



EXPOApp3

Deliverable D2.2

8 June 2020

Project Acronym	Grant Agreement #	Project title
ATHLETE	874583	Advancing Tools for Human Early Lifecourse Exposome Research and Translation

Nature	Dissemination level	Leading institution
Websites, patents filling, etc.	Public	Bettair

DELIVERABLE REFERENCE NUMBER AND TITLE	D 2.2 EXPOApp3 REVISION: V01
LEADING BENEFICIARY	Bettair
NATURE	Websites, patents filling, etc.
DISSEMINATION LEVEL	Public

AUTHORS

LEONARDO SANTIAGO
Bettair Cities

ADRIAN RODRIGUEZ
Bettair Cities

JOSE MANUEL SABIN
Bettair Cities

REVISION HISTORY

REVISION	DATE	AUTHOR	ORGANISATION	DESCRIPTION
V.1	17.06.2020	JM. Sabin A. Rodriguez L. Santiago	BETTAIR	<i>First release of document to be shared with the coordinator</i>

Contents

1 EXPOApp3 and EXPOHub	5
1.1 Security and Privacy of the Platform	6
2 Designing EXPOApp3 and EXPOHub	7
2.1 EXPOApp3 Mock-up.....	8
2.2 EXPOHub Mock-up.....	9
3 Implementation of EXPOApp3 and EXPOHub	13
3.1 Expo HUB.....	15
3.1.1 Registering in the web platform as a new organization	15
3.1.2 Add users to an organization.	15
3.1.3 Recover Account Password.....	16
3.1.4 Configure Experiments	16
3.1.5 Modifying the legal advice.....	18
3.1.6 Share experiments deep links	19
3.1.7 Experiment Status	21
3.1.8 Experiment Groups.....	22
3.1.9 Searching Experiments	22
3.2 Using EXPOApp3 Mobile app	24
3.2.1 Handle device boot events	25
3.2.2 Handle Android save battery mode (Doze)	25
3.2.3 Using EXPOApp3 on Xiaomi devices running MIUI	26
3.2.4 Use of mobile data.	27
3.2.5 Update experiment start and finish date	28
4 Consult and Download Data	28
Annex I: EXPOApp3 Validation Test	32
Annex II: Validated devices	34
Annex III Security Analysis	35
1 Security Analysis	35
1.1 Privacy Protection.....	35
1.2 Secure Connection.....	36
1.3 Secure Local Storage	37
1.4 Third-party Services	39

List of Acronyms

Acronyms	Description
AES	Advanced Encryption Standard is a symmetric encryption technique
CA	Certificate authority
GDPR	General data protection regulation
ISRG	Internet Security Research Group
JSON	JavaScript object notation
OTP	One-time password
RAM	Random access memory
RSA	Rivest-Shamir-Adleman is an asymmetric encryption technique
PEP	Police Enforcement Point

1 EXPOApp3 and EXPOHub

The main objective of Task 2.3 is to develop a smartphone app that will be part of a bigger data collection tool that includes data from wearable and indoor monitoring devices to record personal exposure data in adolescent cohort follow-ups and intervention studies, including air pollution, light, physical activity, sleep, location.

The SME Bettair Cities is in charge of the development of EXPOApp3 and its software platform (EXPOHub) to collect the data from the subject's smartphones for the duration of the studies.

The app will monitor, in real-time

- Location (GPS).
- Accelerometer (ACC)
- Physical activity (calculated from the device accelerometer data).
- Screen (ON/OFF)

EXPOApp3 and EXPOHub are expected to be commercialised to institutions carrying out similar studies that require the data collection of location and physical activity in a centralised manner from a smartphone as data source. The combination of remote data collection and centralised data processing and analysis is a must in this kind of studies where the raw datasets are too large to handle by research institutions. The business behind EXPOApp3 and EXPOHub is very scalable for future use (e.g. in citizen science) and Bettair Cities is capable of offering international services from Barcelona.

EXPOApp3, is an updated version of the former EXPOApp (and EXPOApp2), developed in the EXPOsOMICs and HELIX projects. This new version will be used in the ATHLETE project and will transmit data automatically to a server platform (EXPOHub), also developed by Bettair and running on ISGlobal servers, in which the data can be extracted and analysed by the research institutions conducting the experiments. This approach makes the data available in nearly real time and also reduces the workload for researchers. As mentioned before, the app will record real-time location and physical activity levels of the subject, which will be used to improve exposure estimates for ambient exposures and the external exposome (task 2.4). The new app EXPOApp3 will be applied in the entire new HELIX subcohort follow up and in the urban intervention studies of WP7.

As the app collects data that can be identified as personal data (user location), the following principles have been when processing personal data: lawfulness, fairness and transparency; purpose limitation; data minimization (necessary and proportionate for the research objective); accuracy; storage limitation and integrity and confidentiality. General procedures to be included in the research protocol to safeguard the privacy of study subjects:

- Written (and digital) consent will be obtained from all the participants in the study to use their personal data. Consent forms include a specific clause on personal data protection informing the study participants how their data is going to be treated and stored, the research purpose, the DPO contact and their rights.
- Pseudonymization will be implemented as a general standard, meaning that all sensitive or non-sensitive personal data obtained in the framework of the project will be identified through a unique identifier, the name and/or other personal data that could allow the identification of the participant will never be indicated. This unique identifier will link all basic data required for the study. The master key file linking the centre's study numbers with personal identifiers will be maintained in a password protected file with limited access.

Whenever possible, anonymization will be applied.

- All files containing personal data will be stored in encrypted and password-locked files. Access to these files will be limited to authorized project personnel;
- In the case of tracking participants by geo-localization techniques, the geo-localization data will be store separately from the other participant's personal data.
- Personal data will not be transferred, except in the cases considered by law.
- All project personnel will be trained in the importance of confidentiality of individual records and required to sign a confidentiality agreement.

1.1 Security and Privacy of the Platform

The EXPOHub has the Identity Manager modules developed by FIWARE¹ to manage the authentication of users through the OAuth 2.0 framework and the encryption of all sensitive customer information. And the PEP Proxy module also created by FIWARE to manage the authorization of access to data through the implementation of policies under the OASIS XACML 3.0 standard.

In addition, all connections between users and the platform are made over HTTPS. The security of the storage unit is assured by encryption at different levels.

- The first basic encryption is computer volume encryption: the volumes storing data are encrypted using OS level tools, such as encrypted LVM, protecting data from physical access.
- The second layer of security is added in network communications.
- All data transferred between nodes of the cluster or between nodes and clients is ciphered using industry standard SSL technology (Certificate 2048 bits).
- Finally, only computers (employees with access for development and testing) connected via a VPN can access the platform. Each user has a specific file generated to access the VPN and connect to the platform services.

¹ FIWARE is an open source initiative defining a universal set of standards for context data management which facilitate the development of Smart Solutions for different domains such as Smart Cities, Smart Industry, Smart Agri-food, and Smart Energy.

2 Designing EXPOApp3 and EXPOHub

The first step was to define the requirements and user experience for the EXPOApp3 platform. To accomplish this task, a list of user stories for EXPOHub (institutions carrying a study) and EXPOApp3 (volunteer subjects) users was created. The user stories are listed below.

R1.- As a user of the EXPOHub platform I want to be able to create an organization with my work team where only we have access to the data collected by our cohort(s).

R2.- As a user of the EXPOHub platform, I want to be able to invite other users (within my organization) to join our organization.

R3.- As an EXPOHub user, I want to be able to configure batches of experiments with the same setup (start date, end date, sampling rate of data).

R4.- As an EXPOHub user, I want to be able to capture the location of the subjects who use the EXPOApp3 application, including the error in the estimation of each measurement.

R5.- As an EXPOHub user, I want to be able to capture the accelerometer sensor record of the ExpoApp application that subjects use on the X, Y, and Z axes.

R6.- As an EXPOHub user, I want to be able to obtain the activity index in METs units from the accelerometer data record of the ExpoApp application.

R7.- As an EXPOHub user, I want to be able to obtain the screen state events log (screen on and off events), and device energy-saving mode events log (doze mode on, off).

R8.- As a user of EXPOHub and EXPOApp3, I want the collected data to be handled safely and deleted from the mobile device once uploaded to EXPOHub.

R9.- As an EXPOApp3 user, I want the use of the mobile app to be performed anonymously and not required to use personal data, or any information that could identify me when authenticating myself in the application.

R10.- As an EXPOApp3 user, I want the captured data to occupy as little storage as possible before being uploaded to the server.

R11.- As an EXPOHub user, I want to be able to modify the start and end finish date of an experiment remotely whenever it is possible.

R12.- As an EXPOHub user, I want to be able to group the experiments in groups to consult their general state (total of experiments started, finished and completed).

R13.- As an EXPOHub user, I want to be able to indicate a legal text to each experiment where the ExpoApp user must accept before he can start it. Since it might be modified, I want to be able to consult which version was agreed.

R14.- As an EXPOHub user, I want to be able to view a summary report of the data collected from each experiment.

R15.- As an EXPOHub user, I want to be able to download the raw data to process it outside the EXPOHub platform.

R16.- As an ExpoApp user, I want to be able to configure the experiment in a simple, safe way and without having to remember to start and stop the experiment on the planned dates.

R17.- As a user of the EXPOHub platform, I want to be able to search for a specific experiment within the platform.

R18.- As an EXPOHub user, I want to be able to recover my account if I have forgotten the password.

From the list of user stories listed above, a series of mockups were designed for the mobile application (ExpoApp) and the web platform (EXPOHub). The design of the app is quite simple, as the user only needs to configure whether the data is being uploaded using mobile data or a Wi-Fi connection.

