

EVOTION

727521 – EVOTION

DELIVERABLE No: D5.4

Mobile Application

Authors: Nikos Dimakopoulos, Panagiotis Kokkinakis, Ilias Papas (ATC), Michail Smyrlis, Manolis Stefanakis (EMP).

Dissemination level	
PU	PU - Public



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 727521

Project acronym and GA no	EVOTION- 727521
Project full Title	Evidenced based management of hearing impairments: Public health pOlicy making based on fusing big data analytics and simulaTION.
Project Type	RIA
Start date – end date	01.11.16 – 31.10.19
Website	www.h2020EVOTION.eu
Deliverable type	DEM - <i>NB: Report contains external links for verification of demonstrators, see section 4 and 5</i>
Delivery date	M12 (31 OCT 2017)
Authors:	Nikos Dimakopoulos, Panagiotis Kokkinakis, Ilias Papas, (ATC) Michail Smyrlis, Manolis Stefanakis (EMP). REVIEWERS: Marco Anisetti, Marco Cremonini (UNIMI), George Spanoudakis, Bin Ye (CITY), Louisa Murdin (GST)
Contact:	Nikos Dimakopoulos (n.dimakopoulos@atc.gr)
To be cited as:	Dimakopoulos et al (2017), Mobile Application, Deliverable D5.4 to the EVOTION-727521 Project funded by the European Union, ATC, Greece
Subject and keywords	This report presents the Mobile Application of the EVOTION project. Keywords: mobile application, hearing aids, interface, wearable sensor, android, evotion platform, peripheral devices.
Disclaimer:	This document's contents are not intended to replace consultation of any applicable legal sources or the necessary advice of a legal expert, where appropriate. All information in this document is provided "as is" and no guarantee or warranty is given that the information is fit for any particular purpose. The user, therefore, uses the information at its sole risk and liability. For the avoidance of all doubts, the European Commission has no liability in respect of this document, which is merely representing the authors' view.

Table of Contents

Executive Summary	1
1. Component overview	2
1.1 Mobile Application	2
1.2 Peripheral Devices	3
1.3 EVOTION Platform	3
2 Design	4
2.1 Methodology	4
2.2 Architecture	4
2.3 Security and privacy.....	7
2.3.1 Threats.....	7
2.4 Web services API	8
2.5 UI development.....	9
3 Implementation	11
3.1 Technology	11
3.1.1 Android SDK.....	12
3.1.2 SQLite Database.....	12
3.1.3 Bluetooth API.....	12
3.1.4 Libraries and Dependencies used by application.	12
3.2 Security and privacy.....	13
3.2.1 Security objectives and functionality	14
3.3 Mobile API	15
4 User Manual	18
4.1 Configurator user manual.....	18
4.2 Patient user manual	18
5 Demonstrator	18
6 Conclusion	19
ANNEX 1 – Observation testing steps.....	21
ANNEX 2 – Observation test results	26
ICCS test results	26
OTC test results	34

Table of Figures

Figure 1: Conceptual EVOTION ecosystem of the Mobile Application component	2
Figure 2: Logical architecture diagram of the Mobile Application component	5
Figure 3: Logical architecture diagram of the Mobile Application component	6
Figure 4: UX Wireframe of EVOTION mobile application	10
Figure 5: Menu mockup.....	11
Figure 6: Controls mock-up	11

List of Tables

Table 1: Mobile API.....	8
Table 2: Operations of the EVOTION Mobile Application	16

List of Abbreviations

ATC	ATHENS TECHNOLOGY CENTER SA
BLE	BLUETOOTH LOW ENERGY
CA	Certification Authority
CITY	THE CITY UNIVERSITY LONDON
EDR	EVOTION Data Repository
EHS	EVOTION Hospital System
EMApp	EVOTION Mobile App
EMP	EMPELOR GMBH
ERESL	EVOTION REST Service Layer
GST	Guys St. and Thomas NHS Trust
HA	HEARING AID
HL	HEARING LOSS
LDAP	Lightweight Directory Access Protocol
NHS	National Health System (UK)
NIHL	Noise Induced Hearing Loss
OTC	OTICON A/S
PHPDM	Public health policy decision making models
PTS	Permanent Threshold Shift
PTT	Pure Tone Threshold
TTS	Temporal Threshold Shift
UCL	UNIVERSITY COLLEGE LONDON
UNIMI	UNIVERSITA DEGLI STUDI DI MILANO
PKI	Public Key Interface
SDK	Software Development Kit
UOA	University of Athens

Executive Summary

This document is accompanying the *mobile application component's demonstrator*, as developed within the WP5 work package. This component, which was designed based on the technology and security specifications defined in WP2, and holds a key role in the EVOTION ecosystem as it is the main component for the data gathering process of the EVOTION platform. Furthermore, this component provides an interface for collecting HA user inputs, controlling HAs, recording and providing context data (e.g., HA user location, time, surrounding noise, user activities), collecting data from the wearable sensors and transmitting them to the EVOTION repository.

Please note that the formal deliverable is the demonstrator of the mobile application component, however this document serves the purpose of an extended technical description. The information found herein includes:

- The overview of the prototype Mobile Application component's demonstrator;
- A description including the design and the implementation details of the demonstrator;
- A link to first version of the user manual on how to use the demonstrator, together with some example use cases;
- A link to first version of the user manual on how to configure the mobile application
- A link to the executable (.apk) for the demonstrator;
- A link to a brief video presentation of the demonstrator.

Following on, the next section (section 1), provides a short overview of the component and the components that interacts. Next section (section 2), focuses on the design principles and the security aspects regarding the mobile application component. The methodological development approach is presented and the component architecture together with the offered UI and API is described in detail. Furthermore, in section 3, the security and privacy considerations is described together with the technologies used and the exposed mobile application API. In section 4 links may be found for the User Manual for the users of the mobile application, and the public demonstrators of the prototype may be accessed via the links in section 5.

1. Component overview

The Mobile Application is installed as an Android application inside the mobile device of the patient, is external to the EVOTION platform and communicates remotely with it. It constitutes the access point between the participant enrolled in the clinical trial and the EVOTION platform and it is used to securely collect, store and transmit user inputs, information generated by the Hearing Aids and the Wearable sensor device towards the EVOTION platform. Figure 1 illustrates these inter-relationships. The main key success points that has been taken into consideration during the design and the implementation phase are security, efficiency and robustness.

To that end, the current section will describe the fundamental organization of the mobile application component, including the rest of the components that interacts with, their relationships with each other and principles guidelines for system design and implementation process.

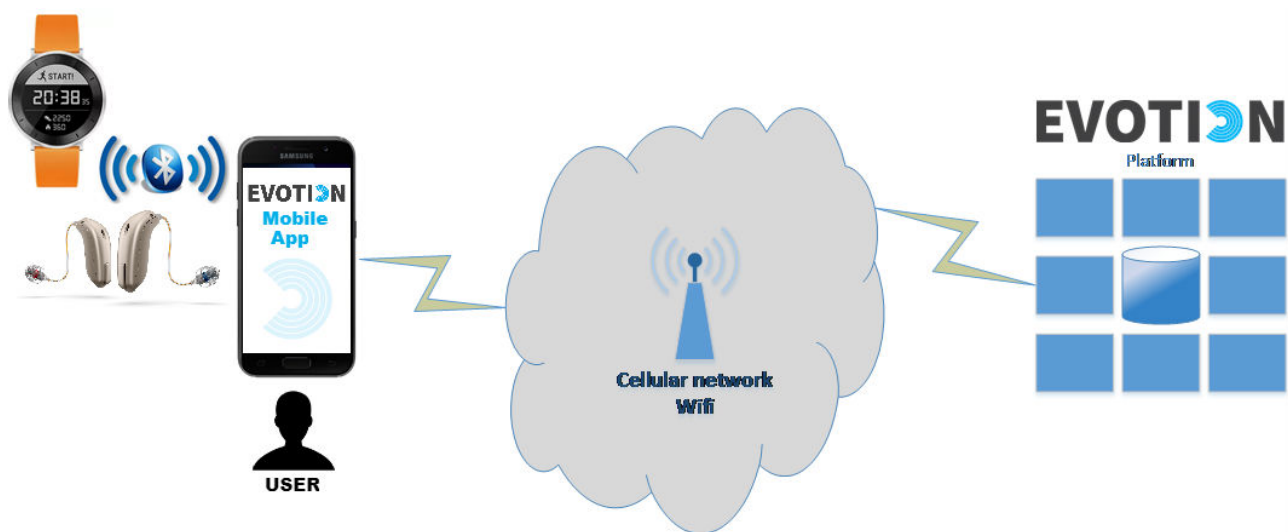


Figure 1: Conceptual EVOTION ecosystem of the Mobile Application component

The Mobile Application component interacts with the peripheral devices, namely the *Wearable Sensor device* and the *Hearing Aids* and with the EVOTION Platform.

1.1 Mobile Application

The EVOTION mobile application is a component aimed at providing a user-friendly graphical user interface for the participant accessing EVOTION's utilities and functionalities. At the same time, the component will handle the communication between the user, the peripheral devices (the HAs and the wearable sensor device) and the mobile device.

Part of the EVOTION mobile application's functionality will be to store sensitive data. All information that is collected by the wearable sensor device will be transmitted and stored by the EVOTION mobile application, before being transferred to the EVOTION platform. All collected information from participants is considered sensitive and should be managed in a secure and private way. Therefore, security and privacy requirements have been analysed since the design phase of the components and mechanisms have been decided and implemented to ensure a secure data storage. All security threats and assumptions related to the mobile device and the communication with peripherals are analysed below (see section 2.3), together with the security objectives that are mentioned in detail in section 3.1.1.

Periodically (once per day), the mobile application transmits to the EVOTION platform all data collected by the HAs and wearable sensor device. These data are collected through the day and stored locally on the mobile device, after being encrypted for security reasons.

Note that the communication channel between the mobile application and the EVOTION platform is not guaranteed to flow through a stable connection, because it could vary based on context-dependent conditions and the network type available to a specific participant (e.g., 2G, 3G, 4G, or Wi-Fi). The battery charge level is the other parameter that could affect a data communication from the mobile application to the EVOTION platform. To that end, the mobile application should constantly monitor the available network type and the battery level before submitting data over the internet. On the other hand, under specific and pre-defined circumstances, the mobile application could decide to communicate data frequently, in order to inform the EVOTION platform that a Temporary Threshold Shift/ Noise-Induced Hearing Loss (TTS/NIHL) event, which is a very peculiar event type that EVOTION aims to measure, is happening to a given participant.

