SmICS

The Smart Infection Control System (SmICS) is an application for the support of the infection control units in clinics. For the general use it is necessary to connect the application to an openEHR Repository like ehrbase. It offers different statistics, a patient timeline of the patients locations and a contact network for patients to track possible transmission paths.

Requirements

Repository

Installed and functional openEHR Repository which provides the basic REST API from the openEHR Reference Model.

The openEHR Repository needs to be prefilled with following templates and compositions for these templates:

- Stationärer Versorgungsfall
- Patientenaufenthalt *(Altough "Station" is no mandatory field in the template, it is necessary for the full functionality for the SmICS)*
- Virologischer Befund
- Imfpstatus
- Symptome

Upcoming:

- *Mikrobiologischer Befund*

Hardware

Server

- CPU: 4 Cores[1]
- RAM: 4 GB[1]
- Storage: 5 GB[1]
- OS: Linux *(recommended)*[2]

[1] *Estimated Requirements*

[2]*Although you could use it with Windows if your Docker is able to work with Linux Docker Container. On Windows Server there is a LinuxKit necessary which is available for Windows Server 2019*

Workstation

- Full HD Monitor (or higher)
- Google Chrome Browser Version 88 (or newer)

Docker

Docker or docker-compose tool.

Installation: https://docs.docker.com/engine/install/ and if necessary:
https://docs.docker.com/compose/install/

Execution

Get the Software

Download the latest versions of the SmICSCore and the SmICS Visualization

SmICSCore: https://github.com/highmed/SmICSCore/releases
SmICS Visualization: https://github.com/highmed/SmICSVisualisierung/releases

Certificates

Before you build and run the SmICSCore you need to copy your Root Certificates of your local CA in the
Certificates folder.

Build & Run Process - Docker

Within each local git repository following commands need to be executed. **You need to start with the
SmICSCore Repository**

If you didn't created an Docker network you need to do so. You just need to do this ones.

```
docker network create smics-net
```

To build and run the containers run the following commands.

```
docker build -t smics .
docker run --name smics_core --network smics-net -e
OPENEHR_DB="$OPENEHR_REST_PATH" -e AUTHORITY=$AUTHORITY -e CLIENT_ID="$CLIENT_ID"
-e CLIENT_SECRET=$CLIENT_SECRET -d -p 9787:9787 smics
```

Environment Variablen - SmICSCore

Environment	Description
OPENEHR_DB	The path to the RESTful API from the OpenEHR Repository e.g. for local Better: http://localhost:8081/rest/openehr/v1
AUTHORITY	The link to your oauth2 authority e.g. for local keyclaok: http://localhost/auth/realms/realmName
CLIENT_ID	Your ClientID of your oauth2 client
CLIENT_SECRET	Your ClientSecret of your oauth2 client

```
docker build -t smicsvisualisierung .
docker run --name smics_visualisierung --network smics-net -d -p 3231:3231
smicsvisualisierung -e USE_AUTH=$bool -e SMICS_HOSTNAME=$SMICS_HOSTNAME -e
AUTH_PROVIDER_URL=$AUTH_PROVIDER_URL -e AUTH_REALM=$AUTH_REALM -e
AUTH_CLIENT_ID=$AUTH_CLIENT_ID -e AUTH_CLIENT_SECRET=$AUTH_CLIENT_SECRET
```

Environment Variablen - SmICS Visualization

Environment	Description
USE_AUTH	Set true for enabling oauth2 authentication
SMICS_HOSTNAME	DNS of your server where the smics is running
SMICS_PORT	The port which you use for the SmICS Core Default: 9787
AUTH_PROVIDER_URL	The root link to you oauth2 server
AUTH_REALM	Name of you oauth2 realm
AUTH_CLIENT_ID	Your ClientID of you oauth2 client
AUTH_CLIENT_SECRET	Your ClientSecret of your oauth2 client