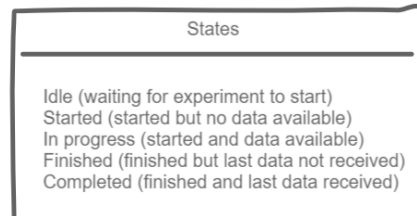
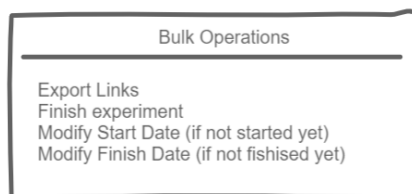
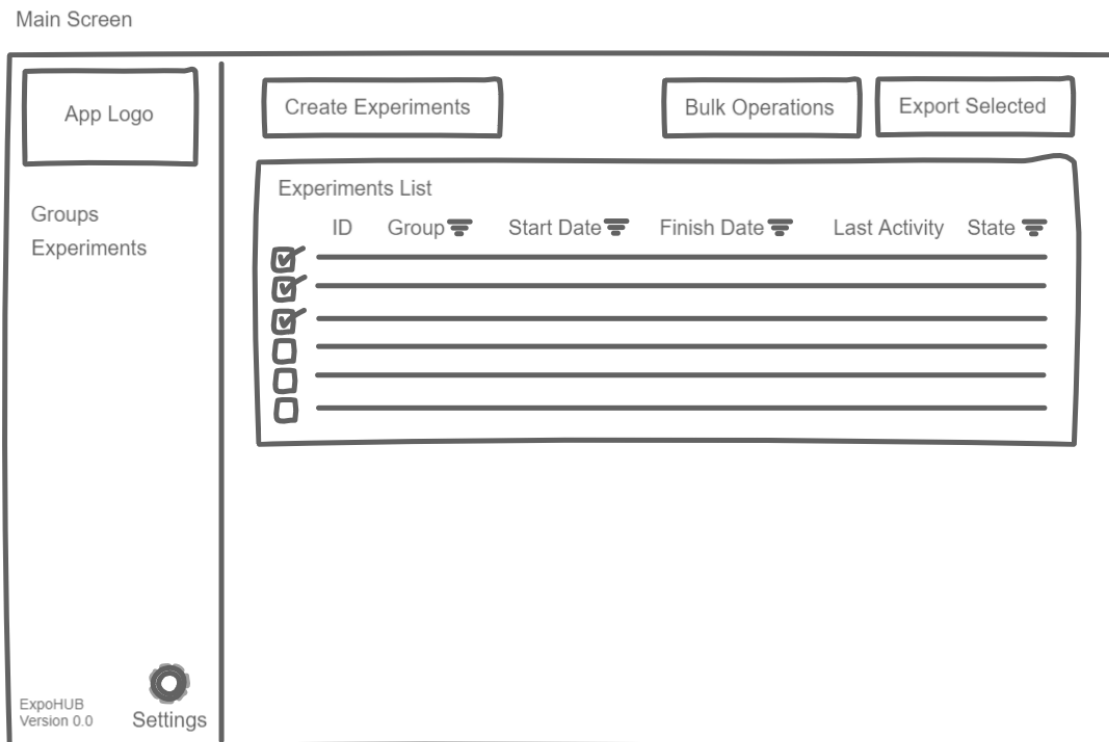
2.1 EXPOApp3 Mock-up

The main screen displays relevant information about the current experiment.



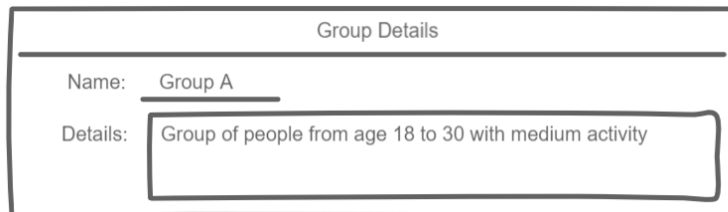
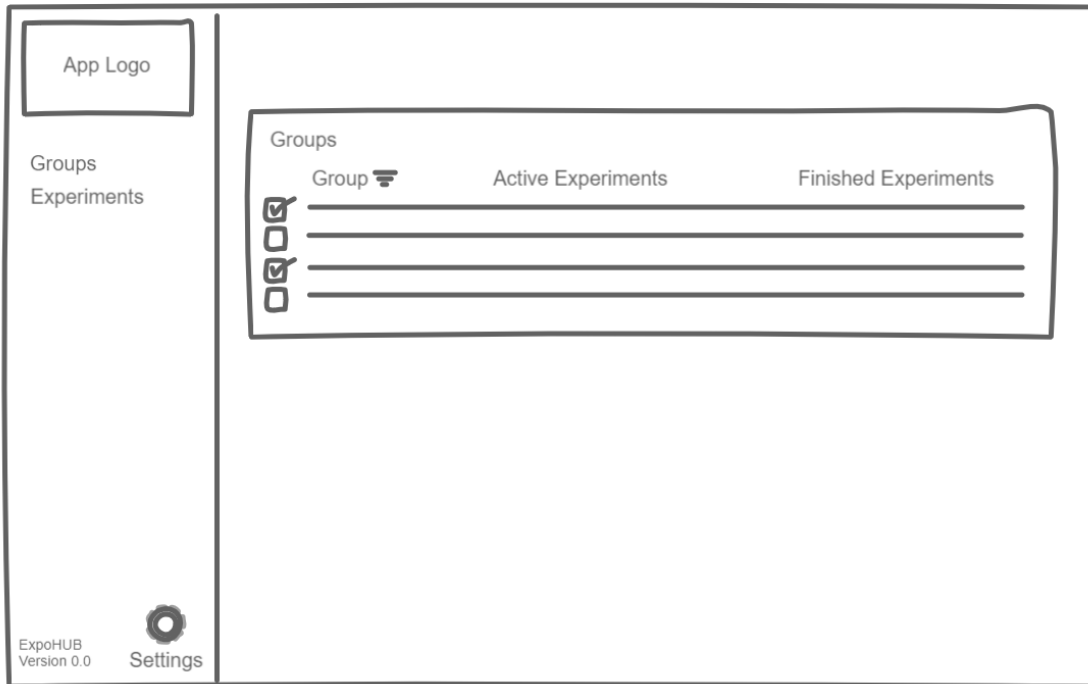
2.2 EXPOHub Mock-up

The main screen of EXPOHub displays the current status of the different experiment. Bulk operations are available to set new “states” to the experiments at any time.



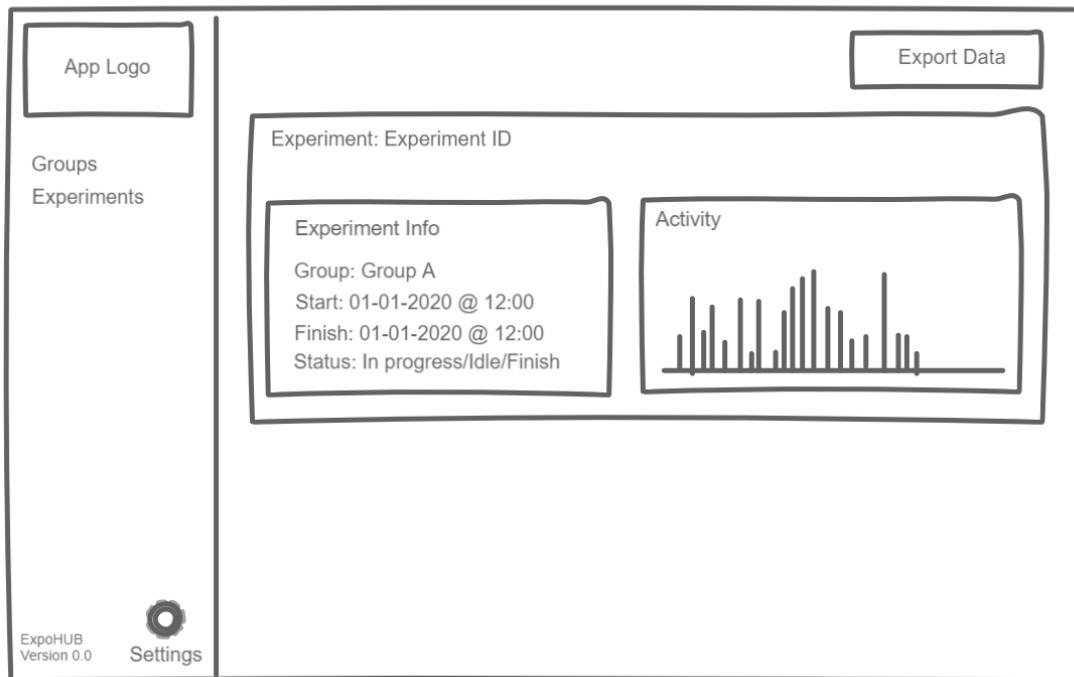
In the group (cohort) screen a list of the different experiment by cohort can be seen, a summary of current active experiments and finished experiments can be seen in this screen.