1.2 Peripheral Devices

The peripheral devices consist by the *Hearing Aids* and the *Wearable Sensor device*. The purpose of the Hearing Aids is to enable the collection of sound environment parameters from the patient's everyday life, and the collection of how the patients operate their hearing aids, i.e. program shifts and volume shifts. Moreover, the HAs should also enable measuring the patients' audiogram, and change and suggest program shifts/volume changes in specific settings as well as adapt the default processing according to the collected usage patterns or suggestions from the BDA. The connection between the HAs and the mobile application will be established using Bluetooth Low Energy (BLE) protocol.

The Wearable Sensor device is a specialized device for fitness, health and life style monitoring (smartwatch - Huawei fit) that the participant wears 24/7 capturing various sensor biometric data, like the participant's heart rate. Prior to the biometric data collection, the wearable sensor device will be connected to the participant's mobile device using the EVOTION mobile application (for more information refer to D5.3). The connection between the wearable sensor device and the mobile application will be established using Bluetooth Low Energy (BLE) protocol.

1.3 EVOTION Platform

The EVOTION Platform is an integrated platform supporting evidence based public health policy making related to the management of hearing loss (HL). The platform is to support the acquisition, management and processing of patient medical, physiological, behavioural, hearing aid usage and cognitive activity data to support decision making.

To acquire the data that it is meant to process, the EVOTION platform will interact with external devices and systems. These include the mobile application, as well as medical systems and devices which are used in current clinical practice and support patient testing for the purposes of hearing aid fitting and the process of hearing aid fitting itself.

The EVOTION platform will also incorporate capabilities for big data analytics (e.g., data mining algorithms and statistical analysis, parallel data processing), decision making and simulation to aid the analysis of the data that it will collect and produce evidence that can aid public health policy making. The processes underpinning data analytics and policy making will be model driven. To enable this vision, the EVOTION platform will also incorporate health policy decision making model specification and execution capabilities.

2 Design

2.1 Methodology

For development purposes of the Mobile Application component, the Agile Software Development Practices¹ was followed with frequent development cycles, rapid prototyping and close collaboration between self-organising, cross-functional teams. A defined set of principles guided the development process of the components together with the use of specific tools that fostered this process (like RUP and Spiral). A special part of this process is the Agile testing, which defines that all members of a cross-functional agile team are involved to ensure delivering the business value desired by the customer at frequent intervals, working at a sustainable pace. Furthermore the basis for the implementation was the EVOTION stakeholder requirements (Dimakopoulos et al., 2017), and the outcome, the EVOTION Mobile Application was tested internally by members of the consortium (ICCS and OTC) following a black box testing scenario with the results of the test at ANNEX 2 – Observation test results. It should be noted that the EVOTION mobile application has been tested by using the following set of devices selected for the EVOTION project: Samsung A3 2017 mobile device, Oticon EVOTION Has, and Huawei fit wearable sensor.

Such methodology can decrease the time required to produce releases and engage end users in the development process, maximising the possibilities for a high-quality output. On the other hand, the effectiveness of this methodology is tightly coupled to the proper communication between end users and engineering team, while the lack of specific documentation might put the final acceptance at risk.

2.2 Architecture

This section is dedicated to presenting and analysing the high-level architecture of the EVOTION Mobile Application component. It is focused on illustrating the internal component structure, identifying the subcomponents and their relationships with each other and the communication aspects between the mobile device / application and the peripheral devices (HAs and Wearable Sensor). The description will try to focus on the components layout, their internal architecture as well as the interactions among them.

Figure 2 shows the positions of the Mobile Application component within the overall EVOTION architecture (Ye et al., 2017).

¹ <http://agilemethodology.org/>

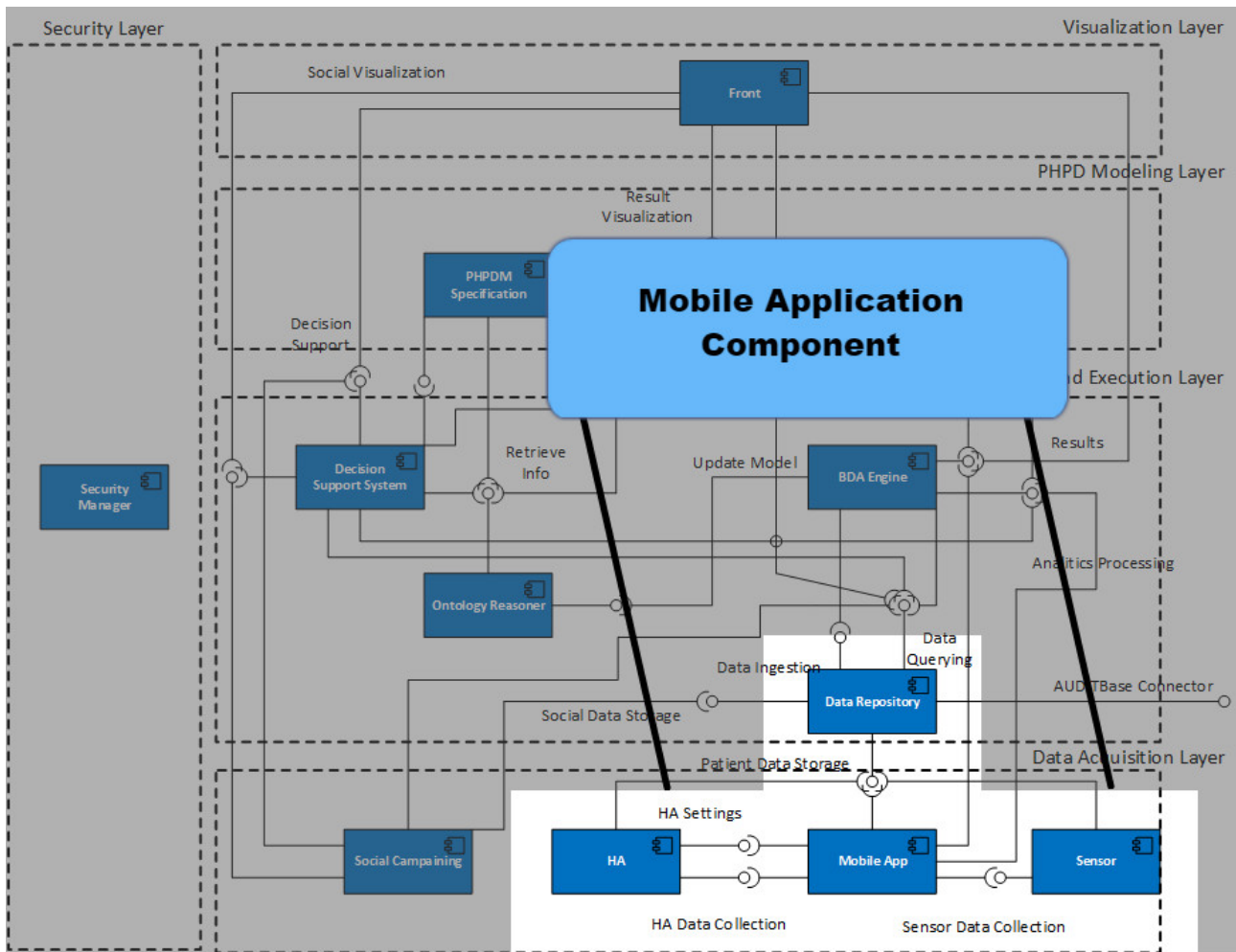


Figure 2: View of Mobile Application component within the EVOTION architecture diagram (Ye et al., 2017)

From Figure 2, it should be noted that the mobile application component is external to the EVOTION Platform - in other words, the mobile application component is part of the EVOTION ecosystem, while the communication channel is not strictly part of it, because it relies on the specific mobile network available to a participant.

As part of the EVOTION platform, the mobile application component consists of the following logical layers (see Figure 2):

- **Mobile application:** The mobile application is a software application that will be implemented in the EVOTION project and will offer an interactive and easy to use graphical user interface. It is aimed to provide the main access point to the EVOTION platform for the participants and, at the same time, to collect, securely store and transmit sensitive information to the EVOTION platform.
- **Hearing Aids and Wearable Sensor:** In the EVOTION project, the mobile device will communicate with peripheral devices, namely the *Hearing Aids* and the *Wearable Sensor device* and collect information. The HAs is to enable the collection of sound environment parameters from the patient's everyday life, and the collection of how the patients operate their hearing aids, i.e. program shifts and volume shifts, while the sensor device is a specialized device for fitness, health and life style monitoring (smartwatch) that measures and makes available biometric data (e.g. participant's heart rate) to the mobile application.

- **EVOTION Platform / Integration Layer:** It facilitates the communication between the Mobile Application and the EVOTION platform, by providing transparency, decoupling and independent scaling/update.

