CORE-Storage AAI

Current Planning

Marius Dieckmann[1,2,3]
Marius.Dieckmann@computational.bio.uni-giessen.de

[1] Justus-Liebig-Universität Gießen

[2]NFDI4Biodiversity

[3]de.NBI

October 25, 2021

Current situation

- Keycloak OIDC endpoint with Github as IdP provider
- Users are assigned a group to access the overall CORE-Storage API
- Token is a JWT token that can be passed in via Header and is verified inside the App
- "Project" level authorization is checked internally via user id in sub field
- APIToken for machine level authorization, managed internally
- Data objects are authorized via presigned URLs

Current ideas - OIDC

- Common NFDI OIDC endpoint that supports various IdP
- JWT contains information about project level access rights that are transistent across multiple apps
- Management is provided via a centralized component
- OIDC client management is done by the Ops people
- More fine grained control optional on per app basis?
- Some kind of API-Token required, either centrally or from the app -¿ is it possible to use long-lived JWT token for this?