Group Screen



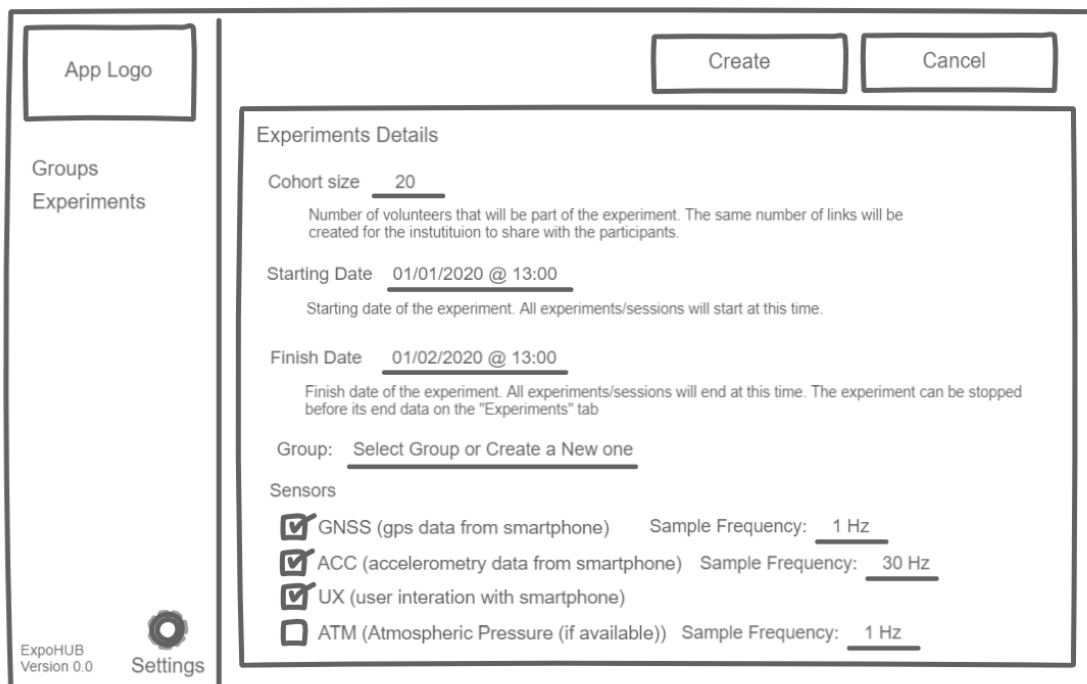
In the Experiment Screen, details of a specific experiment are displayed. In this screen it is possible to export the raw data of the experiment even before it has been finished.

Experiment Screen: Details



Experiments are easy to be created. This screen generates a batch (list) of links to be given to participants to install the app and carry out the measurements. The batch of experiments can be added to an existing group (cohort) or it is possible to create a new group

New Experiments: Create new experiments (links)



A sub screen is a new group (cohort) that need to be created.

New Group

Name:

Details:

3 Implementation of EXPOApp3 and EXPOHub

As mentioned before, EXPOApp3 is a tool created for the ATHLETE project, its main objective is to collect data from subjects (see Table 1) using a mobile device with the Android operating system (Android 6 or higher).

Data	Description
User location	epoch, longitude, latitude and measurement error, with a sampling rate that can reach 1Hz
Accelerometer	epoch, x, y, z axes, with a sampling rate that can reach 30Hz
Activity index	Calculated from the accelerometer data
Screen status	Screen on and off events
Device charging status	Charger connected and disconnected events
Battery saving mode state	Doze mode on and off ²
Firebase Id	Firebase id is required to send push notifications to a specific device. It is used to update the experiment finalization date from the web dashboard.

Table 1 Data collected by EXPOApp3

The application was created considering security and privacy (see Annex III Security Analysis) and designed to facilitate its use by automating the entire process using deep links.

Deep links enable sharing experiment credentials and at the same time allow to install the app if it is not already installed in the device. They can be shared using any communication channel (email, WhatsApp, etc.). Once clicked, the experiment is started using the its metadata (The deep link provides a single-use credential).

At the beginning of the experiment, the user must grant permission to use the location system and consent to a legal agreement configured by each cohort on the web platform (see Figure 1). From this point on, the application automates the rest of the process registering tasks that do not require user interaction (start of data capture, data upload, end of the experiment).

² <https://developer.android.com/training/monitoring-device-state/doze-standby>

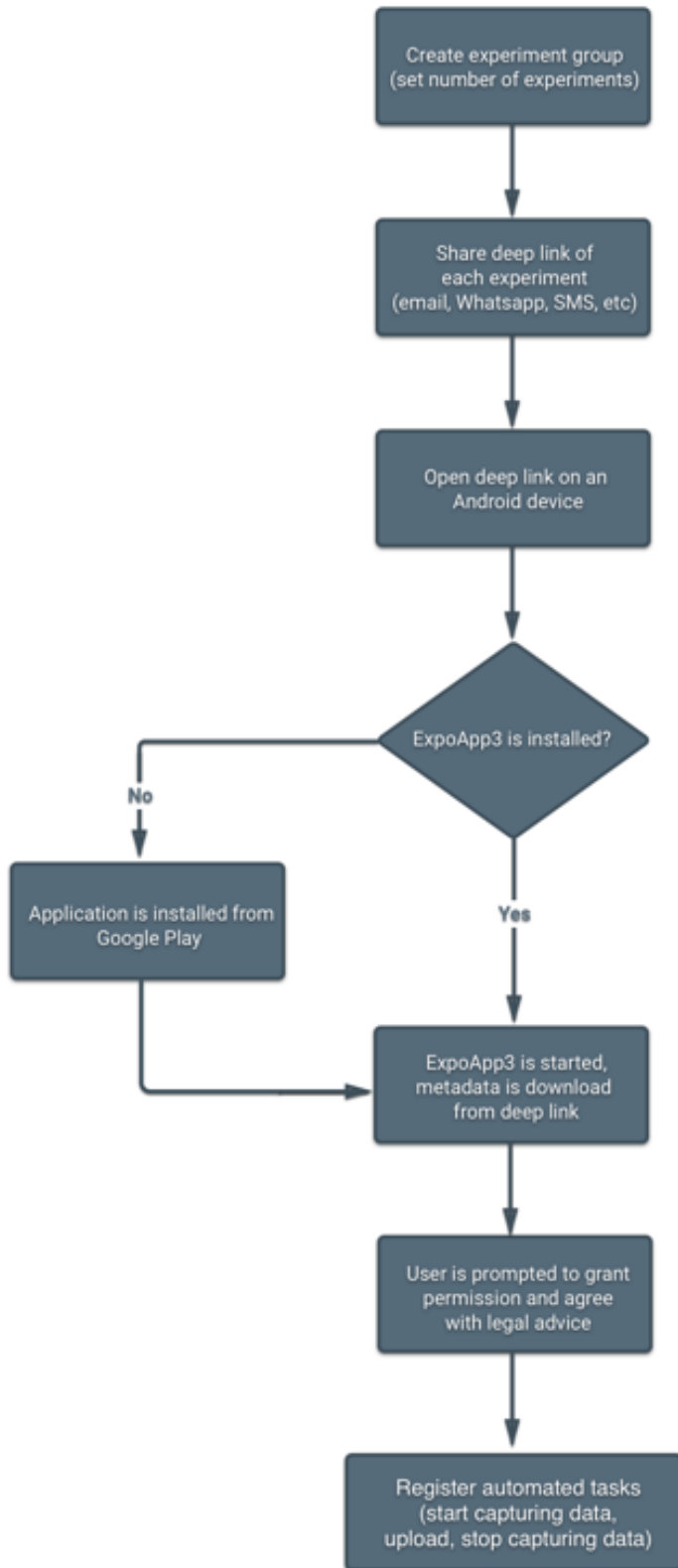


Figure 1 Start an experiment using deep links

Once an experiment is finished its data can be consulted and downloaded from the web platform.

Below is detailed each step for using the EXPOHub latform.

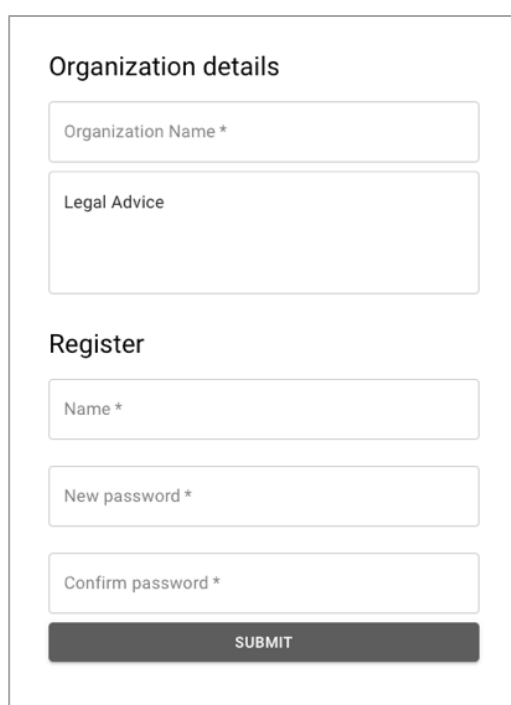
3.1 Expo HUB

The EXPOHub platform is supported by a backend³ service. The implemented front end is as follow:

3.1.1 Registering in the web platform as a new organization

To register on the platform as an organization you must receive a user invitation from a system administrator. Admin invitations allow creating an organization and a user account in the same form. During the registration process, you will have to fill the data shown in Figure 2. Legal advice is not mandatory since it could be modified later. You can find more details of how to update the legal advice at [Modifying the legal advice](#).

Once your account and the organization are created, you can invite other collaborators to join the organization.



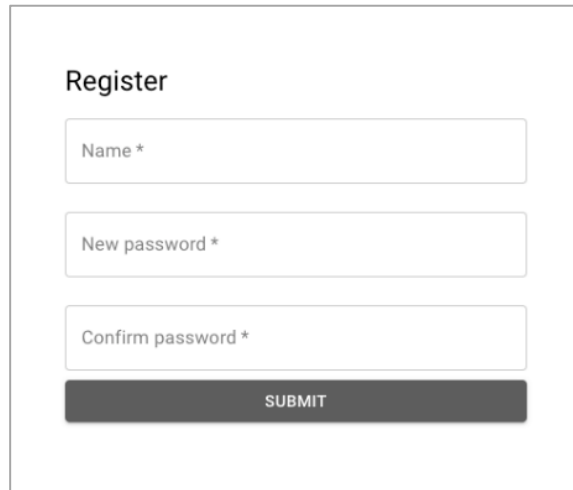
The image shows a registration form with two main sections: 'Organization details' and 'Register'. The 'Organization details' section contains two input fields: 'Organization Name *' and 'Legal Advice'. The 'Register' section contains three input fields: 'Name *', 'New password *', and 'Confirm password *'. Below these fields is a dark grey 'SUBMIT' button.

