Generic permissions model implementation with Apache Shiro
Authentication and authorization

Context
Annotation platforms: Vesta and Pacte
Registered users, private data, sharing data to collaborate on projects and studies
REST API backend (Scalatra)

Authentication service
- Login with Apache Shiro (username and password)
- Returns JWT with authentication data
- Token sent on each request to the Platform backend API

Authorization service
- Each method defines its authorization requirements (roles and/or permissions)
- Validation:
  - Wildcard Permission syntax
  - role names
- Shiro Realm implementation
Permission model

Models
- Users: admin@platform.com, student-one@u.com
- ResourceType: Project, Corpus, Lexicon, Platform
- Resources: Vesta Platform, Wikipedia Corpus
- Actions: VIEW-Project, VIEW-Corpus, CREATE-Corpus, DELETE-Corpus
- Roles: MANAGER-Project, MEMBER-Study, ADMIN-Platform

Examples
- User student-one@university.com can Create any Corpus in the Training Project
- User student-one@university.com can View the Training Project
- User admin@platform.com has Role ADMIN-Platform in the Vesta Platform
- Role MANAGER-Project in the ABC Project can Create any Corpus in the ABC Project
- Role MANAGER-Project in ABC Project can View the Wikipedia Corpus