Bluetooth positioning in the Flowscape system

Conditions,

To be able to gain a position in Flowscape's system, several things are required.

- You have downloaded Flowscapes mobile app.
- You have connected to a Flowscape server.
- You have Bluetooth enabled on your device.
- You have logged in to this server, been approved as a user, and approved the customer-designed consent notification.
- You are in the customer's premises where Beacons connected to this customer are installed.

If all the above is met, then the mobile device sends position data to the Flowscape server, this position is stored in runtime.

This position can then be used for GPS-style wayfinding in the office.

If the user has made himself "visible" (opt in) the position will be shared on the map, and you will be searchable for position.

Description of the BLE subsystem

We (Flowscape) starts the Senion SDK on the mobile device by specifying a MapKey, a key that points out which building positioning is to be calculated and an API key (unique, secret, each customer has their own).

When the SDK is first launched, it calls Senion Clouds (located in Amazon AWS in Ireland) with Map Key and API Key. There is a check that the API key is allowed to download data for that particular Map Key. If ok, a radio map is downloaded to the phone. The radio map is not a geographical map but a map that contains what beacons are in the building and what signal strength they have in different locations.

If the phone is in the building and hears some beacons, a position is calculated (longitude, latitude and floor). This is where the Radio Map is used. This position is handed over to the Flowscape application. We **do not** send this position to the positioning cloud!

However, we send two kinds of data to our (Senion) cloud:

Session data - we send out an anonymous message that someone has started positioning in this building. The ID is anonymous and random and cannot be traced to the phone. The data contains the type of telephone used and the time.

The session data is used to improve the service, we see how many people use the system and which phone types are most common.

Beacon status data: When a beacon sends out its message, which the phone intercepts, it also sends includes battery status. This battery status is then sent in the background up to our cloud, also anonymously, we do not see who reported it. The battery status is used to monitor beacon health, if it is time to change the battery, etc.

All communications are encrypted.

Customers have access to the Beacon Management portal. The user authenticates himself with the username and password that a Senion employee has set up and linked to a specific customer. A user can only see the beacon status of the buildings it is linked to with the current customer ID.

The separation is thus done on the customer ID.

If the user comes to another building using positioning for another customer nothing happens as the SDK has not been able to calculate any position and then it is completely silent.