Figure 2 Organization and user register form

3.1.2 Add users to an organization.

Any user can send invitations to join an organization. To send an invitation you have to press the invite button in the organization section, a pop-up will show up prompting the receiver's email address (example of registration form in Figure 3). This email cannot be associated with another user or any organization.

³ The documentation about the API can be found here <https://EXPOHub.docs.apiary.io/>

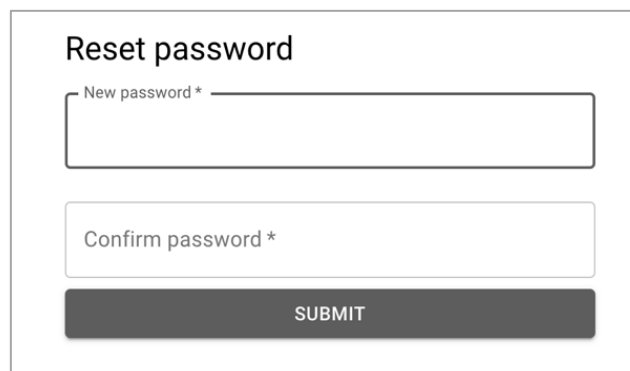


The image shows a registration form titled "Register". It contains three input fields: "Name *", "New password *", and "Confirm password *". Below the fields is a dark grey button labeled "SUBMIT".

Figure 3 User register form

3.1.3 Recover Account Password

It is possible to recover your account by pressing the forgot password button and typing the email associated with it. You will receive an email that contains a link where you can enter your new password (see Figure 4).



The image shows a password reset form titled "Reset password". It contains two input fields: "New password *" and "Confirm password *". Below the fields is a dark grey button labeled "SUBMIT".

Figure 4 Change password form

3.1.4 Configure Experiments

The EXPOHub web dashboard supports creating multiple experiments at the same time. Such experiments must be associated with a group (It is possible to associate as many batches of experiments with the same group).

Each experiment of the batch has a composed name, the prefix common for every experiment of the batch, followed by the index. Besides the name, every experiment has a unique identifier associated with it. So, there is no problem if different groups have created experiments with the same prefix.

To create experiments, you have to access the experiment section on the Dashboard sidebar and then press the create experiment button.

Once there (see Figure 5) you need to fill the parameters described in Table 2 and press the create button.

CREATE CANCEL

Experiments Details

Prefix of experiments *
Prefix to be used to create the names of the experiments followed by a number.

Number Experiments *
Number of volunteers that will be part of the experiment. The same number of links will be created for the institution to share with the participants.

Start Date
2020/06/08 12:14

Starting date of the experiment. All experiments/sessions will start at this time.

Finish Date
2020/06/08 12:14

Finish date of the experiment. All experiments/sessions will end at this time. The experiment can be stopped before on the "Experiments" tab.

Select a Group ▼

Sensors:

GNSS (gps data from smartphone)	<u>Smample Frequency *</u>	<u>1</u> Hz
ACC (accelerometry data from smartphone)	<u>Smample Frequency *</u>	<u>30</u> Hz
UX (user interaction with smartphone)		

Figure 5 Configure experiments form

Parameter	Description
Prefix	Combined with the experiment index represents the visible name of each experiment. For example, if we create an experiment with prefix "experiment_" and indicate the number of experiments as 3, the following experiments will be created: "experiment_1", "experiment_2", "experiment_3"
Number of experiments	Indicates the total number of experiments to create with this setup
Start date and Finish date.	Represents the date and time where all experiments created in this batch should start and finish.
Group	This is a mandatory field. All experiments must belong to a group. You can select or create a group in the dropdown menu.
GPS and ACC sample frequency	These values represent the sampling rate used by the EXPOApp3 mobile application. By default, they are configured with the ATHLETE project setup.

Table 2 Experiments parameters description

If the experiments are successfully created, a pop-up window will be shown where you can copy each experiment link to share using your favourite channel.

3.1.5 Modifying the legal advice

All experiments must provide a legal advice message which the subject must accept to start an experiment.

This legal text is indicated when creating an organization account, however, it can be modified by pressing the legal edit button under the organization section (see Figure 6).

Given the possibility of modifying, the platform will record which version of the legal text has been accepted when starting each experiment.

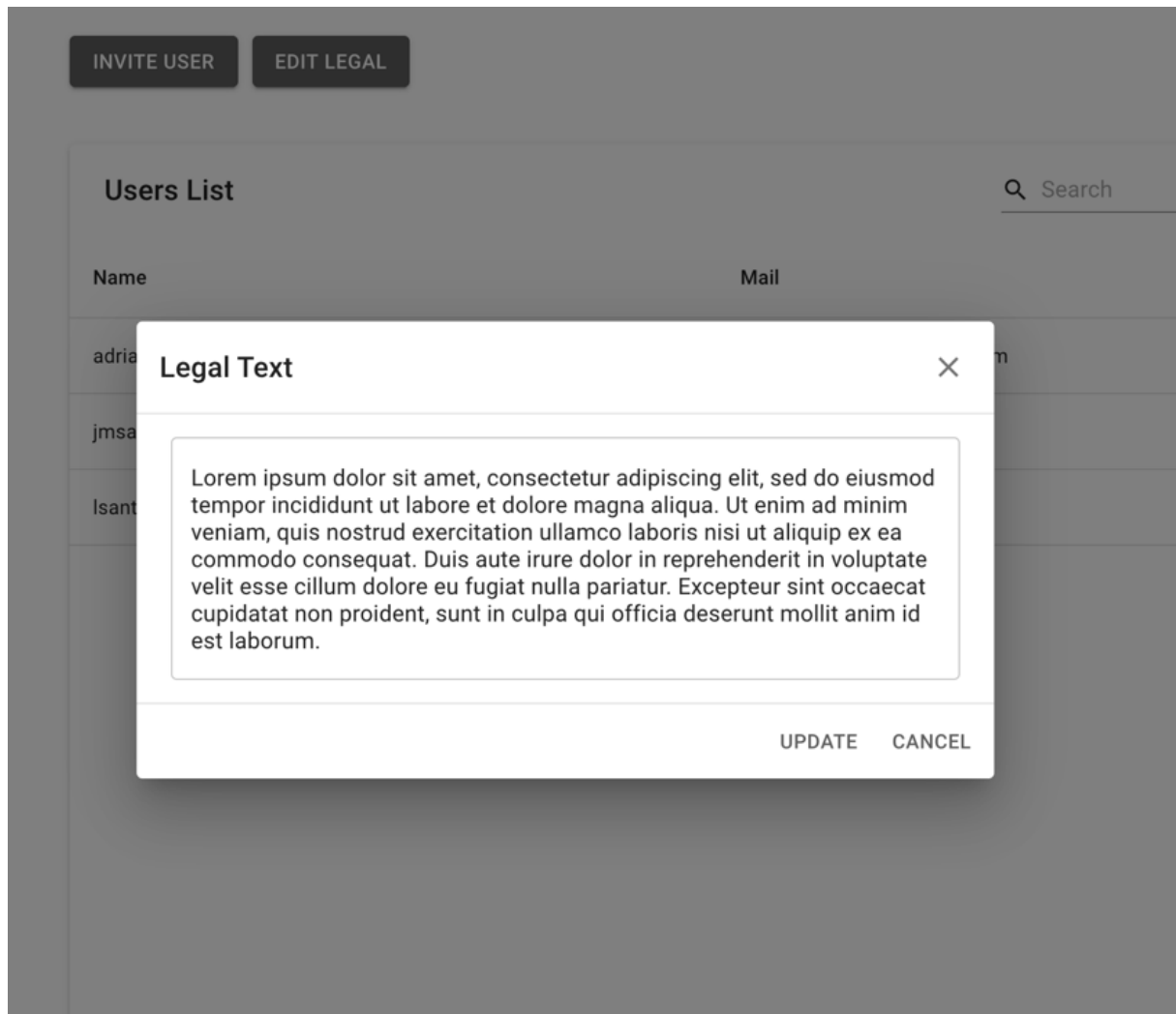


Figure 6 Legal advice modification form

3.1.6 Share experiments deep links

Once the experiments have been created, it is possible to share with the subjects by copying each link from the pop-up screen and paste it in your preferred communication channel (email, WhatsApp Web, etc.).

If you close the pop-up screen and want to consult the links once again you will need to go to the experiments section, select the experiments you need and press the bulk operations button, finally, select export links in the dropdown menu (see Figure 7). A pop-up window will display the links where they can be individually copied to the click board by clicking each one (see Figure 8).

CREATE EXPERIMENT

EXPORT SELECTED

3 row(s) selected

ID	Group	Start Date	Finished Date	Last Activity	State
ExportLink1	jmsabin	08/06/2020, 10:58:00	16/06/2020, 10:58:40	Idle	Idle
ExportLink2	jmsabin	08/06/2020, 10:58:00	16/06/2020, 10:58:40	Idle	Idle
ExportLink3	jmsabin	08/06/2020, 10:58:00	16/06/2020, 10:58:40	Idle	Idle

Export Links
Finish experiment
Modify Start Date
Modify Finish Date

Figure 7 Consulting experiments links

CREATE EXPERIMENT

BULK OPERATIONS

3 r

Experiments Created

Experiment: ExportLink1
https://expoapp3.app.link/QGdpDUEpm7

Experiment: ExportLink2
https://expoapp3.app.link/GDCrzUEpm7

Experiment: ExportLink3
https://expoapp3.app.link/UYJUfwApm7

FINISH

State
Idle
Idle

08/06/2020, 16/06/2020,

Figure 8 List of experiments link

3.1.7 Experiment Status

Once you create and share your experiment you can monitor its state in the experiment section.