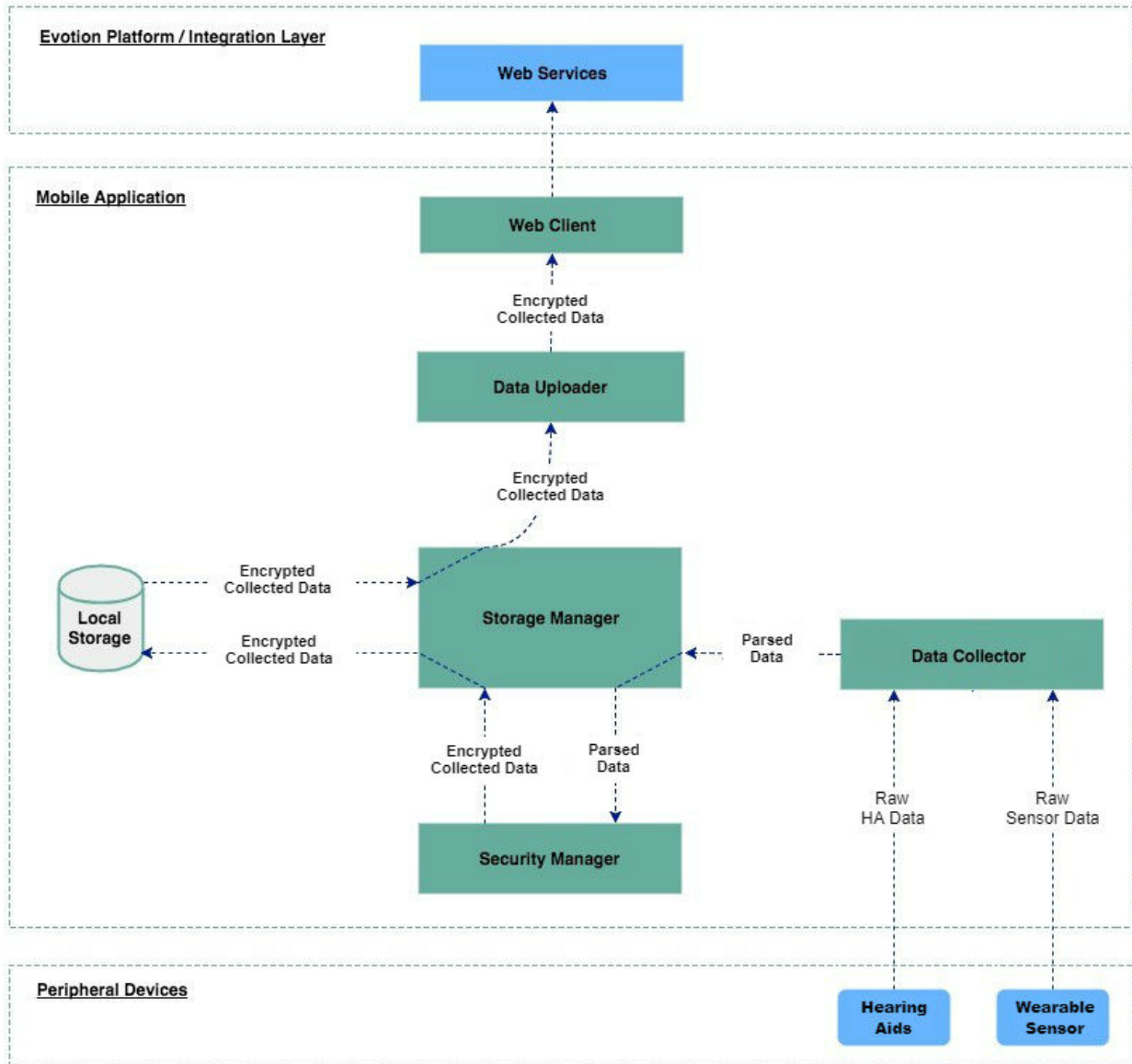


Figure 3: Logical architecture diagram of the Mobile Application component

Internally, the mobile application consists of the following subcomponents (see Figure 3):

- **Data Collector:** It establishes the connection between the mobile application and the peripheral devices. Additionally, it parses the raw binary data that gets from the hearing aids and wearable sensor and passes them to Storage Manager for local storage.
- **Storage Manager:** It encrypts the data (by calling the Security Manager) and saves them in the Local Storage. In addition, it exposes search queries that allow other subcomponents to search for saved data.

- **Security Manager:** It signs and encrypts data, by using symmetric and asymmetric encryptions.
- **Local Storage:** It is a secure local database, since all sensitive data are encrypted before storage.
- **Data Uploader:** It uploads the saved data from the peripheral devices, once an internet connection is available. The frequency has initially been set to once per day, but this will be fine-tuned later based on feedback that will be available during the pilots' execution.
- **Web Client:** It communicates with the Web Services, which are part of the EVOTION Platform Integration Layer. The web client is responsible for establishing a secure connection with the EVOTION platform through which all the collected data will be uploaded.

2.3 Security and privacy

2.3.1 Threats

Mobile devices are subject to threats of traditional computer systems and threats entailed by their mobile nature. The threats considered in this document are those of network eavesdropping, network attacks, physical access, malicious or flawed applications, persistent presence, backup, cloud, biometric impersonation, revocation of biometric credentials, and revocation of biometric template as detailed in the following sections. These threats are described in more detail in the following sub-sections. The ways that the mobile application counters the aforementioned threats will be thoroughly described in section 3.2.

2.3.1.1 T.MALICIOUS_APPS - Malicious or Flawed Application

Malicious or flawed mobile application threats exist because such applications (aka "apps") may include malicious or exploitable code prior to installing them on a mobile device. Malicious or exploitable code can be included unwittingly by its developer, perhaps as part of a software library. Malicious or flawed apps may attempt to exfiltrate data which they have access to. Malicious apps may also attempt to control the device's sensors (geolocation, camera, microphone, etc.) in order to gather intelligence about the user's surroundings even when these activities do not involve data resident or transmitted from the device. Malicious or flawed apps may also give an attacker access to perform network based or physical attacks that otherwise would have been prevented. This threat is labelled as [T.MALICIOUS_APPS].

2.3.1.2 T.NETWORK_ATTACK - Network Attack

An attacker may position himself/herself on a wireless communications channel or elsewhere on a network infrastructure. If an attacker manages to do this successfully, he/she may initiate communication with the mobile device or alter communication between elements of the operating environment and other endpoints. By altering this communication, the attacker may be able to spoof networked components of the EVOTION Platform. This threat is labelled as [T.NETWORK_ATTACK]

2.3.1.3 T.NETWORK_EAVESDROP - Network Eavesdropping

In an analogous manner to the network attack threat, attackers may position themselves on a wireless communications channel or elsewhere on the network infrastructure. The attacker may then monitor or gain access to data being sent or received by the EVOTION mobile app. By monitoring such data, the attacker may intercept not only normal payload data but also security critical metadata including cryptographic keys and human-user authentication data. This threat is labelled as [T.NETWORK_EAVESDROP]

2.3.1.4 T.PHYSICAL Physical Access

The loss or theft of a mobile device may give rise to a physical access threat and through it loss of confidentiality of user data, including, most importantly, user security credentials. Physical access attacks involve attempts to access the device through external hardware ports, through its user interface, or through direct and possible destructive access to its storage media. Such attacks are intended to gain access to data from a lost or stolen mobile device that it is not expected to be returned to its owner. This threat is labelled as [T.PHYSICAL_ACCESS]

Although these attacks are primarily directed against the mobile device, the EVOTION mobile app configures features which address this threat.

2.3.1.5 T.PERSISTENT - Persistent Presence

Persistent presence on a device by an attacker, who is not authorised to be present upon it, implies that the device has lost integrity and cannot regain it. The device has likely lost this integrity due to some other threat vector, yet the continued access by an attacker constitutes an on-going threat. In this case, the device and its data may be controlled by an adversary as well as by its legitimate owner.

2.4 Web services API

As mentioned previously on this document, the mobile application periodically collects data through the peripheral devices as well as environmental data of the mobile device, encrypts them and stores them locally. These data are later uploaded to the data repository of the EVOTION platform via a RESTful API over secure TLS channel that is offered from ERESL (please refer to D5.2 for more information about ERESL). All external calls to this API are routed through the Routing layer path *'/patientstorage'* to the Mobile Engine that offers the following POST operations for uploading data to the Data Repository:

Table 1: Mobile API

Path for data upload	Type of data	Description of data
/upload/audiological_result	List of Audiological Test Results	The results of all the audiological tests the user has taken
/upload/audiometry_record	Timestamped values	HAs tone and speech audiometry
/upload/cognitive_result	List of Cognitive Test Results	The results of all the cognitive tests the user has taken.
/register/device	Serial number and PKI of the mobile device	Data that are stored in LDAP after the successful registration of the device on the EVOTION platform
/upload/environmental_data	Coordinates and set of coordinates	A set of latitude/longitude values showing the user's current location and moving speed. Additionally, a collection of points (lat/lot pairs) showing a user's route.
/upload/haenvironment_data	Environmental data of the Hearing Aids	Volume, Program, Location and sound levels of the HAs

/upload/audiological_data	Audiological data set	Audiological data taken by the user
/upload/hearing_training	Training Data Records	Hearing tests or auditory trainings that are performed by the user
/upload/person_log	User input Text and Date-time	The answers selected by the user through the mobile application. The date and time that the questionnaire was answered. The free-text answer of the user.
/upload/problem_reports	Enumeration and text	Problems of the mobile app or peripheral devices that reported by the users
/upload/user_rating	Rating values	Ratings of the mobile app that are asked from the users
/upload/sensor_data	Timestamped values	Wearable sensor data collected by the mobile app (heart rate)
/upload/episodes	TTS/PTS episode data	Data gathered when PTS/TTS episodes occur to the users. Logged information about audiological data, recorded with the respective timestamp. All data recorded by the mobile device. The exact moment that the user has perceived a PTS/TTS event taking place. The exact moment that the user has perceived a TTS/NIHL event finishing.

The mobile engine is then responsible for decrypting the data that are received and uploading them to the Data Repository.

2.5 UI development

In order to help adult users of all ages with minimal technological background to navigate through the EVOTION application we tried to design mobile's app UI by:

- avoiding font sizes smaller than 16 pixels;
- providing a feature the users are able to adjust text size themselves
- paying particular attention to contrast ratios with text
- using bright colours and large icons

With the above requirements, a UX (User Experience) Wireframe has been initially constructed. Figure 4 demonstrates the Flowchart of this UX Wireframe:

UX FLOWCHART MOBILE APPLICATION | FLOWCHART SCHEME 01

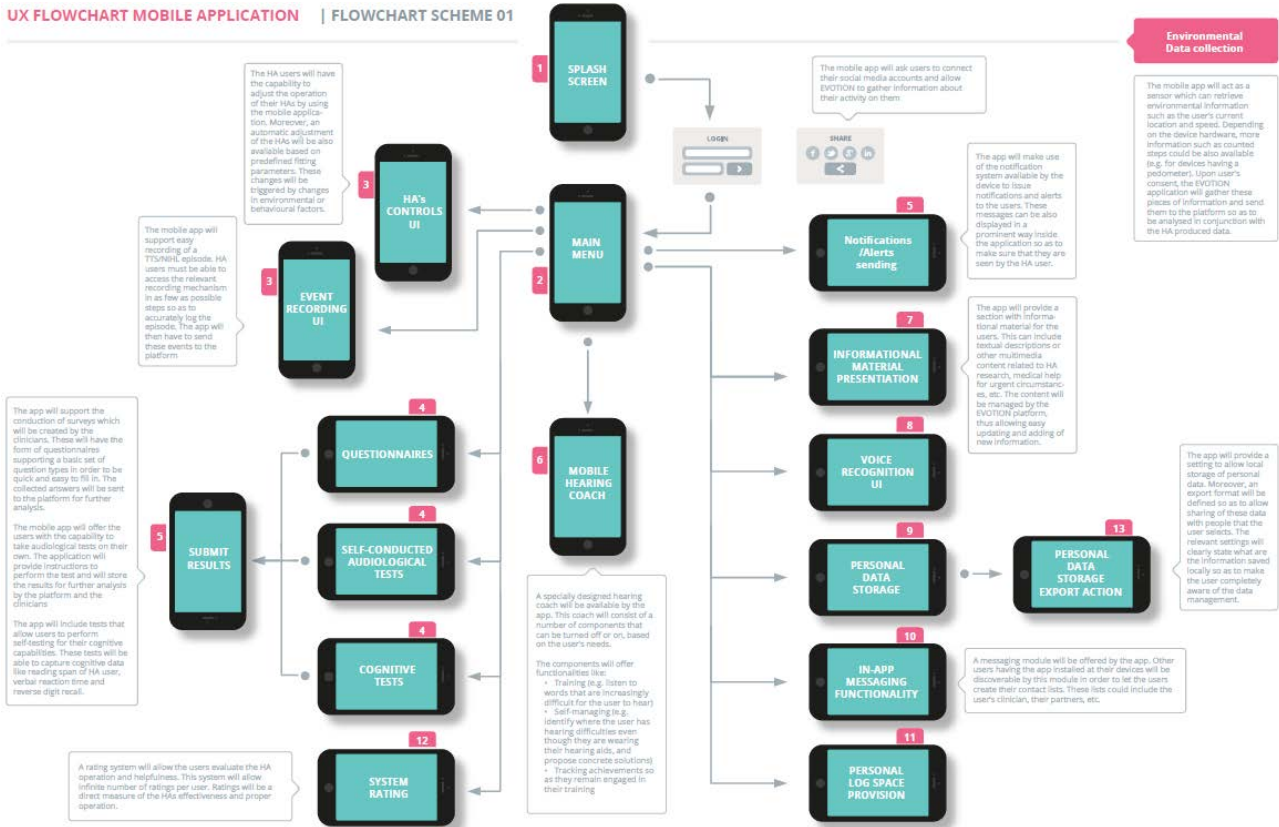


Figure 4: UX Wireframe of EVOTION mobile application

As a next step in the design of the UI development, mock-ups have been designed. Next figures are samples of the mock-ups that have been presented in the Consortium:



Figure 5: Menu mockup

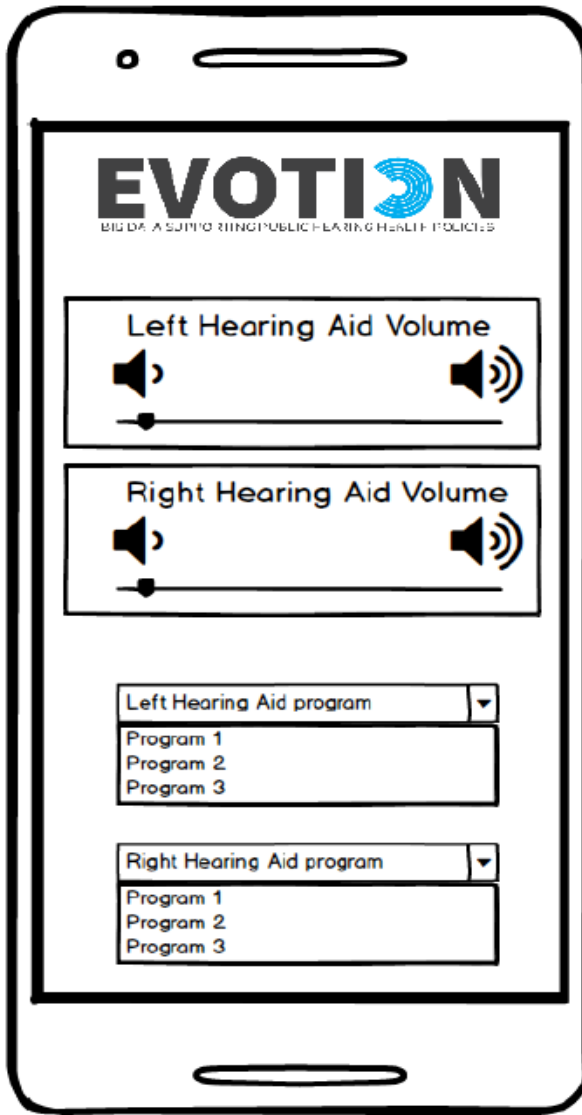


Figure 6: Controls mock-up

The above mock-ups have been discussed with the consortium, comments from all partners were collected and analysed, and used in the final version. The final version is thoroughly presented in section 4 (User Manual), with screenshots and guidelines of the mobile application.

3 Implementation

3.1 Technology

In the following sections, the technologies that were used to implement the mobile application are presented. Additionally, a detailed description of the dependencies and the versions currently used by the mobile application is provided.

3.1.1 Android SDK

The Android SDK Platform is required to compile the application. Every SDK release, contains a set of development tools used to develop applications for Android Platform. The Android SDK includes all the required libraries, debugger, documentation for the android application program interfaces and sample source code.

The minimum SDK that the EVOTION mobile application is developed is SDK 21, supporting devices that operate with Android 5 released in December 2014. The mobile device that has been chosen for the EVOTION project uses Android 6.0. However, the targeted SKD is set to 25 (Android 7.0) covering possible future OS upgrades of the mobile device.

3.1.2 SQLite Database

Android provides several options for saving persistent application data. SQLite has been chosen for storing data of the EVOTION mobile application on the mobile device. Android supports full support for SQLite databases. Any database that is created by the application is accessible by name to any class in the application, but not outside the application. SQLite is a self-contained, high-reliability, embedded, full-featured, public-domain, SQL database engine.

3.1.3 Bluetooth API

The EVOTION mobile app uses the Bluetooth protocol and API for the connection and the communication with the peripheral devices (HAs and the wearable sensor). The protocol that is used is the Bluetooth Low Energy protocol. The protocol is designed to provide stable and robust connections as well as significantly lower power consumption.

3.1.4 Libraries and Dependencies used by application.

Various dependencies are used by the mobile application in order to achieve the required functionalities described in this document.

Firestore v. 11.0.4

Firestore is Google's mobile platform that helps you quickly develop high-quality apps and grow your business. A library that is used from Firestore in EVOTION mobile app is Firestore Cloud Messaging (FCM) is a cross-platform messaging solution that lets you reliably deliver messages at no cost. Using FCM, you can notify a client app that new email or other data is available to sync. You can send notification messages to drive user reengagement and retention. For use cases such as instant messaging, a message can transfer a payload of up to 4KB to a client app.

GreenDao v. 3.2.2

GreenDAO is an open source Android ORM providing an easy and very fast way to use SQLite databases to help developers handle data efficiently.

EventBus v. 3.0.0

EventBus is a publish/subscribe event bus optimized for Android. EventBus simplifies the communication between components. It decouples event senders and receivers, performs well with Activities, Fragments, and background threads avoids complex and error-prone dependencies and life cycle issues.

Retrofit v. 2.3.0

Retrofit is a REST Client for Android and Java by Square. It makes it relatively easy to retrieve and upload JSON (or other structured data) via a REST based web service. Retrofit uses the OkHttp library for HTTP requests.

MayI

MayI is yet another library that simplifies the process of requesting permissions at runtime for devices that run Android Marshmallow and above. As of Androids Marshmallow and above a new functionality has been added that lets users grant or deny permissions while an app is running instead of granting them all together when installing it. This approach gives the user more control over applications but requires developers to add lots of code to support it. This library aims to reduce boilerplate code needed to request permissions at runtime by featuring a simple chainable API.

3.2 Security and privacy

To make sure that the data stored on the mobile device's storage are protected, the mobile app implements encryption mechanisms. In particular, data will be encrypted upon arrival from the biosensors and the hearing aids and stored in encrypted form on the mobile storage. The encrypted data will not be accessible on the mobile device whilst stored on it and will be transferred to the EVOTION platform (the EDR component through its ERESL interface) in encrypted form. Hence, whilst data reside on the mobile app will be safe. EDR will be able to decrypt the data received from the mobile app. Also, to establish a connection with the EDR platform, the mobile app will need to be authenticated by it. This will take place through the use of certificates. This security mechanism is described with more details in the following steps:

1. Peripheral devices are connected and periodically send data to mobile application through BLE.
2. Each time these data are received:
 - The mobile application generates a random symmetric key.
 - Received data are encrypted with the symmetric key.
 - The mobile app encrypts the symmetric key using the EVOTION platform's public key.
 - Encrypted data together with the encrypted symmetric key are stored on the mobile device's disk.
3. Once per day, when the mobile device has enough power and good network connection, the stored data are transmitted to the EVOTION platform:
 - Mobile initiates a TLS connection with the EVOTION platform.
 - During the connection initialization, both sides make sure that they verify and trust each other.
 - Data are transmitted securely over SSL.
 - The EVOTION platform decrypts the data received and stores them on EDR.

Furthermore, a secure registration process of the mobile device against the EVOTION platform when the initial installation of the mobile application occurs is followed. The mobile device registration process consists of two phases and is described with more details in the following steps:

1. **Phase A:**
 - A configurator (person responsible for mobile configuration) receives the mobile device, opens it and downloads the EVOTION mobile application.
 - The configurator opens the mobile application.
 - The mobile application generates a pair of a private and a public key locally.

- The mobile application recognizes the mobile device's unique serial number.
- The mobile application asks for the configurators credentials.
- The configurator provides his/her credentials.
- The mobile application sends the configurators credentials together with the serial number and the PKI of the mobile device to the EVOTION platform, under secure TLS connection.
- If credentials are correct, the mobile is registered as a verified EVOTION mobile device and the serial number and PKI are stored on LDAP and CA.

2. **Phase B:**

- A patient receives a registered and verified mobile device with the installed EVOTION mobile application.
- The serial number of the mobile device is correlated to the respective patient id.
- Data are updated on LDAP and CA.

After the above two phase registration process, the mobile device is considered as a verified EVOTION mobile device ready to be used by a real patient.

