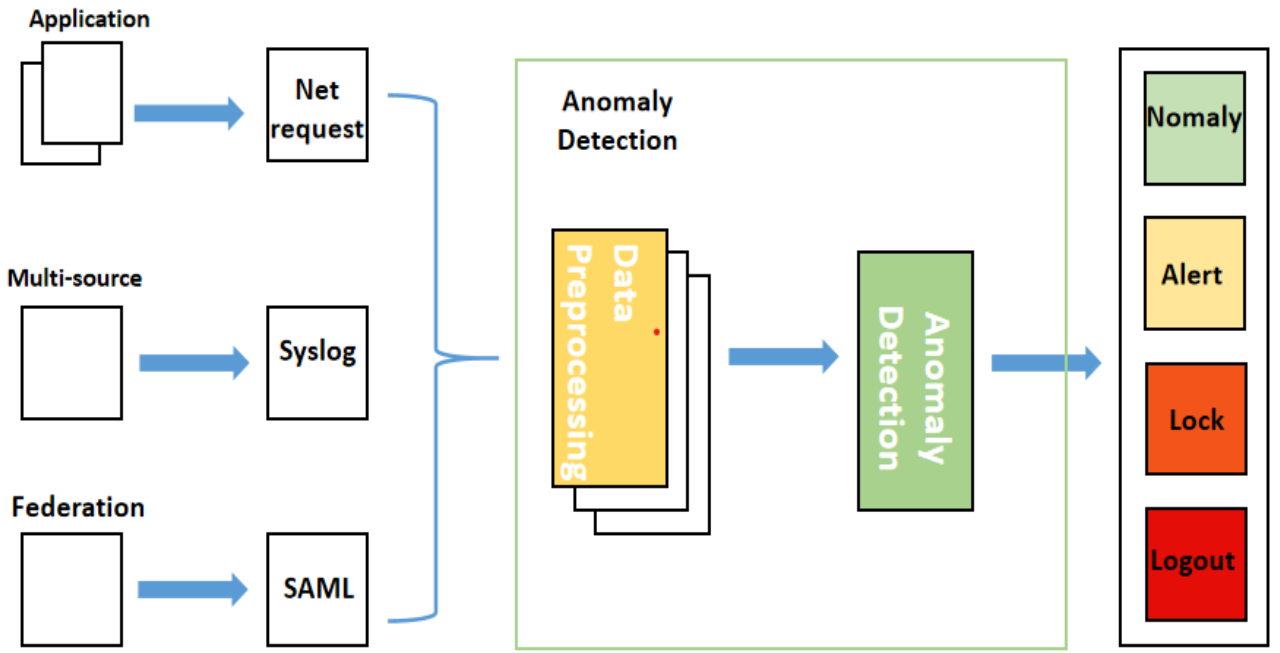
- Fill in your IHEP contact person mail
- Fill in you want apply resources
- It will send a apply mail to your contact person



Illegal Login Detection

Detection & Alarm

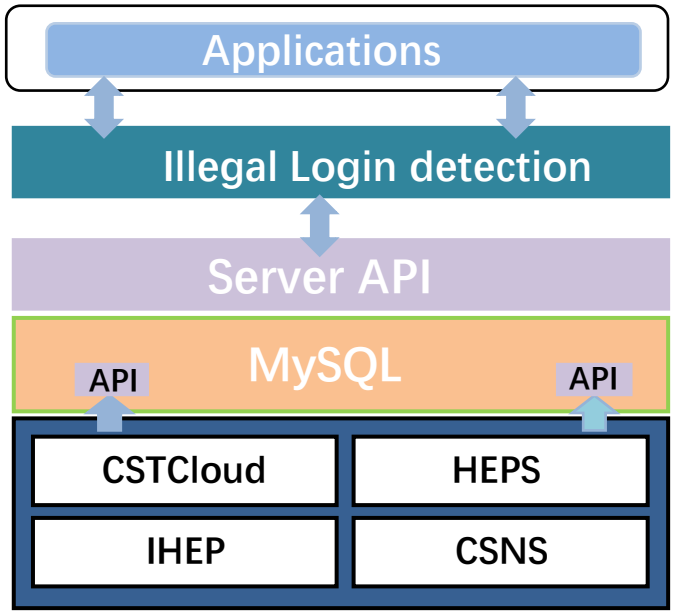
- Collect multiple types of data
  - ✓ Net request、Syslog and SAML information
- Use Deep learning to detect exception
- Automatic classification alarm
- Different levels of alarm automatically do corresponding processing
  - ✓ Alert、Lock and Logout
- For different levels of alarm, there are corresponding unlock policies



Extensibility and Compatibility

Unified interface

- For better extensibility and access the application
- The modules communicate with each other using standard Restful API
- Allow experimental applications access by Oauth2 、Shibboleth and so on



Summary

- Build multi-site multi-source authentication
  - Realize multi-source data synchronization
  - Multi-site interworking
- Dynamic authority management
  - Realize the dynamic change of experimental permission
  - Simple and convenient application process
- Anomaly Detection
  - A unified and comprehensive big data monitoring platform
  - Use deep learning to automatic handle
  - Exception automatic classification
- Unified interface to better expand and access the application

Next Plan

The plan

- 2023.8 to achieve the first version of HEPS the Unified Identity Authentication System
  - ✓ Support the first batch of 14 beamline stations
  - ✓ Synchronization Multi-site accounts data to realize Multi-function of one account
  - ✓ Dynamic authority apply function

Thanks for your attentions!