Below is presented a table with all possible states.

State	Description
Idle	This status occurs when an experiment has been configured but has not yet been initialized on a mobile device.
Started	The started status is displayed when the subject has registered (started the app with the link) the experiment, but the start date has not been reached.
In Progress	In Progress indicates that the experiment has been registered and is within the experiment period.
Finished	Once the end date is reached, the status change to finished (the experiment must be started). However, the mobile device may not yet have sent all the stored data.
Completed	The completed status indicates that the device has sent all the data it had stored. Once the mobile application sends all the data, it notifies the platform that the experiment has been completed.

Table 3. Experiment states description

It is important to wait for the completed status in the web dashboard before starting a new experiment on the same device.

In addition to the state of the experiment, there is another column that indicates the last contact of the mobile application with the server. Both columns give you information about the behaviour of the mobile device and the experiment stage.

3.1.8 Experiment Groups

The group's section (see Figure 9) allows visualizing the general status of a group of experiments. In Table 4 Groups column description is described the information displayed in this section.

Groups				
Name	Active Experiments	Completed Experiments	Total Experiments	Actions
test group	2	0	2	
ACC_Experiment	10	18	40	
jmsabin	3	19	28	

Figure 9 Groups section of web dashboard

Column	Description
Name	Represents the name to which one or more batches of experiments belongs
Active experiments	Represent the total number of experiments with state Idle, started, or in Progress.
Completed experiments	Represent the total number of experiments with state completed.
Total experiments	Indicates the total number of experiments created that are associated with this group.
Actions	Allows to see the detail of the current group.

Table 4 Groups column description

You can determine the number of finished experiments by subtracting completed and active experiments from the total number of experiments.

3.1.9 Searching Experiments

The experiment section (see Figure 10) includes a search field that enables you to filter the experiments by name or by the group to which it belongs. You can also sort the experiments by pressing the title of each column, facilitating the search for a specific experiment.

CREATE EXPERIMENT BULK OPERATIONS EXPORT SELECTED

Experiment List Q jmsabin X

<input type="checkbox"/>	ID	Group	Start Date	Finished Date	Last Activity	State	
<input type="checkbox"/>	change start date1	jmsabin	29/05/2020, 06:00:00	30/05/2020, 00:00:00	Idle	Idle	 i 🛡️
<input type="checkbox"/>	Test1 schedule start and finish1	jmsabin	28/05/2020, 11:05:00	28/05/2020, 11:35:00	28/05/2020, 11:34:55	Completed	 i 🛡️

Figure 10 Searching for an experiment in the web dashboard

3.2 Using EXPOApp3 Mobile app

When participants receive a deep link, they will be able to start the experiment by just clicking on it. If the application is not installed, it will be downloaded automatically from Google Play (see Figure 11). Once it is installed, the experiment will be started using the deep link metadata.

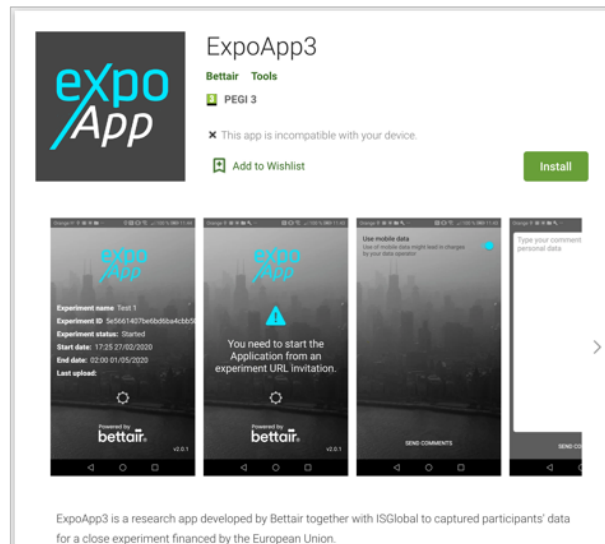


Figure 11 EXPOApp3 Google play app description

Before starting the experiment, the user will be prompted to grant permission to use the device's location system, disable the energy-saving mode (Doze mode) and finally accept the data consent indicated when configuring the experiment in the Dashboard (see Figure 12).

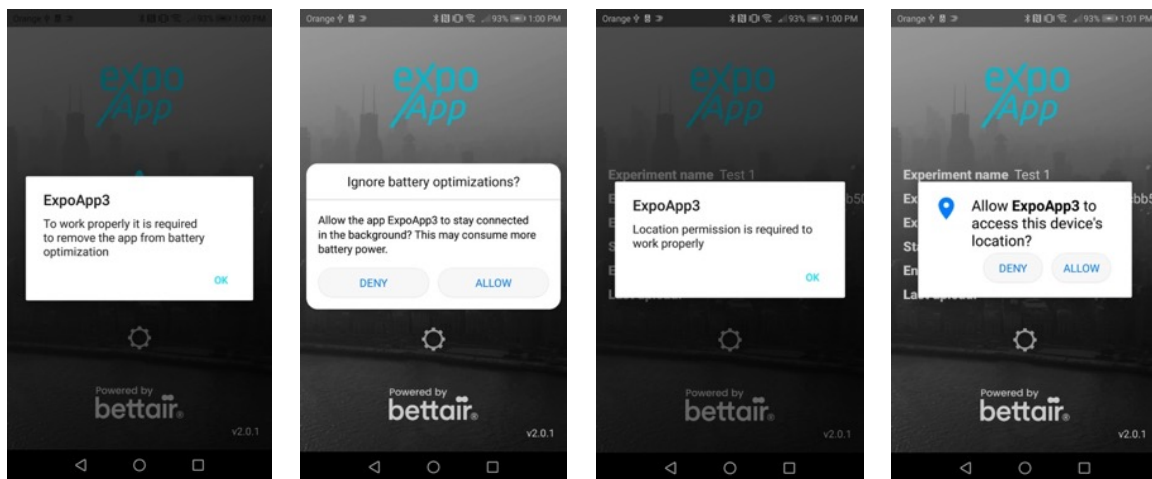


Figure 12 EXPOApp3 pop-ups prompt user to grant use permissions

After the experiment is successfully initiated, it is displayed a screen with its information (see Figure 13). A relevant indicator is the state of the experiment. This indicator might hold three states, programmed, started, and finished.

The programmed state occurs when the start date of the experiment has not been reached, in this scenario, the application schedules a task to start collecting data without any user interaction.

Just like the data collection automation, the application will take care of finalizing the experiment automatically upon reaching the finalization date.

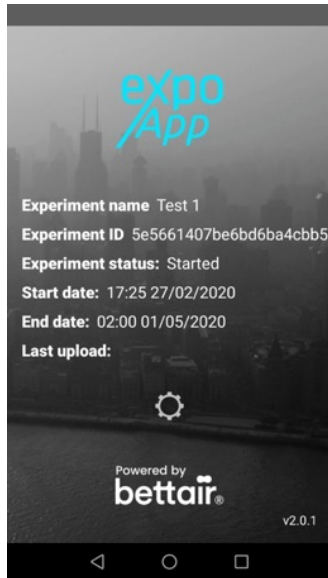


Figure 13 EXPOApp3 home screen after starting an experiment

3.2.1 Handle device boot events

EXPOApp3 is designed to be restarted automatically if an experiment was previously running at the time the device is started. This operation might require that the user unlock the device because of operating system security measures. Once started it will continue capturing data, or finalize the experiment if the finalizing date was reached.

3.2.2 Handle Android save battery mode (Doze)

Since Android 6, it was implemented an energy-saving mechanism that limits the functionality and execution of mobile applications. This mechanism is activated after a certain period elapsed without detecting any movement of the device (using the device accelerometer).

When an experiment is started, EXPOApp3 prompts the user to exclude the application from this battery saving mode, however, certain restrictions still apply as detailed in the official Android documentation⁴.

These limitations affect the device's location system and the implementation of data synchronization mechanism.

It could be assumed that by not detecting any movement of the device and entering the energy-saving mode, the device does not change its location, However, this affirmation will not always be true. An example of this could be traveling in public transport with the device in a bag and there are no sudden changes in acceleration.

Fortunately, the saving mechanism is designed to open small windows (maintenance window) of approximately 1 minute where the location system is enabled, these maintenance windows become more spaced as the device remains longer in the doze mode (see

Figure 14).

⁴ more detail about doze mode in <https://developer.android.com/training/monitoring-device-state/doze-standby>

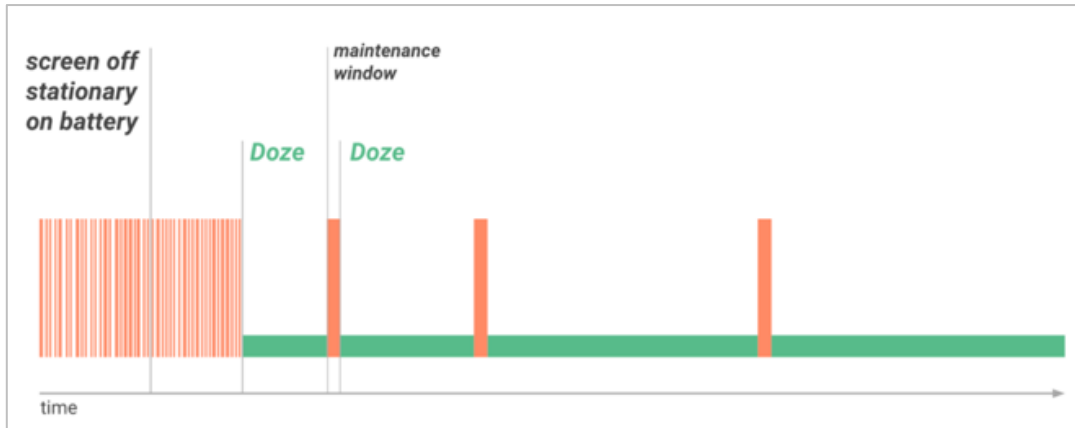


Figure 14 Doze mode diagram from Google Play official documentation

Because of the inevitable impact of this mechanism on the resulting data, the application tracks the doze mode events to contrast them with the location data in the data analysis process.