All the steps help to provide a robust and reliable security shield for the sensitive data of each patient. Some very important points that worth to be highlighted are:

- PKI is generated and stored only on the mobile application. Private key is not sent and not generated on the EVOTION platform.
- Patient does not need to authenticate since PKI together with LDAP is used for this.
- A CA (Certification Authority) is used to validate PKI. If a device is lost or stolen the public certificate is revoked and the device cannot further be used.
- Sensitive data stored are encrypted and only ERESL is capable of decrypting them.

3.2.1 Security objectives and functionality

Moreover, in following sub-sections, an analysis on how the above functionalities of the mobile application address the threats identified in Section 2.3.1 is presented. The security functionality provided includes protected communications to and from the Subsystem mobile app", configuration of security policies for mobile devices, and system reporting for detection of security relevant events.

3.2.1.1 O.DATA_PROTECTION_TRANSIT - Protected Communications

The mobile app will use a trusted communication path. The trusted channel to and from the mobile app is implemented using the standard protocols: TLS/SSL. To address the threat of network attacks (i.e., [T.NETWORK_ATTACK]), the mobile app provides encryption and mutual authentication to and from it, in a cryptographically secure manner. Thus, any attempt by a malicious attacker to represent himself/herself to the mobile app as another subsystem of the EVOTION will be detected.

3.2.1.2 O.STORAGE - Protected Storage

To address the issue of loss of confidentiality of user data in the event of a physical access threat (i.e., [T.PHYSICAL]), the mobile app will use data-at-rest protection. It will also be capable of encrypting data and keys stored on the device and will prevent unauthorized access to encrypted data.

3.2.1.3 O.AUTH - Authorization and Authentication

To address the issue of loss of confidentiality of user data in the event of loss of a mobile device (i.e., [T.PHYSICAL]), users are required to enter an authentication factor to the device prior to accessing protected

functionality and data. Some non-sensitive functionality (e.g., emergency calling, text notification) can be accessed prior to entering the authentication factor. The device will automatically lock following a configured period of inactivity in an attempt to ensure authorization will be required in the event of the device being lost or stolen. Authentication of the endpoints of a trusted communication path is required for network access to ensure attacks are unable to establish unauthorized network connections to undermine the integrity of the device. Repeated attempts by a user to get authorised access on the mobile device will be limited or throttled to enforce a delay between unsuccessful attempts.

3.2.1.4 O.ACCOUNTABILITY - System Reporting

To ensure that information exists that allows administrators to discover unintentional issues with the configuration and operation of the mobile device, the mobile device and app have the capability of generating reports which may indicate such issues. Auditing of administrative activities provides information that may hasten corrective action.

3.2.1.5 O.APPLY_POLICY - Mobile Device Configuration

Mobile devices will be configured with security policies in order to ensure the protection of enterprise or personal data that they may store or process. The mobile app is responsible for interacting with the mobile device to get information about the policies that regulate the execution of commands from other components of the EVOTION Platform, and sending data to the EVOTION Platform.

3.2.1.6 O.INTEGRITY - Mobile Device Integrity

To ensure their integrity the EVOTION mobile device and mobile App performs self-tests to ensure that the integrity of critical functionality, software/firmware and data has been maintained. The user shall be notified of any failure of these self-tests. This will protect against the threat [T.PERSISTENT]. To address the issue of an application containing malicious or flawed code threat (i.e., [T.FLAWAPP]), the integrity of downloaded updates to software/firmware will be verified prior to installation/execution of the object on the mobile device. In addition, the mobile app will restrict applications to only have access to the system services and data they are permitted to interact with according to the installed security policies. Through the functionality of the operating system, the mobile device will further protect against malicious applications from gaining access to data they are not authorized to access by randomizing the memory layout.

3.2.1.7 O.PRIVACY - End User Privacy and Device Functionality

An EVOTION mobile device may be used for both personal activities and the transmission of EVOTION data. A separation of personal and EVOTION data is realised. The privacy of the personal activities and data on the device is ensured by restricting the transmission of data from the mobile app to the EVOTION platform only to EVOTION data. This will protect against the threats [T.FLAWAPP] and [T.PERSISTENT].

3.3 Mobile API

The mobile application itself, offers an exposed API in order for the platform to be able to communicate with the users of the mobile application. For the moment, the exposed APIs of the mobile application are the ones that communicate with the peripheral devices through Bluetooth protocol and the Notification service that is subscribed to Google Firebase in order to receive alerts and notifications from the EVOTION platform.

Except for the above operations, mobile application has a significant number of services that are running on the background and are responsible for collecting and storing data. These services are:

1. Mobile Application is connected with the peripheral devices automatically.
2. When peripheral devices are connected the respective icons turn green on application's Status Bar.
3. Mobile Application collects device's Environmental Data every 5 minutes and 200 meters, encrypts them and stores them locally.
4. Mobile Application collects Hearing Aid's Environmental Data every 1 minute encrypts them and stores them locally.
5. When extensive noise is detected on the HAs, application starts recording an episode (either PTS or TTS). The application collects data from all devices and immediately sends them to the EVOTION platform. If the internet connection is not stable or the battery is low, the data are encrypted and stored locally until the internet and battery are restored.
6. Mobile Application stops the episode recording according to the episode's duration time that can be configured on the Settings page.
7. Mobile Application connects to Wearable Sensor three times per day and collects Sensor Data for 2 minutes, then encrypts and stores the average values locally.
8. Mobile Applications transmits to EVOTION Platform all encrypted data every 24 hours. If the internet connection is not stable or the battery is low, it will sleep and retry after a while. As soon as the data are transmitted successfully, they are deleted from mobile device.
9. Mobile Application stores all Hearing Aid's usage data and keeps records of all the actions of the user.
10. If there are frequent disconnections or excessive control's usage application sends to EVOTION Platform corresponding Feedback Data.

The table below summarizes the main classes and services of the mobile application and provides a short description for each of one:

Table 2: Operations of the EVOTION Mobile Application

Operation	Description
HAControl Class	The class through which the user can control the HAs (volume, program, etc.).
Security Class	The class that is in charge of all the security requirements of the mobile application. This class generates the keys, encrypts the data before being stored on the mobile device and handles all the security algorithms and libraries of the mobile application.
AlertMessaging Class	The class that creates and raises all the alerts on the mobile application.
WebClient Class	The class that establishes secure TLS connection with the EVOTION platform and uses the REST API that is offered by the platform.
EpisodeDetector Class	The class that analyses the data that are periodically received from the HAs and automatically detects if the user suffers from a PTS/TTS episode.
LoginAndRegistration Service	This service handles the registration process of the mobile device to the EVOTION platform.

HADataCollector Service	The service that connects the mobile application with the HAs and collects the respective data, encrypts them and stores them locally in the mobile device.
EnvironmentalDataCollector Service	The service that collect the environmental data of the mobile device (location, speed, routes, etc.)
EnvironmentalDataEpisodeCollector Service	The service that collects all the data that is needed when a PTS/TTS episode occurs to the patient. These data are all environmental, HA and wearable sensor data and they are sent directly to the EVOTION platform when the episode is ended. If the service is not able to upload these data, it encrypts them and stores them locally in the mobile device.
Update Service	The service that checks if a new version of the mobile application is released. If there is a new version, this service prompts the user to automatically update the mobile application.
SensorCollector Service	The service that connects the mobile application with the wearable sensor and collects the respective data, encrypts them and stores them locally in the mobile device.
UploadData Service	The service that uploads all encrypted data that are collected and stored through the day to the EVOTION platform. The service deletes the data from the mobile device after the successful transmission.
ControlsUsageReport Service	The service that detects frequent disconnections of the HAs as well as extensive use of the HAs and reports it to the EVOTION platform.
AudiologicalTest Service	The service that collects all audiological data, encrypts them and stores them locally in the mobile device.
CognitiveTest Service	The service that collects all the cognitive tests, encrypts them and stores them locally in the mobile device.
HearingCoach Service	The service that collects all the data from the Training tests, encrypts them and stores them locally in the mobile device.
Rating Service	The service that collects the rating results, encrypts them and stores them locally in the mobile device.
FirebaseNotification Service	The service that subscribes to Firebase and is in charge of receiving all the notifications coming from EVOTION platform towards the mobile application. The service also stores the notifications in the mobile device.
NetworkChange Service	The service that is in charge of detecting all the changes of the network status (Internet status, Bluetooth connectivity, etc.)

4 User Manual

4.1 Configurator user manual

The component's guide for the user role of Configurator is accessible through the following URL:

<http://h2020evotion.eu/?ddownload=528>

4.2 Patient user manual

The component's guide for the user role of Patient is accessible through the following URL:

<http://h2020evotion.eu/?ddownload=529>

5 Demonstrator

The executable (.apk) of the demonstrator is available at:

<http://h2020evotion.eu/?ddownload=530>

Please note that for the proper use of the demonstrator it is required that:

- The mobile device must be Bluetooth paired with the EVOTION peripheral devices (Oticon EVOTION and Huawei fit wearable sensor)
- The mobile device should have internet access
- Mobile's battery should be over 20%
- The user should have the hearing Aids connected with the mobile for at least 2 hours
- The user should wear the wearable sensor for at least one-day period during the tests

Also, a short video presentation of demonstrator is accessible through the following URL:

<http://h2020evotion.eu/?ddownload=533>

6 Conclusion

The EVOTION Mobile Application is an important part of the EVOTION ecosystem. It is the link between the patient and the EVOTION platform. It has been thoroughly tested and it is considered to be ready for deployment.

Furthermore, this report as part of deliverable D5.4 documents the design and implementation of the prototype EVOTION Mobile Application and the components interacting and exchanging data from and to it. The outcome of the report points to a reliable, robust and user friendly Mobile Application that is focused on offering great user experience. During the design and implementation of the mobile application, special attention is given on different sections of the app in order to be coherent. A consistent flow of the layout throughout the mobile application is also followed. At the same time the mobile application gathers all the data that is needed, while having minimum interaction with the users of the HAs and the wearable sensors and it allows the users controlling the EVOTION HAs. It silently collects and transmits all the data that are required by the EVOTION platform in order to process and extract useful information and advices that will help the patient in the future.

To conclude, the EVOTION Mobile Application that is described in this document is a fully functioning and tested Mobile Application.

Additional functionality of the prototype EVOTION Mobile Application such as collecting data coming from Audiological and Cognitive tests performed by the end-users, is to be included in the application by the next months of the project. Enhancements or updates of the EVOTION mobile application will be available to the end-users through a transparent and automatic update procedure.

