Interview-Evaluation

Goal of the exercise

1. Connect to SCA Tork Easycube API
2. Display the siteName of the Site on a web page

Resources available

- Postman collection: "SCA Tork EasyCube API v3.0.1.postman_collection.json"

The file is shared during the test.

Credentials to access the API

Do not share the credentials nor store them on GIT!!!

- client_id : [client_id]
- client_secret : [client_secret]
- grant_type : client_credentials
- scope : EasyCube.External.Api

API addresses

1. Use **“login/authentication”** api
    1. URL for the authentication: https://login.easycube.torkglobal.com/connect/token
2. Use the **“api/Site”** api
    1. Prefix the url
       with https://easycube-external-api-web-c2m2jq5zkw6rc.azurewebsites.net

Accepted technologies

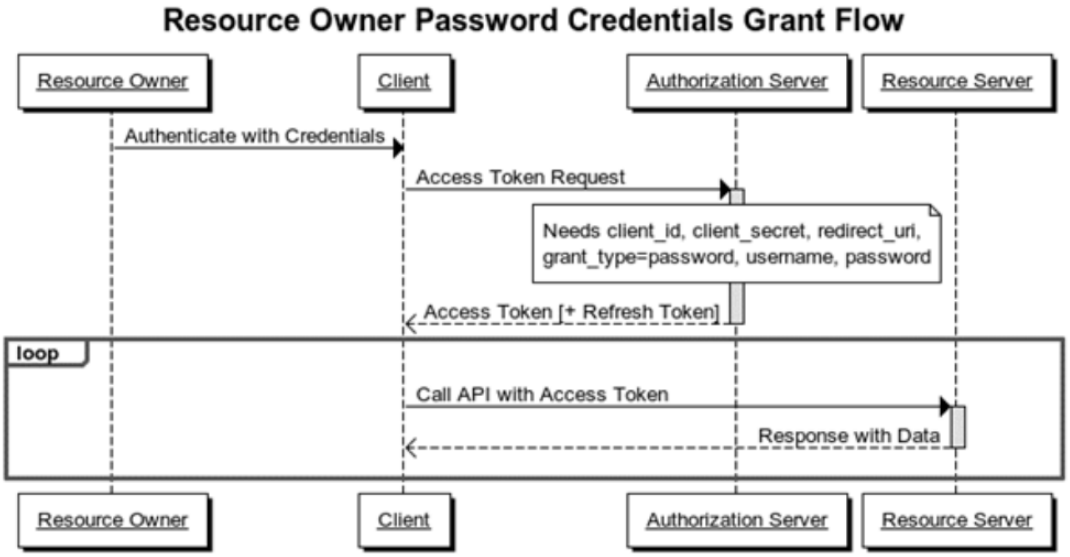
- Python, Flask, Gunicorn
- Angular
- React, NextJS

Authentication and Authorization

The system API is secured with OAuthv2(see https://tools.ietf.org/wg/oauth/)and uses the "Resource Owner Password Credentials Grant" as the authentication.

Each third-party integrator is given a specific client id and secret which must be used to connect to the authorization server. The integrator must ensure the secrecy of those identifiers (client_id and client_secret).

Authorization to a specific company is arranged by creating a company specific System API user, which has its own username/password.
This user can only access one company and can be given a specific role, for example "Status Client" or "Personal Locker Control Client", which limits what the user can do.
With the 3client id/secret and the company specific System API user account, the integrator can use the system API.
Preferably the client follows the offline OAuth mode, with using an Access Token & Refresh Token.



-- end of the report