As far as data synchronization is concerned it does not represent a major issue since the data is stored locally and the synchronization is restored when exiting power-saving mode.

Besides the Android native energy saving mechanism, given the open-source nature of Android, each manufacturer can implement its energy-saving mechanisms. Such is the case of the Huawei devices, which integrates an application (com.huawei.powergenie) that closes other apps that are in the white list of energy savings mode⁵.

Therefore, the performance of the app cannot be guaranteed on all Android devices, and it is recommended to use any of the validated devices listed in Table 7.

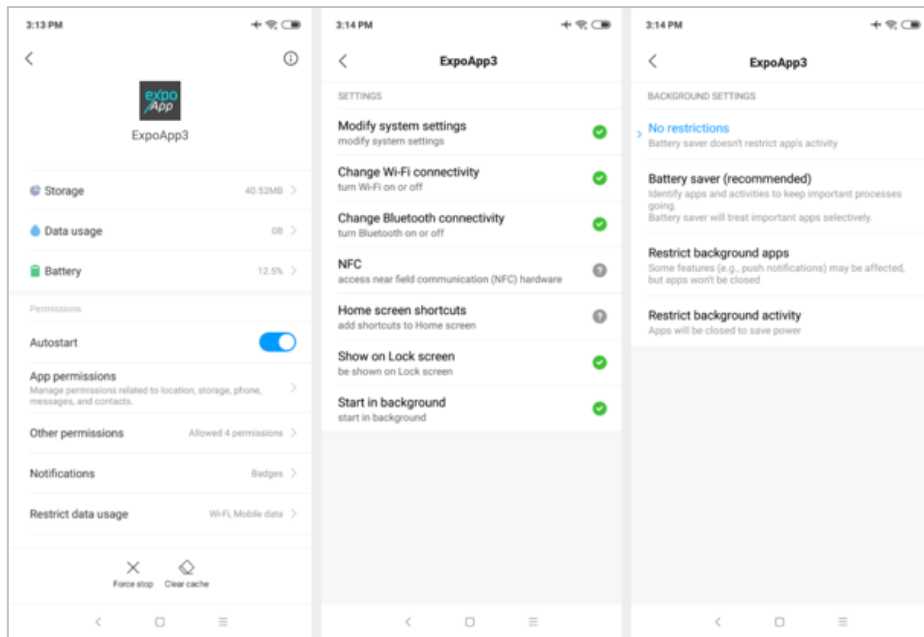
3.2.3 Using EXPOApp3 on Xiaomi devices running MIUI

To run EXPOApp3 on Xiaomi devices with MIUI operating system (based on Android). The application must be installed manually (do not download through the deep link) from Google Play through the following link

<https://play.google.com/store/apps/details?id=com.bettaircities.EXPOApp3>

After installing the application, permissions must be granted manually in the device configuration menu, as shown in image XX.

⁵ For more details, you can visit <https://dontkillmyapp.com/>



Once the permissions have been configured, the experiment can be started by pressing the deep link as described in previous steps⁶.

3.2.4 Use of mobile data.

The use of mobile data may have a monetary cost to the user. For this reason, it has been implemented a configuration option to only upload data when a Wi-Fi connection with internet access is available.

To access the configuration menu (see Figure 15), press the configuration button (engine icon) on the home screen of the application (see Figure 13).



Figure 15 EXPOApp3 configuration screen

⁶ You can find solutions for other devices at [dontkillmyapp](http://dontkillmyapp.com) web site.

3.2.5 Update experiment start and finish date

It is possible to modify the finish date of an experiment right from the web dashboard as long as the current end date has not been reached. In the case of the start date it is possible to update it if the experiment state is in idle or started value. These changes are communicated to the corresponding device through a push notification (in case of a started state). However, the application does not provide feedback when the push has been received, in some scenarios where the devices have not internet connection the experiment may last longer than indicated on the new end date or start after the indicated date.

To update the start or finish date, you have to select the experiments to be updated and press the bulk operation button from the dashboard. Then select change start/finish date option from the dropdown menu (see Figure 16) and pick a date using the date picker view. Finally press the ok button.

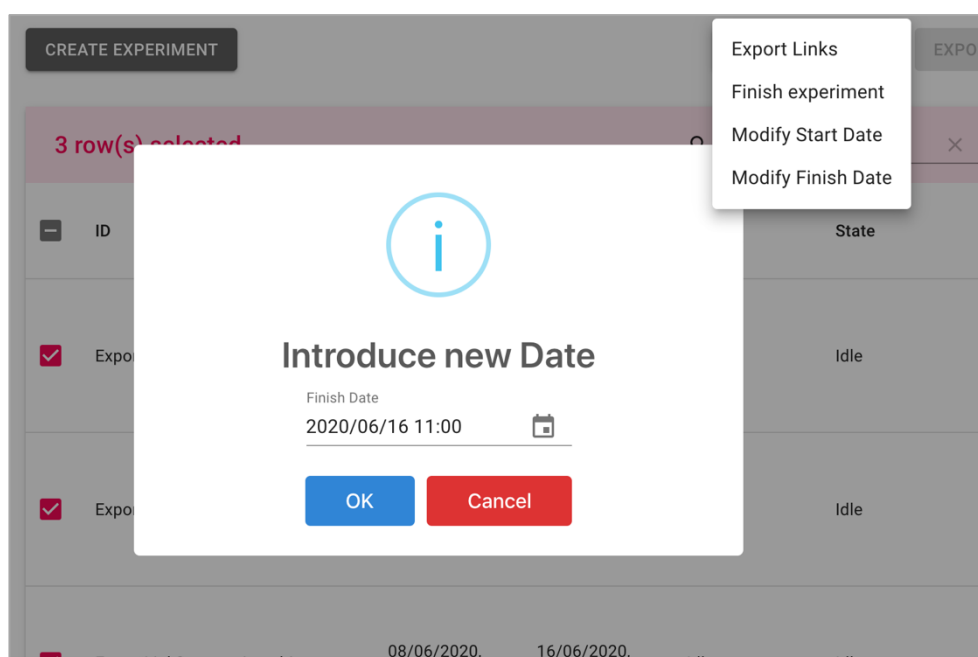


Figure 16 Change experiment finish date view

4 Consult and Download Data

Once the experiment is In Progress status, you will be able to download the raw data by selecting the desired experiments in the experiment section and pressing the export selected button. This action will generate a zip file with a bunch of CSV file described in Table 5.

File	Format
Location	Unix epoch, latitude, longitude, accuracy (meters)
Acceleration	Unix epoch, X (m/s ²), Y (m/s ²), Z (m/s ²)
Activity index	Unix epoch, vertical activity index (METs), horizontal activity index (METs)
UI events	Unix epoch, event name (SCREEN ON/OFF, DOZE MODE ON/OFF, CHARGING ON/OFF)

Table 5 Raw data files format description

In addition to the raw data, you can consult a report on the quality of the data, this will include the data described in Table 6

Data	Description
GPS chart	<p>This graph (see Figure 17) shows the quality of the GPS signal. It details the minutes per hour of the GPS signal distributed in 3 ranges according to the magnitude of the signal error. The first range is made of signals with less than 10 meters of error, the second with errors ranging from 20 to 30 meters, and the last range of measurements with more than 30 meters of error.</p> <p>In addition to the GPS data, the chart displays the minutes per hour that the device has been in Doze mode (energy saving state without GPS signal) and the periods where the device has not captured any type of data during the course of the experiment (the device was turned off or was application closed).</p>
Minutes of GPS signal table	<p>This table (see Figure 18) describes with numbers the information on the previous GPS chart. In it, you can see the number of minutes with GPS data for each hour of the experiment.</p>
Empirical threshold for wearing time	<p>This information allows us to determine the empirical threshold of the activity index where the user is wearing the device (see Figure 19).</p>
Wearing hours per day applying the empirical threshold	<p>Estimated hours of use per day applying threshold (Q3) obtained from the empirical threshold described above.</p>
Activity index plots	<p>This graph shows the activity index values (METs) on the vertical and horizontal axis per day (see Figure 20).</p>