References

- Dimakopoulos, N., Giotis, G., Kokkinakis, P., Economou, A., Fritaki, M., Gavalas, G., Prasinos, M., Smith, A., Spanoudakis, G., Papagrigoriou, P., Stefanakis, M., Koloutsou, N., Murrin, L., Katrakazas, P., Koutsouris, D., Brdarić, D., Milas, J., Dudarewicz, A., Pawlaczyk-Łuszczynska, M., Śliwińska-Kowalska, M., Zaborowski, K., Laplante-Lévesque, A., Memic, A., Pontoppidan, N.H., Kaloyanova, G., Trenkova, L., Tsokova, N., Bamiou, D.-E., Dritsakis, G., Anisetti, M., Bellandi, V., Cremonini, M., Damiani, E., Bibas, A., Kikidis, D., 2017. EVOTION stakeholders, scenarios, and requirements, Confidential Deliverable D2.1 to the EVOTION-727521 Project funded by the European Union. Athens Technology Center, Athens, Greece.
- Ye, B., Spanoudakis, G., Prasinos, M., Dimakopoulos, N., Kokkinakis, P., Giotis, G., Papas, I., Papagrigoriou, P., Smyrlis, M., Stefanakis, M., Katrakazas, P., Koutsouris, D., Brdaric, D., Pandzic, Z., Salavarda, D., Urban, M., Milas, J., Pontoppidan, N.H., Trenkova, L., Kaloyanova, G., Tsokova, N., Anisetti, M., Bellandi, V., Cremonini, M., Damiani, E., 2017. EVOTION Architecture and Detailed Design, Deliverable D2.2 to the EVOTION-727521 Project funded by the European Union. CITY University, London, United Kingdom.

EVOTION MOBILE APPLICATION

Observation testing steps

727521 – EVOTION

EVOTION MOBILE APPLICATION - Observation testing steps (Internal document)

Authors: Panagiotis Kokkinakis, Ilias Papas, Nikos Dimakopoulos (ATC)

Test prerequisites:

- ICCS/OTC should have VPN credentials to access CITY’s server
- ICCS/OTC should have internet connection for the mobile device
- ICCS/OTC should have keep mobile’s battery over 20%
- ICCS user should wear the smartwatch for at least one-day period during the tests. In a testing day, the EVOTION mobile app will wakeup smartwatch 3 times and will collect its data. The rest of the day EVOTION mobile app will not connected with the smartwatch.
- OTC user should have the HAs connected with the mobile for at least 2 hours
- OTC user should use HAs under noise exposure in order to surpass the PTS/TTS thresholds noise levels. For TTS the exposure to noise should be at least 1 min and for PTS the exposure to noise should be at least 2 hours.

Step number	Description	Expected result	Result
1. Device configuration (before installation of EVOTION mobile app)			
1.1	ICCS/OTC downloads and installs “SonicWall Mobile Connect” VPN application in the mobile device; https://play.google.com/store/apps/details?id=com.sonicwall.mobileconnect&hl=en .	Installed VPN app in the mobile device	
1.2	ICCS/OTC connects mobile device to CITY’s VPN using the above app	Connectd mobile device to CITY’s VPN	

2. EVOTION mobile app installation & mobile device registration to EVOTION ecosystem <i>(this set of actions should be performed only for the first time of EVOTION mobile app usage – Configurator’s actions)</i>			
2.1	ICCS/OTC downloads and installs “EVOTION” mobile application (https://evotion03.city.ac.uk:443/patientstorage/download/evotion_update)	Installed EVOTION mobile app in the device	
2.2	ICCS/OTC launches “EVOTION” mobile application.	EVOTION mobile app launches	
2.3	ICCS/OTC logs in to application (username and password will be provided by ATC)	If credentials are correct, device is considered as registered.	
2.4	ICCS/OTC accesses the Main Menu of the mobile app either by clicking top left button in App Bar or by sliding the screen to the right	User is able to access main menu	
2.5	ICCS/OTC finds mobile device’s serial number via “Information” button (bottom right) in Main menu.	User can get device’s serial number	
2.6	ICCS/OTC contacts ATC to correlate device’s serial number with a patient. ICCS/OTC should send the serial number of their mobile device by email.	User gets ATC’s confirmation that the mobile device has been correlated with a patient pseudo ID	
3. EVOTION mobile app usage <i>(Patient’s actions)</i>			
3.1	ICCS/OTC launches “EVOTION” mobile application	EVOTION mobile app launches	
3.2	Refresh connections with the peripheral device(s) via top right button in App Bar or “Refresh Connections” button in “Main menu”	Connection of mobile and peripheral device(s) is	

		active (green icon)	
3.3	Click "Controls" button of the Home Screen or "Hearing Aid's Controls" link in "Main Menu".	Controls screen is open	
3.3.1	Change hearing program (for both aids) by selecting/tapping one of "P1", "P2", "P3" or "P4" in Controls Screen.	Label "P1", "P2", "P3" or "P4" can be selected/tapped	
3.3.2	Adjusts hearing levels (for each aid) by sliding the corresponding slider in Controls Screen.	ICCS/OTC should check if slider works as is should be. OTC should check if sliders corresponds to HA volume level	
3.3.3	Lock both aids to adjust their hearing levels simultaneously by clicking "Link Sliders" button in Controls Screen.	ICCS/OTC should check if "Link Sliders" button can be tapped and slider works as is should be. OTC should check if sliders corresponds to HAs volume level	
3.3.4	Mute both aids by clicking "Mute All" button in Controls Screen	ICCS/OTC should check if "Mute All" button can be selected. OTC should check if HAs are muted.	

3.4	Configure episode duration time of “Uncomfortably loud sound” by clicking “Settings” button in Main Menu and adjusting slider’s level.	Settings screen is open and slider works as it should be.	
3.5	Overview all received Notifications via “Notification” button in Home Screen or “Notifications/Alerts” link in Main Menu.	Notifications/Alerts screen is open and includes several demo listed content	
3.6	Overview all information material via “Information” button in Home Screen or “Information Material” link in Main Menu.	Information screen is open and includes several demo listed content	
3.7	Insert manually an episode of “Uncomfortably loud sound” by clicking the red button on the bottom of Home and Controls screen.	Red button of Home and Controls screen can be tapped	
4. EVOTION mobile app – Automatic services			
4.1	Mobile app is connected with the peripheral devices automatically	When peripheral devices are connected, corresponding labels in the top app bar turns into green. ICCS please note that smartwatch label will be green only for 3 times per day.	
4.2	Mobile app collects device’s Environmental Data when user moves for at least 200 meters in the last 5 minutes and stores them locally in mobile	ATC/CITY should check EVOTION repository to	

	device (all personal data are encrypted). Applications sends to Evotion Platform all Environmental Data every 24 hours.	validate that data are being collected and stored as it should be.	
4.3	Mobile app collects Hearing Aid's Environmental Data every 1 minute and stores them locally in the mobile device. Mobile app calculates SPL values based on collected data and sends them to EVOTION Repository every 24 hours.	ATC/CITY should check EVOTION repository to validate that data are being collected and stored as it should be	
4.4	Mobile app connects to Wearable Sensor three times per day and collects Sensor Data for 2 minutes, then stores their average value locally in the mobile device (all personal data are encrypted). Mobile app sends to EVOTION repository all Sensor Data every 24 hours.	ATC/CITY should check EVOTION repository to validate that data are being collected and stored as it should be	
4.5	Mobile app stores all Hearing Aid's usage. If there are frequent disconnections or excessive control's usage application sends to EVOTION repository corresponding Feedback Data.	ATC/CITY should check EVOTION repository to validate that data are being collected and stored as it should be	

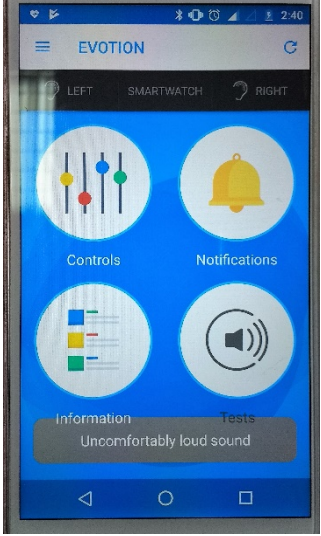
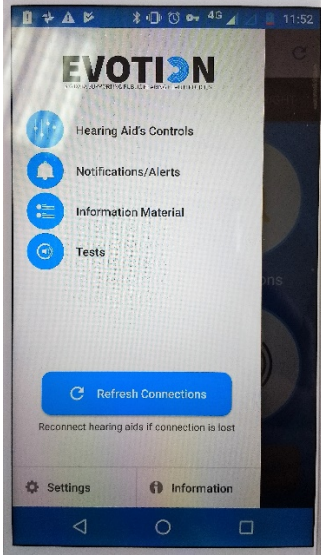
ANNEX 2 – Observation test results

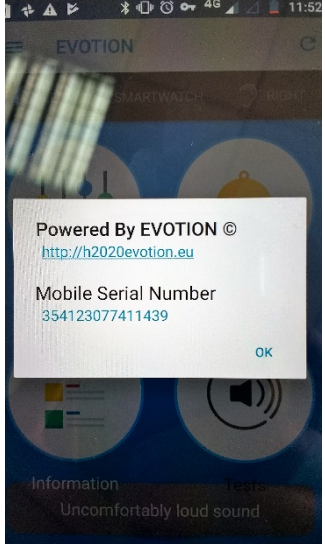

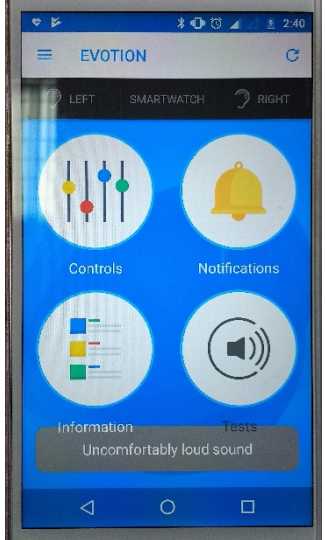
ICCS test results

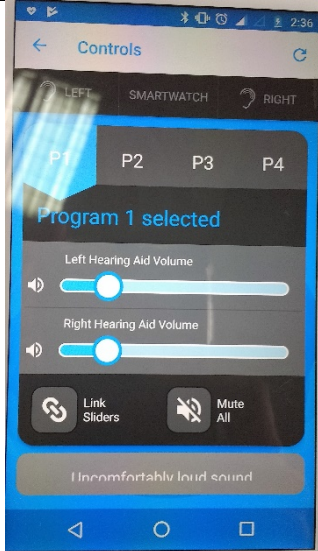
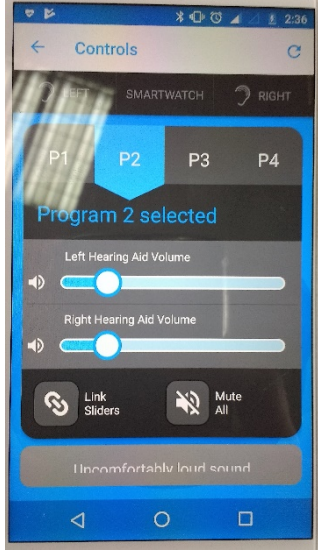
Test prerequisites:

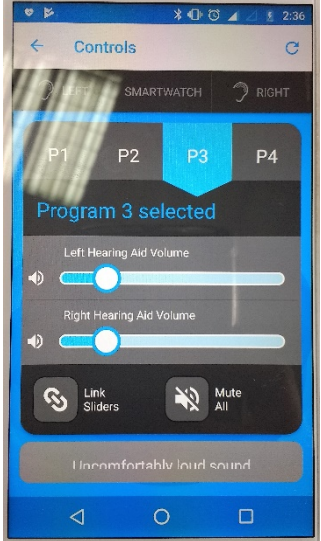
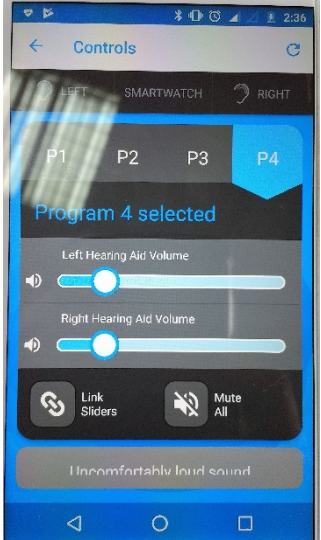
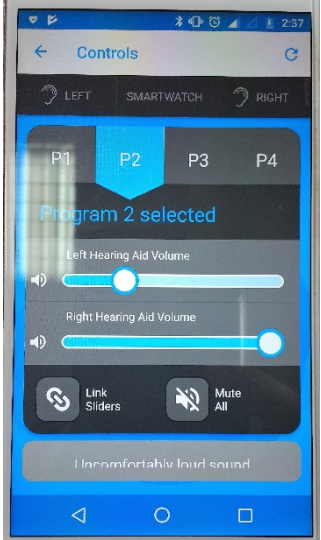
- ICCS/OTC should have VPN credentials to access CITY’s server
- ICCS/OTC should have internet connection for the mobile device
- ICCS/OTC should have keep mobile’s battery over 20%
- ICCS user should wear the smartwatch for at least one-day period during the tests. In a testing day, the EVOTION mobile app will wakeup smartwatch 3 times and will collect its data. The rest of the day EVOTION mobile app will not connected with the smartwatch.
- OTC user should have the HAs connected with the mobile for at least 2 hours
- OTC user should use HAs under noise exposure in order to surpass the PTS/TTS thresholds noise levels. For TTS the exposure to noise should be at least 1 min and for PTS the exposure to noise should be at least 2 hours.

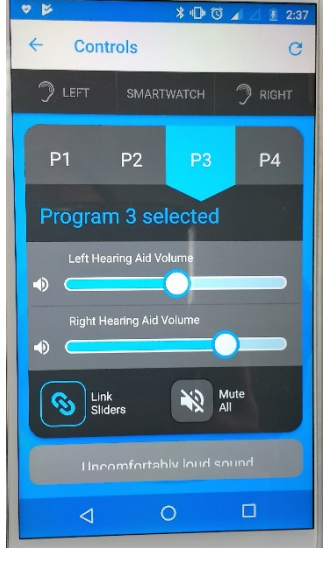
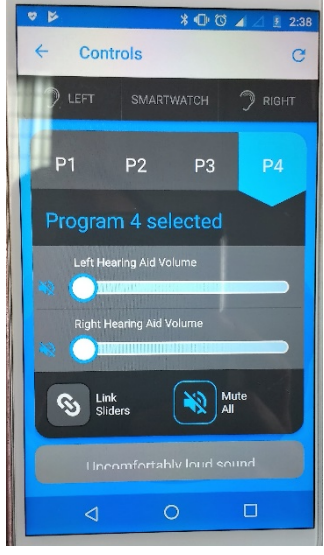
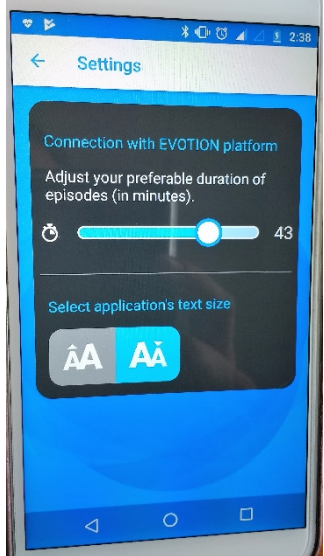
Step number	Description	Expected result	Result
1. Device configuration (before installation of EVOTION mobile app)			
1.1	ICCS/OTC downloads and installs “SonicWall Mobile Connect” VPN application in the mobile device; https://play.google.com/store/apps/details?id=com.sonicwall.mobileconnect&hl=en .	Installed VPN app in the mobile device	Successful installation
1.2	ICCS/OTC connects mobile device to CITY’s VPN using the above app	Connectd mobile device to CITY’s VPN	Successful connection
2. EVOTION mobile app installation & mobile device registration to EVOTION ecosystem <i>(this set of actions should be performed only for the first time of EVOTION mobile app usage – Configurator’s actions)</i>			
2.1	ICCS/OTC downloads and installs “EVOTION” mobile application (https://evotion03.city.ac.uk:443/patientstorage/download/evotion_update)	Installed EVOTION mobile app in the device	Successful installation

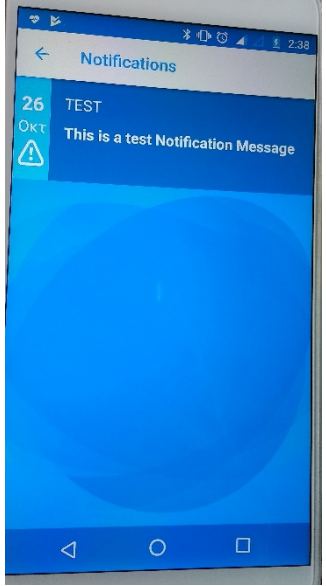
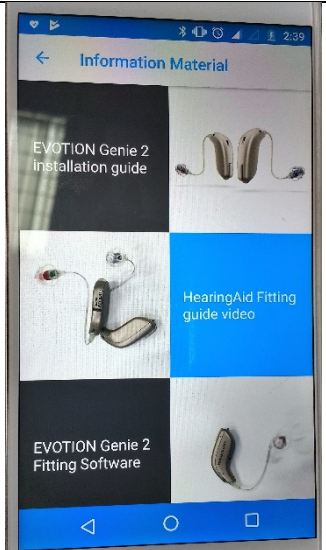
2.2	ICCS/OTC launches "EVOTION" mobile application.	EVOTION mobile app launches	
2.3	ICCS/OTC logs in to application (username and password will be provided by ATC)	If credentials are correct, device is considered as registered.	
2.4	ICCS/OTC accesses the Main Menu of the mobile app either by clicking top left button in App Bar or by sliding the screen to the right	User is able to access main menu	

2.5	ICCS/OTC finds mobile device's serial number via "Information" button (bottom right) in Main menu.	User can get device's serial number	
2.6	ICCS/OTC contacts ATC to correlate device's serial number with a patient. ICCS/OTC should send the serial number of their mobile device by email.	User gets ATC's confirmation that the mobile device has been correlated with a patient pseudo ID	<p>Internal communication between ATC and ICCS for step 2.6</p> 
<p>3. EVOTION mobile app usage <i>(Patient's actions)</i></p>			
3.1	ICCS/OTC launches "EVOTION" mobile application	EVOTION mobile app launches	

3.2	Refresh connections with the peripheral device(s) via top right button in App Bar or “Refresh Connections” button in “Main menu”	Connection of mobile and peripheral device(s) is active (green icon)	Refresh pressed but not active connections are shown
3.3	Click “Controls” button of the Home Screen or “Hearing Aid’s Controls” link in “Main Menu”.	Controls screen is open	
3.3.1	Change hearing program (for both aids) by selecting/tapping one of “P1”, “P2”, “P3” or “P4” in Controls Screen.	Label “P1”, “P2”, “P3” or “P4” can be selected/tapped	

			 
3.3.2	Adjusts hearing levels (for each aid) by sliding the corresponding slider in Controls Screen.	<p>ICCS/OTC should check if slider works as is should be.</p> <p>OTC should check if sliders corresponds to HA volume level</p>	

3.3.3	Lock both aids to adjust their hearing levels simultaneously by clicking “Link Sliders” button in Controls Screen.	ICCS/OTC should check if “Link Sliders” button can be tapped and slider works as it should be. OTC should check if sliders corresponds to HAs volume level	
3.3.4	Mute both aids by clicking “Mute All” button in Controls Screen	ICCS/OTC should check if “Mute All” button can be selected. OTC should check if HAs are muted.	
3.4	Configure episode duration time of “Uncomfortably loud sound” by clicking “Settings” button in Main Menu and adjusting slider’s level.	Settings screen is open and slider works as it should be.	

