Postponed

API Authentication

This page is a discussion base and documentation about the authentication system of the API.

Questions

- How can a token be created?
  - Every User (here we can differentiate between roles) can create a token fixed on his username
  - Every admin can make a new token, which is linked to a descriptive name and available through the admin interface
  - Every application can create a token through a link (e.g. /api/0.1/get_token?name=pelagios)
  - Everybody can get a token through a link but need to login via the link (e.g. /api/0.1/get_token?user=admin&password=adminpassword)
- How long should a token be valid?
  - Differentiate between user token and application token?

Token-Based vs. CORS

To be filled.... (What is Token-Based and CORS, advantages and disadvantages, usage, flask compatibly?)

Discussion stuff

- Tracking the IP of the first login

- API Authentication (#1185, #1233, #1211)
  - Who should be allowed to make tokens? -> admins and manager
  - Can an application make a token of its own with the needed credentials? -> Has to
  - Should we make a time limit for a token? -> 15 minutes, credentials get no expire date
  - Do we want to know who and when a token is created?
  - Do we want, that information about a token is store, so we can reject it? Yes

Resources

- JWT Handbook
- https://pyjwt.readthedocs.io/en/latest/

Files

jwt-handbook-v0_14_1.pdf	1.65 MB	2020-06-02	Bernhard Koschicek