Table 6 Experiment summary report

GPS Report

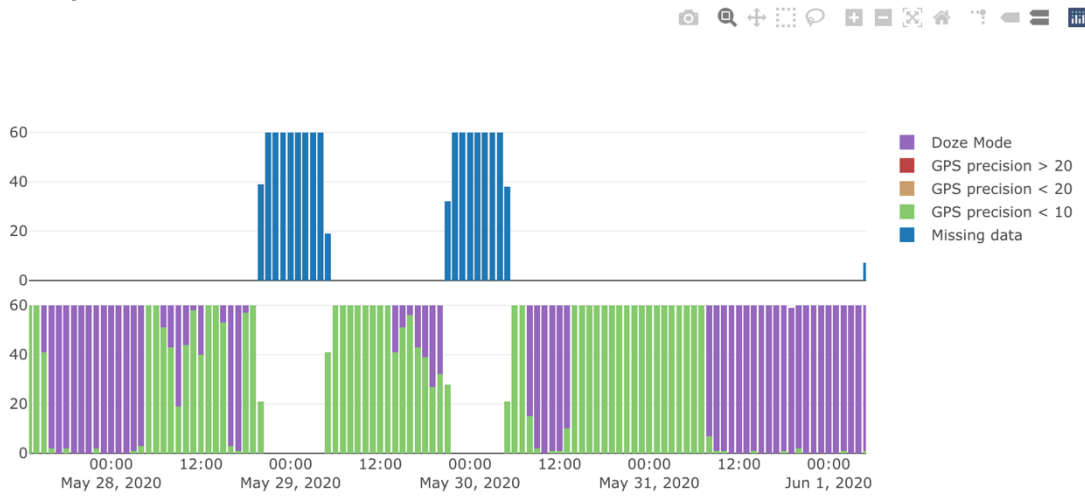


Figure 17 GPS data summary report

GPS Minutes Report

Date	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
27/5	-	-	-	-	-	-	-	-	-	-	-	-	21	60	60	41	2	0	2	0	0	0	2	0
28/5	0	0	0	1	3	60	60	51	43	19	44	58	40	60	60	53	3	1	57	60	21	0	0	0
29/5	0	0	0	0	0	41	60	60	60	60	60	60	60	60	41	51	56	43	39	27	32	28	0	0
30/5	0	0	0	0	0	21	60	60	15	2	0	1	1	10	60	60	60	60	60	60	60	60	60	60
31/5	60	60	60	60	60	60	60	60	7	1	1	0	0	0	1	0	0	0	1	0	2	0	0	0
1/6	0	0	1	0	0	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

Figure 18 GPS minutes of data per hour report

Wearing Time



Empirical threshold for wearing time

Min	Q1	Median	Mean	Q3	Max
0.00208	0.00365	0.00421	0.00814	0.00487	3.43048

Wearing hours per day applying the threshold Q3

Date	Hours
2020-5-27	0:23:08
2020-5-28	0:48:41
2020-5-29	1:31:57
2020-5-30	1:50:33
2020-5-31	1:59:22
2020-6-1	0:35:04
2020-6-2	0:19:06
2020-6-4	0:00:04

Figure 19 Wearing empirical threshold and wearing hours per day

Activity Report

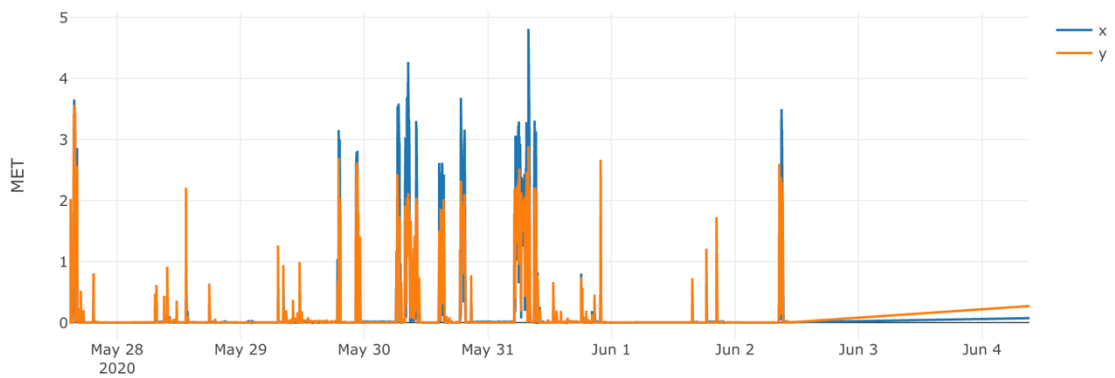


Figure 20 Activity report

Annex I: EXPOApp3 Validation Test

Below is described a list of tests that were carried out to validate the ExpoApp performance.

Result	Name	Device state	Validating
OK	Test 1 schedule start and finish1	App in background, activity killed	Schedule start date
			Schedule finish date
OK	Test 2 schedule start and finish doze mode	Doze mode	Schedule start date in doze mode
			Schedule finish date in doze mode
OK	Test 3 schedule finish not internet connection retries 1 time	Device with not internet connection when finish time is reached. It lost internet connection at 28/05/2020, 12:46:00 and recover connection at 28/05/2020, 12:48:00 Device retry after every 15min	Finish experiment no internet scenario retry once
OK	Test 4 schedule finish not internet connection retries twice	Device with not internet connection when finish time is reached. It lost internet connection at 28/05/2020, 13:16:00 and recover connection at 28/05/2020, 13:39:00 Device retry twice	Finish experiment no internet scenario retry twice
OK	Test 5 schedule start and finish after device restart	Device restarted after the experiment start date was first scheduled	Schedule start date after restart
			Schedule finish date after restart
OK	Test 6 continue experiment after device restarted	Device restarted, and turn on again after start date reached (restarted at 28/05/2020, 14:58:00)	Continue experiment after restart
OK	Test 7 device finish experiment after device restart	Device restarted, experiment finish date reached. (device turned off at 28/05/2020, 15:25:00 and turn on at 28/05/2020, 15:29:00)	Finish experiment after restart
OK	Test 8 change start and finish date	App in background, activity killed	Change start and end date in normal device normal state
OK	Test 9 change start and call finish in doze mode	Device in doze mode	Change start and call end date in device doze mode
OK	Test 10 change finish date in doze mode	Device in doze mode	Change finish date in device doze mode

OK	Test 11 change start date after reboot to a future date	Device just restarted receive a change start date push to a future date	Change start date to a future date after reboot device
OK	Test 12 change start date after reboot to a past date	Device just restarted receive a change start date push to a past date	Change start date to a past date after reboot device
OK	Test 13 change finish date after reboot to a future date	Device just restarted receive a change finish date push to a future date	Change finish date to a future date after reboot device
OK	Test 14 change finish date after reboot to a past date	Device just restarted receive a change finish date push to a past date	Change finish date to a past date after reboot device

Annex II: Validated devices

Below is a list of devices where the correct operation of the application has been validated by carry out the test described in Annex I: EXPOApp3 Validation Test.

Brand	Model	Operating system
Samsung	Galaxy Tab A 2019	Android 9
Samsung	Galaxy A20e	Android 9
Samsung	Galaxy 9	Android 9
Samsung	Galaxy 10	Android 9
Xiaomi	Pocophone F1	Android 10

Table 7 Validated devices using EXPOApp3

Annex III Security Analysis

1 Security Analysis

1.1 Privacy Protection

To protect the identity of users, EXPOApp3 manages the experiments by creating anonymous credentials with random identifiers and one-time passwords (OTP) generated by a cryptographically strong random string generator library. They are automatically created after setting the number of participants of each cohort. With the use of random credentials, it is unnecessary to use emails or identifiable nicknames that might in some way compromise the user's identity.

These credentials are individual use only, once the experiment has started with a specific credential, this one is disabled so that it cannot be used on another device.

To facilitate starting the experiment, a deep link⁷ service has been implemented (Branch), it allows to download the application if it has not been previously installed on the device and automatically initialize the experiment by extracting the credentials from the metadata of the deep link (see Figure 1).

⁷ Deep linking is when a link sends users directly into a specific point in the app experience, rather than an external website or app homepage.

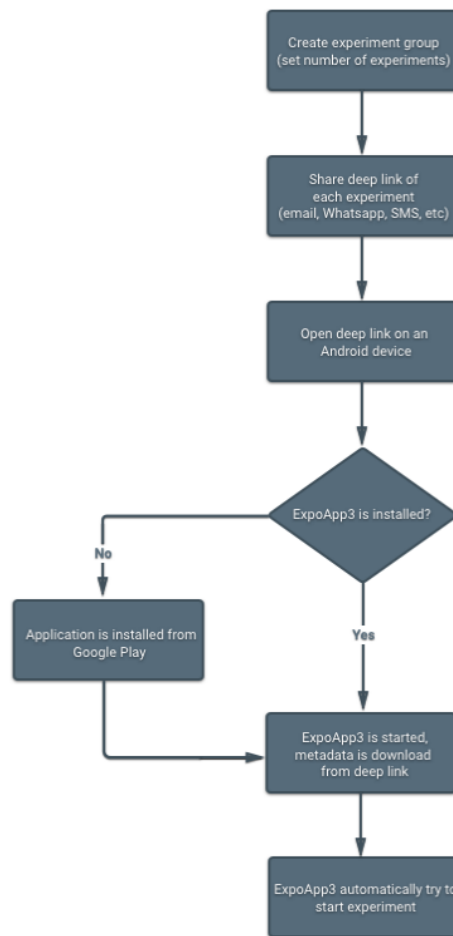


Figure 21 Start experiment using deep links

1.2 Secure Connection

The connection with the cloud platform uses a secure communication channel thanks to the HTTPS protocol and a digital certificate generated with *Let's Encrypt* with a 4096-key size and self-renewed every three months.

Let's Encrypt is a free, automated, and open certificate authority (CA), run for the public's benefit. It is a service provided by the Internet Security Research Group (ISRG).

Let's Encrypt gives people the digital certificates they need in order to enable HTTPS (SSL/TLS) for websites, for free, in the most user-friendly way. They do this because they want to create a more secure and privacy-respecting Web.

Besides the secure channel, each request made to the cloud platform requires a session token that expires after 24 hours. This token should be refreshed using a refresh token (see Figure 22). This mechanism prevents the identity of the user from being supplanted.