3.5	Overview all received Notifications via “Notification” button in Home Screen or “Notifications/Alerts” link in Main Menu.	Notifications/Alerts screen is open and includes several demo listed content	
3.6	Overview all information material via “Information” button in Home Screen or “Information Material” link in Main Menu.	Information screen is open and includes several demo listed content	
3.7	Insert manually an episode of “Uncomfortably loud sound” by clicking the red button on the bottom of Home and Controls screen.	Red button of Home and Controls screen can be tapped	No red button shown or found in Home and Controls Screen
4. EVOTION mobile app – Automatic services			
4.1	Mobile app is connected with the peripheral devices automatically	When peripheral devices are connected, corresponding labels in the top	Successful

		app bar turns into green. ICCS please note that smartwatch label will be green only for 3 times per day.	
4.2	Mobile app collects device's Environmental Data when user moves for at least 200 meters in the last 5 minutes and stores them locally in mobile device (all personal data are encrypted). Application sends to Evotion Platform all Environmental Data every 24 hours.	ATC/CITY should check EVOTION repository to validate that data are being collected and stored as it should be.	Successful
4.3	Mobile app collects Hearing Aid's Environmental Data every 1 minute and stores them locally in the mobile device. Mobile app calculates SPL values based on collected data and sends them to EVOTION Repository every 24 hours.	ATC/CITY should check EVOTION repository to validate that data are being collected and stored as it should be	Successful
4.4	Mobile app connects to Wearable Sensor three times per day and collects Sensor Data for 2 minutes, then stores their average value locally in the mobile device (all personal data are encrypted). Mobile app sends to EVOTION repository all Sensor Data every 24 hours.	ATC/CITY should check EVOTION repository to validate that data are being collected and stored as it should be	Successful
4.5	Mobile app stores all Hearing Aid's usage. If there are frequent disconnections or excessive control's usage application sends to EVOTION repository corresponding Feedback Data.	ATC/CITY should check EVOTION repository to validate that data are being	Successful

		collected and stored as it should be	
--	--	--------------------------------------	--

OTC test results

Test prerequisites:

- ICCS/OTC should have VPN credentials to access CITY’s server
- ICCS/OTC should have internet connection for the mobile device
- ICCS/OTC should have keep mobile’s battery over 20%
- ICCS user should wear the smartwatch for at least one-day period during the tests. In a testing day, the EVOTION mobile app will wakeup smartwatch 3 times and will collect its data. The rest of the day EVOTION mobile app will not connected with the smartwatch.
- OTC user should have the HAs connected with the mobile for at least 2 hours
- OTC user should use HAs under noise exposure in order to surpass the PTS/TTS thresholds noise levels. For TTS the exposure to noise should be at least 1 min and for PTS the exposure to noise should be at least 2 hours.

Step number	Description	Expected result	Result		
			Phone 1 Samung Galaxy (XI)	Phone 2 Samsung Galaxy Note 4 (Lukas)	Phone 3 Samsung Galaxy S6 (Johanna)
1. Device configuration (before installation of EVOTION mobile app)					
1.1	ICCS/OTC downloads and installs “SonicWall Mobile Connect” VPN application in the mobile device; https://play.google.com/store/apps/details?id=com.sonicwall.mobileconnect&hl=en .	Installed VPN app in the mobile device	As expected	As expected	As expected
1.2	ICCS/OTC connects mobile device to CITY’s VPN using the above app	Connectd mobile device to CITY’s VPN	VPN connection asks for credentials every time after restarting the phone	VPN connection asks for credentials every time after restarting the phone	VPN connection asks for credentials every time after restarting the phone

2. EVOTION mobile app installation & mobile device registration to EVOTION ecosystem (this set of actions should be performed only for the first time of EVOTION mobile app usage –Configurator’s actions)					
2.1	ICCS/OTC downloads and installs “EVOTION” mobile application https://evotion03.city.ac.uk:443/patientstorage/download/evotion_update)	Installed EVOTION mobile app in the device	As expected	AS expected	As expected
2.2	ICCS/OTC launches “EVOTION” mobile application.	EVOTION mobile app launches	As expected	AS expected	As expected
2.3	ICCS/OTC logs in to application (username and password will be provided by ATC)	If credentials are correct, device is considered as registered.	As expected	AS expected	As expected
2.4	ICCS/OTC accesses the Main Menu of the mobile app either by clicking top left button in App Bar or by sliding the screen to the right	User is able to access main menu	As expected	AS expected	As expected
2.5	ICCS/OTC finds mobile device’s serial number via “Information” button (bottom right) in Main menu.	User can get device’s serial number	As expected	AS expected	As expected
2.6	ICCS/OTC contacts ATC to correlate device’s serial number with a patient. ICCS/OTC should send the serial number of their mobile device by email.	User gets ATC’s confirmation that the mobile device has been correlated with a patient pseudo ID	Mobile-Serial number: 354361082 235720	Mobile Serial Number:35 420106644 8875	Mobile Serial Number: 99000484 3510714
3. EVOTION mobile app usage (Patient’s actions)					
3.1	ICCS/OTC launches “EVOTION” mobile application	EVOTION mobile app launches	As expected	Stopped working after 2.6 because the hearing aid was not able to	As expected

				connect with app	
3.2	Refresh connections with the peripheral device(s) via top right button in App Bar or “Refresh Connections” button in “Main menu”	Connection of mobile and peripheral device(s) is active (green icon)	Works after rebooting the phone. (Comment: place new batteries into hearing aid before pairing)		As expected
3.3	Click “Controls” button of the Home Screen or “Hearing Aid’s Controls” link in “Main Menu”.	Controls screen is open	As expected		As expected
3.3.1	Change hearing program (for both aids) by selecting/tapping one of “P1”, “P2”, “P3” or “P4” in Controls Screen.	Label “P1”, “P2”, “P3” or “P4” can be selected/tapped	As expected		As expected
3.3.2	Adjusts hearing levels (for each aid) by sliding the corresponding slider in Controls Screen.	ICCS/OTC should check if slider works as is should be. OTC should check if sliders corresponds to HA volume level	As expected		As expected
3.3.3	Lock both aids to adjust their hearing levels simultaneously by clicking “Link Sliders” button in Controls Screen.	ICCS/OTC should check if “Link Sliders” button can be tapped and slider works as is should be. OTC should check if sliders corresponds	As expected		As expected

		to HAs volume level			
3.3.4	Mute both aids by clicking “Mute All” button in Controls Screen	ICCS/OTC should check if “Mute All” button can be selected. OTC should check if HAs are muted.	As expected		As expected
3.4	Configure episode duration time of “Uncomfortably loud sound” by clicking “Settings” button in Main Menu and adjusting slider’s level.	Settings screen is open and slider works as it should be.	As expected		As expected
3.5	Overview all received Notifications via “Notification” button in Home Screen or “Notifications/Alerts” link in Main Menu.	Notifications/ Alerts screen is open and includes several demo listed content	As expected		As expected
3.6	Overview all information material via “Information” button in Home Screen or “Information Material” link in Main Menu.	Information screen is open and includes several demo listed content	As expected		As expected
3.7	Insert manually an episode of “Uncomfortably loud sound” by clicking the red button on the bottom of Home and Controls screen.	Red button of Home and Controls screen can be tapped	Change ‘TTS’ and ‘PTS’ to user friendly explanation, otherwise works as expected		Change ‘TTS’ and ‘PTS’ to user friendly explanation, otherwise works as expected
EVOTION mobile app – Automatic services					

4.1	Mobile app is connected with the peripheral devices automatically	When peripheral devices are connected, corresponding labels in the top app bar turns into green. ICCS please note that smartwatch label will be green only for 3 times per day.	As expected		As expected
4.2	Mobile app collects device's Environmental Data when user moves for at least 200 meters in the last 5 minutes and stores them locally in mobile device (all personal data are encrypted). Applications sends to Evotion Platform all Environmental Data every 24 hours.	ATC/CITY should check EVOTION repository to validate that data are being collected and stored as it should be.	Not applicable for OTC	Not applicable for OTC	Not applicable for OTC
4.3	Mobile app collects Hearing Aid's Environmental Data every 1 minute and stores them locally in the mobile device. Mobile app calculates SPL values based on collected data and sends them to EVOTION Repository every 24 hours.	ATC/CITY should check EVOTION repository to validate that data are being collected and stored as it should be	Not applicable for OTC	Not applicable for OTC	Not applicable for OTC
4.4	Mobile app connects to Wearable Sensor three times per day and collects Sensor Data for 2 minutes, then stores	ATC/CITY should check	Not applicable for OTC	Not applicable for OTC	Not applicable for OTC

	their average value locally in the mobile device (all personal data are encrypted). Mobile app sends to EVOTION repository all Sensor Data every 24 hours.	EVOTION repository to validate that data are being collected and stored as it should be			
4.5	Mobile app stores all Hearing Aid's usage. If there are frequent disconnections or excessive control's usage application sends to EVOTION repository corresponding Feedback Data.	ATC/CITY should check EVOTION repository to validate that data are being collected and stored as it should be	Not applicable for OTC	Not applicable for OTC	Not applicable for OTC
<p>General Feedback:</p> <p>1.) In the main menu and in the home screen, there is an icon called Information, which is confusing as it appears twice. Could it be changed into Instructions for users or manuals in the home screen?</p> <p>2.) Is it possible that when the hearing aids connects to phone to have a pop-up notification as well ?</p> <p>3.)Phone 2 (Lukas) had issues with connecting the hearing devices to the app that could happen to the user as well, is there a 'help desk' button perhaps in the information blocks or a Q&A?</p> <p>4.) After recording for 'uncomfortable loud sound' the button changed to 'comfortably loud sound', which makes no sense.</p> <p>5.) We propose more information provided to the user regarding TTS/PTS and what is the purpose to report 'uncomfortably loud sound'. The user may not need to choose TTS/PTS but instead simply report the event as it was uncomfortably loud. 'Start recording' can be a bit confusing as the recording is always on. We suggest using e.g. 'report event'.</p> <p>6.) We propose instruction to the clinicians on 'How to pair EVOTION hearing aids with the EVOTION phone', if it has not already planned to do so.</p>					

*Phones that used to test the EVOTION app

	Phone 1	Phone 2	Phone 3
Brand and model	Sumsung GALAXY A5	Sumsung GALAXY Note 4	Phone 3

	SM-A510F (16GB)		Samsung Galaxy S6
IMEI	354361/08/223572/0		990004/84/351071/4
EVOTION app recognized serial nb.	354361082235720	354201066448875	990004843510714
S/N	RF8HA1L9V0H		S S17-05

* The hearing aids that were paired with Phone 1 were left on and stay connected since 14:30 Oct. 24th and still on while this report is written 08:30 Oct.25th. No loss of connection was found. The app appears to be stable as well. A couple of ‘uncomfortably loud sound’ were reported and recorded.