RBAC @ GSI

Current State & Outlook

What is RBAC

- **RBAC : Role-Based Access Control**
  - CERNs developed solution for providing a sufficient level of device access security
  - Fully integrated into the CMW RDA library
  - Originally deployed at LHC, but used widely nowadays

- **Motivation behind RBAC *:**
  - Protects against human mistakes
    - A well meaning person from doing wrong thing at the wrong time
    - An ignorant person from doing anything at anytime
  - Can be deployed anywhere in the Controls Infrastructure
  - Aims to enhance the overall Machine Safety
  - Provides Authentication (A1) and Authorization (A2) services

  - **Does not prevent hackers from doing damage**

* taken from CERN Presentation slides

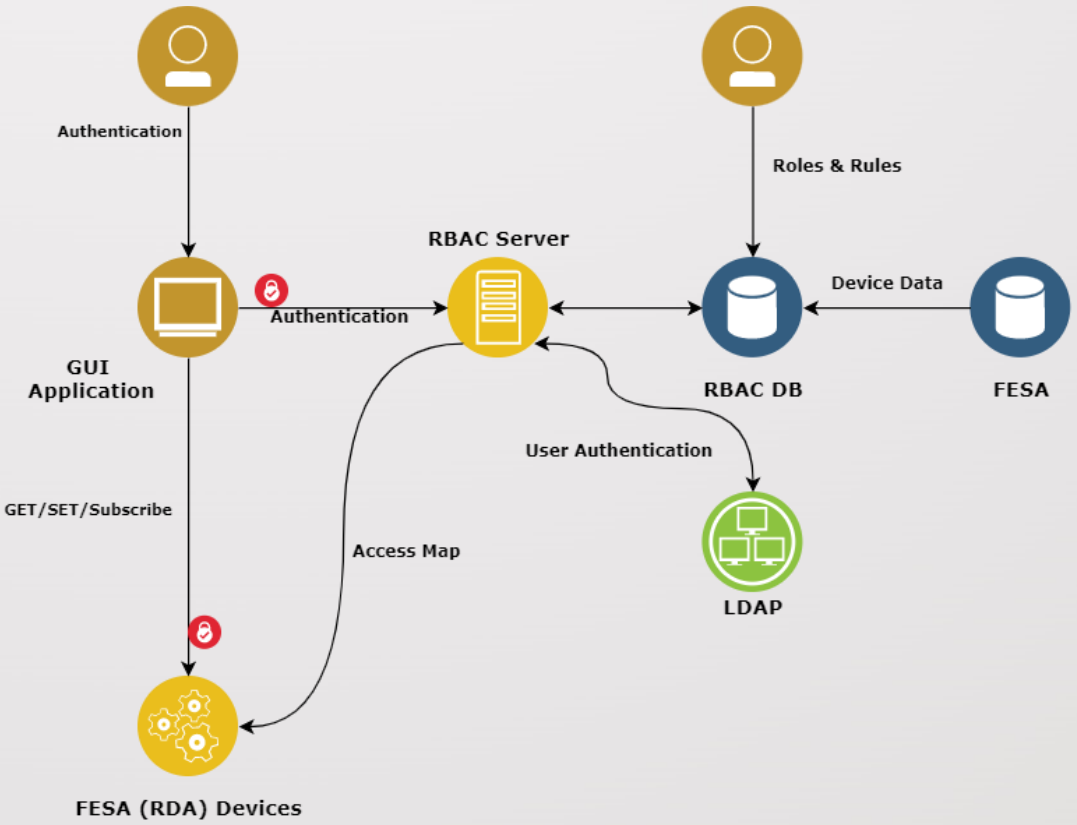
Architecture

- **Authentication**

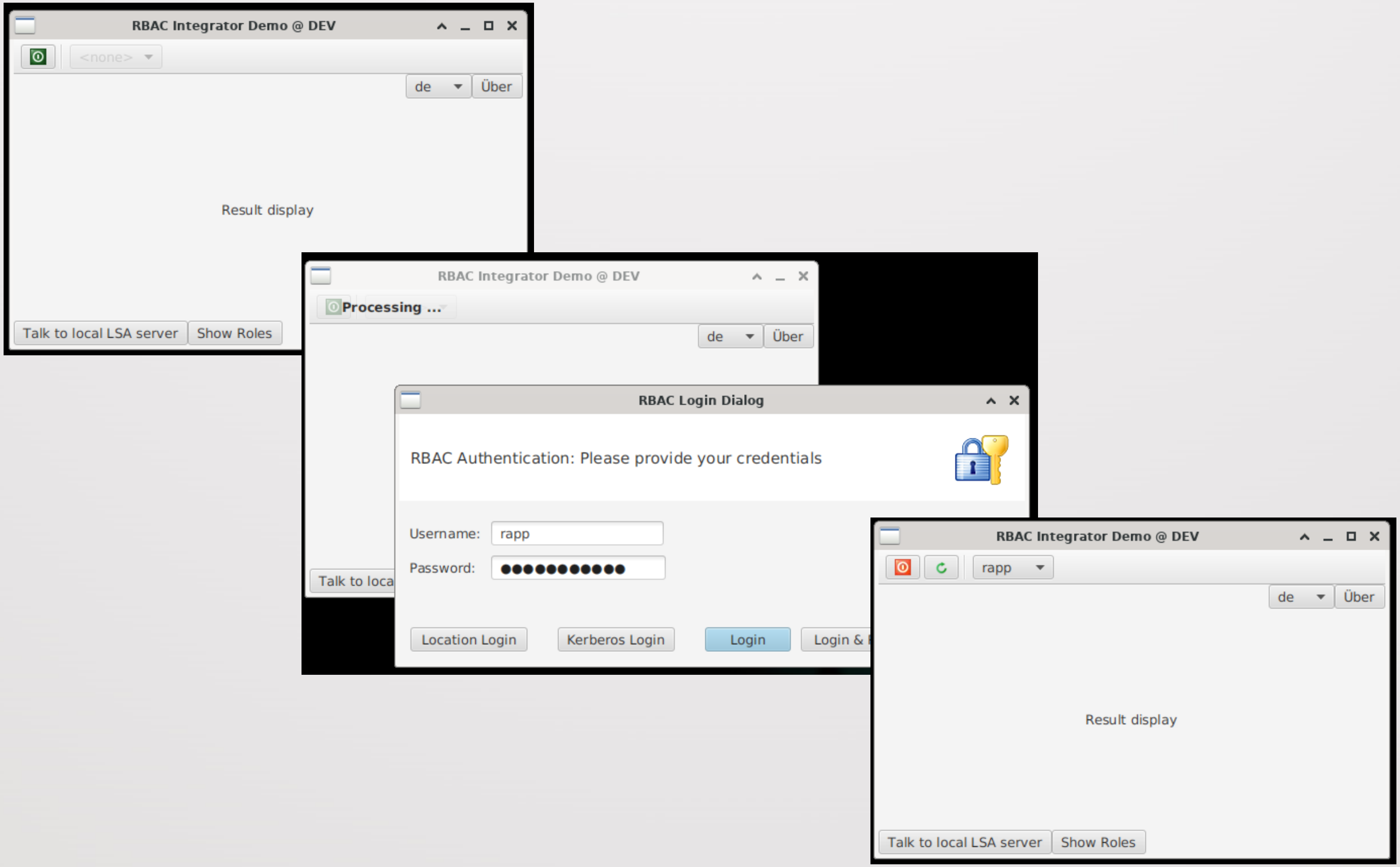
  1. User can be authenticated with password or location
  2. RBAC Server returns a token containing a list of associated roles

- **Authorization:**

  - Application sends token to CMW (FESA) when connecting
  - FESA verifies token signature once and uses the credentials for every subsequent request
  - CMW checks access map to authorize a request



User Perspective



Result display

Processing ...

RBAC Authentication: Please provide your credentials

Username: rapp

Password: ●●●●●●●●●●●

Result display

Components and state @ GSI

- **Database**
  - Database is available but, mostly, empty
  - Will be filled gradually when use-cases are defined
- **Server**
  - Source code adopted for GSI and is up and running
  - Connects to ACC LDAP
    - Controls Account required for personal authentication
- **Client**
  - JAVA and C++ clients are available at GSI
    - Will be integrated into new FESA and YOCTO based devices

- **Summary**
  - Technically RBAC components are available and can be used
  - First simple Use-Cases are in elaboration

Next Steps

- **Definition of a basic Roles and Rule Concept for the operation (*ongoing*)**
  - Can and will be refined in the future
  - *Input from Operations group is required*

- **Step-by-Step integration into the operation**
  - Understanding the actual GSI needs and use cases
  - Identify and address technical shortcomings
  - Refining of the Rule concept
  - Definition of responsibilities
  - etc.

Questions ?