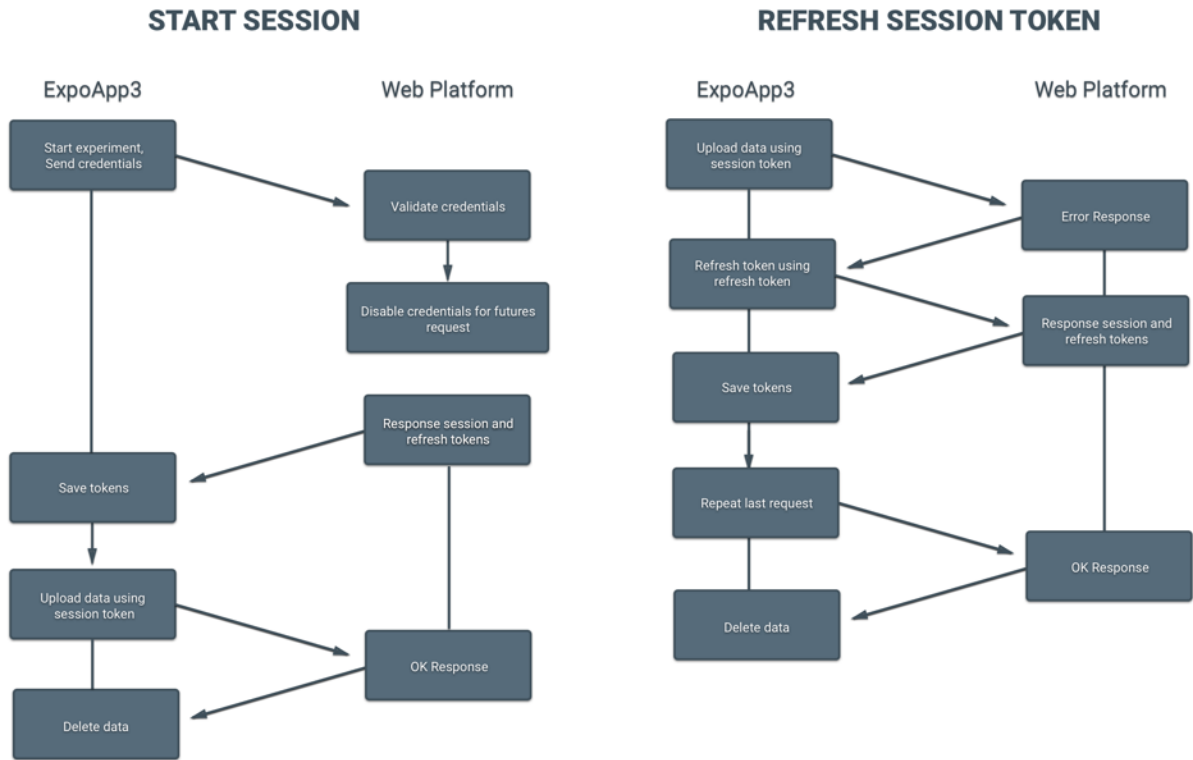


Figure 22 Start session and refresh session flowchart

1.3 Secure Local Storage

EXPOApp's main function is to collect data from the device's sensors (Table 8 Data collected by EXPOApp3) and send it to the cloud platform for further analysis.

This data is temporarily stored on the device and once it is synchronized with the cloud platform, it is deleted from it.

Below is described the data collected by the application

Data	Description
User location	epoch, longitude, latitude and measurement error, with a sampling rate that can reach 1Hz
Accelerometer	epoch, x, y, z axes, with a sampling rate that can reach 30Hz
Activity index	Calculated from the accelerometer data
Screen status	Screen on and off events
Device charging status	Charger connected and disconnected events
Battery saving mode state	Doze mode on and off ⁸
Firebase Id	Firebase id is required to send push notifications to a specific device. It is used to update the experiment finalization date from the web dashboard.

Table 8 Data collected by EXPOApp3

⁸ <https://developer.android.com/training/monitoring-device-state/doze-standby>

For security reasons, the collected data is stored in files located in the application's directory. This directory is not accessible directly from the filesystem, and it requires technical knowledge to access them, providing security in case of loss or theft of the device.

Nevertheless, since the user's location is sensitive data, extra security measures were applied and are described below:

- 1.- A public key is downloaded from the server when starting the experiment and stored on the device.
- 2.- A key and an initialization vector are created locally to perform symmetric encryption (using AES/CBC/PKCS5 Padding algorithm) keeping both in RAM memory⁹.
- 3.- The key from step 2 is encrypted together with the initialization vector using the public key downloaded from the cloud platform from step 1.
- 4.- Location data is stored in files with a ".csv" extension with a maximum of 1 minute of data (60 location samples)¹⁰.
- 5.- Once the file size limit has been reached, they are compressed into a zip file and the original file with the extension ".csv" is deleted.
- 6.- The compressed file is encrypted using the key and the initialization vector from step 2 to obtain a file with the extension ".aes". Once encrypted, the original zipped file is deleted.
- 7.- The path of the encrypted files and the result of encrypting the key and the initialization vector in the Base64 format are stored in an SQLite database.
- 8.- When uploading the encrypted files, a JSON object is created using data from step 7 to let the web platform know which key should use for each file decryption. Once the JSON and the files are uploaded, their local copies are deleted.

* If the application is restarted, a new key is generated for AES encryption (step 2).

The steps described above are detailed in Figure 23.

⁹ Keeping the key and initialization vector in the RAM is a security measure itself since it is a volatile memory and it is quite difficult to extract information from it

¹⁰ One minute of data prevent the encryption to be broken by finding patterns when using small message size. In AES, the repeated use of the same key on similar information can cause patterns to appear. This packet size allows the use of AES / CBC instead of AES / ECB increasing the robustness of the algorithm. https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation

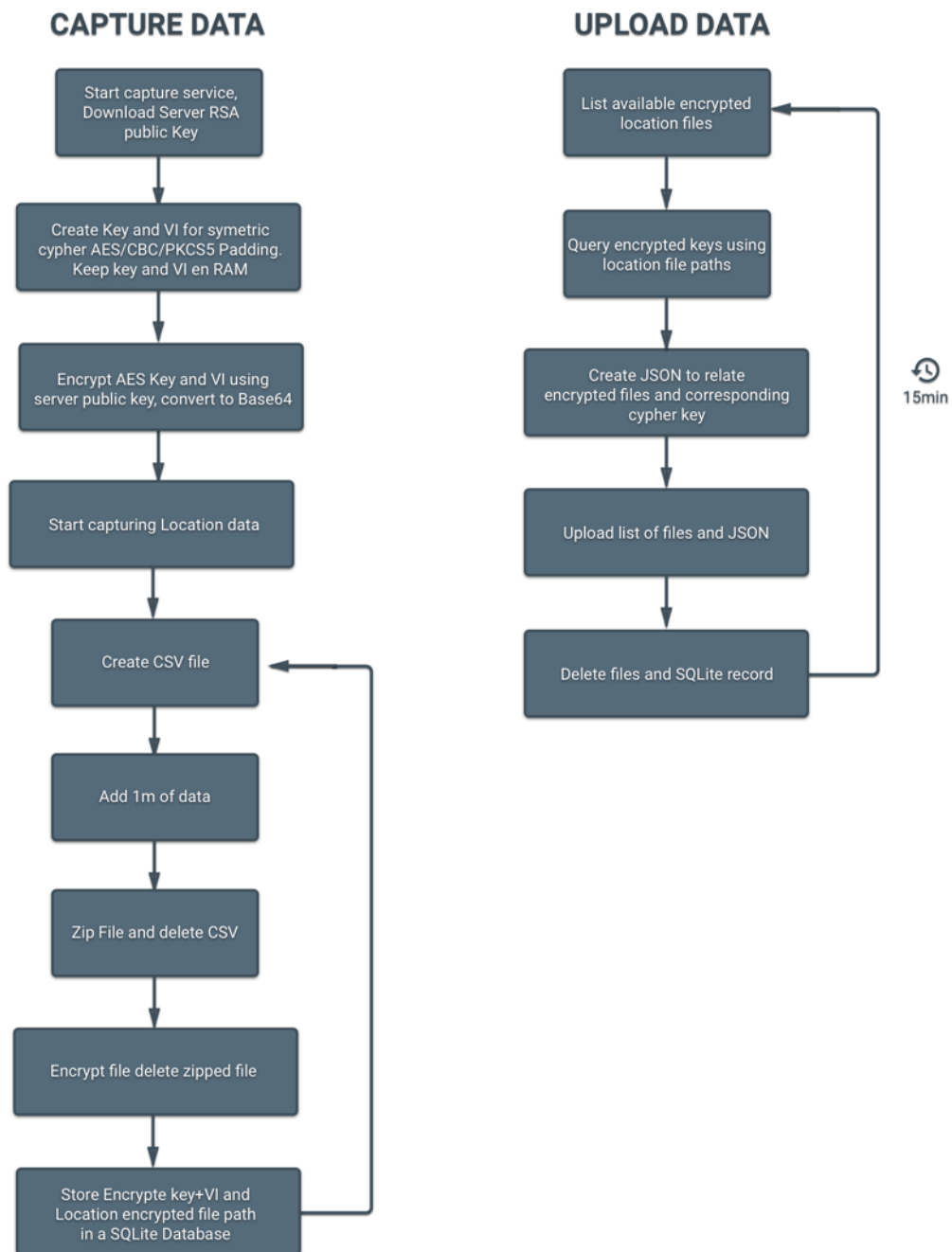


Figure 23 Encrypt data mechanism flowchart

1.4 Third-party Services

Two external services have been implemented in EXPOApp3, Branch, used to implement the login system with deep links and Firebase to send push notifications (Push notifications allow updating the end date of experiments from the Dashboard Of configuration).

Both platforms offer a default user tracking and analytics service which were disabled to protect user privacy^{11, 12}

Below is described the data stored by each service and the reference to the documentation about how to disable to accomplish GDPR

Service	Data collected	Description
Branch	Experiment identifier and password	Branch store deep links with the experiments credentials as metadata
Firebase	Experiment identifier and finalization date	Firebase might temporally store the experiment identifier and finalization date. Once the push is delivered it should be deleted.

Table 9 Data collected by third party services

¹¹ <https://help.branch.io/developers-hub/docs/android-advanced-features>

¹² <https://firebase.google.com/support/guides/disable-analytics>