Project description

VariantPoints: Points of Interest (PI)

VariantName: Administrator

Points of Interest are the main point of the individual part. **What is a PI?**

> **A Point of Interest represents an important location or store which the Actor is looking for almost every day or when going on vacation, is looking for to visit. It can represent a supermarket, the statue 'Gëlle Fra', petrol stations and many more.**

PIs are introduced and classified by categories to differentiate between different types of PIs. **What does the category represent?**

> **The category specifies a set of PIs, grouping together:**
>
> - **multiple equal PIs in different GPS positions or**
> - **same type of Points of Interest but different names.**

So, a lot of petrol stations are stored in the same category but with different GPS coordinates. But also, a lot of supermarkets in a category can have different names (like Cactus, Cora, Auchan, …).

Actors

- MsrCreator
- Authenticated
- Administrator
- Coordinator
- Person
- Driver
- Pedestrian

The **MsrCreator** will have only one functionality and that is to create the system.

The **Authenticated** is a super actor from which multiple actors like the Administrator, the Coordinator and the Person will inherit to use specific operations/functions which all actors can do like logging in and out.

The **Administrator** is responsible for the PIs. He inserts a list of Points of Interest into the system stored by different kind of categories to help the Person from accessing/searching for a PI. He is also in charge of updating the information of a PI when the PIs have changed their GPS location or other information, or new Points of Interest must be added.

The **Coordinator** should be responsible of getting the specific requests to add new PIs and deliver them to the Administrator. Another task should be checking if the PIs are not already in the system and alert the user of the specific requested PI.

The **Person** needs to have a possibility to access PIs. The provided list of PIs from the Administrators is now available for the Actor. He can access the PIs and use the GPS location to localize the Point of Interest. PIs are important for the Person almost every day.

Now if we apply the difference between the **Driver** and the **Pedestrian**, then the **Driver** must receive the GPS locations with maybe the remaining distance in kms differently from the **Pedestrian** because he is walking by his feet.

Variant points: access rights

Variant name: experience level

Access rights are the permissions a person has, to access a certain place or resource. They are assigned following a person's role in the system. This means there is an access control system which defines the system's hierarchy and how the permissions are assigned within it.

The three basic types of access rights are defined as:

- **Read**: The user can view a file's or directory's content.
- **Write**: The user can change a file's or directory's content, which means he can add, delete, update or rename information.
- **Execute**: The user can run executable files.

Every other permission is the result of a combination between these basic access rights.

After having defined and granted permissions within a system, there needs to be a way to verify the user's identity when they are trying to access their account or files with specified permissions. In general, there a are four ways of authentication:

- **Something the user knows**, such as a password or PIN which the user gets when creating their account. This assumes that only the user knows their respective password or PIN.
- **Something the user has**, such as a smartcard or token which the user gets when creating the account. This assumes that only the user has his smartcard or token.
- **Something the user is**, such as fingerprint, voice or retina. This means the user uses his body to identify himself.
- **Where the user is**, such as inside or outside a building. This means the authentication can make use of a location to be sure that only users that are inside a building have access to the system.

A system which has different implemented access rights, needs an authentication method to make sure, the access rights are not violated. This way the system can restrict the access to sensible or valuable information to the designated users.

This means that, regarding the current project, every coordinator receives a set of access rights. These rights define which kind of crisis is attributed to which kind of coordinator. A more complicated crisis requires a more experienced coordinator. This way the system can handle crisis a much more efficient and effective way.

Variant points: authentication

Variant name: max tries

To login you will need to enter your username and password. These are always required but an additional field is required when the user failed to enter his username OR password three consecutive times (within a timeframe of five minutes each time data is sent).

The system has 5 attributes per account stored: The username, password, email and two additional attributes that the user cannot define for himself, but the system needs them to determine the last authentication try and how many times he tried to authenticate himself in the last five minutes.
So in total there are five attributes that will be saved in the database on the system (server): username, password, email, last access, tries in the five last minutes.

When the user entered his username and password and sends it to the system, the server will calculate the time when the data arrived at the system. If the user did not yet send his data once to the system, the ‘last access’ attribute will be 0 and not evaluated. The attribute will be set to the time when the data packet arrived.
If that was not the case and the user did send his data to the system in the past, the system will evaluate: ‘time right now’ - ‘last access’ = ‘delta difference time’.

So now if ‘delta difference time’ (‘ddt’) is equal or less than five minutes, the attribute field ‘tries’ will be incremented by one. The system will check if ‘tries’ attribute is greater or equal to three and if it returns to be true, the system will send a new login field that requires the user to also sent an additional information that is the ‘captcha test’ field.

Also, let’s say the evaluated time difference turns out to be greater than five then the ‘tries’ attribute will be set to one.
And when registering the users first value in the ‘tries’ attribute is set to 0.

When logging in there is also a ‘Reset password’ button. If the user does not remember his password, he can click the button and the system will then ask for the users’ email. If the user enters a valid registered email, the system will send a new password to that email.
If it turns out that that email is not registered at the system, a error message will appear saying that the email does not exist on the systems end.