

THE PRODUCT SPECIFICATION DOCUMENT

TEAM 3

Introduction

The Product Specification Document is written to specify the “Safe Messenger” product. It enables the users of this product to see their location on map and send/receive messages within the group. The Product Requirements Document already explains states the expectations from the product with respect to the market and customer choices. Quality Function Deployment analysis which documents the customer needs have been carried out and presented as a part of the Product Requirements Document.

The Product Specification Document can be regarded as the continuation of the definition of the product. As a difference from the Product Requirements Document, the product and the expectations from it are discussed from the engineering perspective. It also aims to determine the conditions for the test of the product during its development and at the final. In this document, the details regarding the design of the hardware and software parts are excluded.

Authors:

Abdullah Başar Akbay (HW Designer)
İsmail Akpolat (SW Designer)
Kemal Çağrı Bardakçı (SW Designer)
Oğuzhan Avcı (HW Designer)

Hardware Specifications

Hardware part is responsible for the decryption and encryption of the plain text entered by the users using the software. When the user desires to send information, hardware component receives the plain text from the phone, encrypts it and transmits the cipher text to phone. Similarly, when encrypted information is obtained from another user, it is sent to hardware component to be decrypted and plain text is resent to smartphone. Bluetooth wireless channel will be used as the communication channel between the smartphone and hardware component in order to maintain the compatibility of the hardware component with different smartphone brands and models.

Weight and Height Specifications

- The target weight range of the product is 10-35g which is the average weight of Bluetooth products such as earphones in the market (35g [1], 18g [2], 9g [3]). The weight of the product should not exceed 125g which is the average weight of mobile phones (135g [4], 105g [5]).
- The target size of the product can be defined as 50 (L) x 20 (W) x10 (H) mm which is the average size of the Bluetooth products in the market (50x7x30mm [6] and 52x18x10mm [7]) . Considering the ease of transportation, the dimensions should not exceed 80mm for length/width and 40mm for height.

Power Supply Specifications

- The device power supply requirements include voltage outputs 1.5V to 3.3V and current outputs from tens of milliamps to multiple amperes [8].
- The logic device is sensitive to the voltage and current variations. Due to these reasons usage of supply voltage regulator is required. The regulator should be capable of satisfying power supply requirements given above.
- As the power supply voltage, usage of rechargeable batteries which can provide high current outputs above 500mA and nominal voltage output around 5V are required.
- As the power supplier, Li-Ion or Polymer Li-Ion rechargeable batteries can be used. It should have a nominal voltage output around 5V and maximum discharging current rate of 0.2C – 0.5C. Current supply is important, because high current values (above 0.5A) can be drawn by the logic device. The supply voltage shall have high energy density of around 1800 – 5000 mAh and low weight which is around 30 – 50g. This satisfies at least 4 hours of continuous usage of the encryption device.
- Considering the sharp power consumption differences, power supply of logic device unit and Bluetooth connection unit should be separate.

Functional and Performance Specifications

- Bluetooth range shall be at least 3-5m. Bluetooth device should be qualified to work nearby a Wi-Fi device without interfering with it.
- The encryption method must be Public Key Cryptography with sufficient high number of bits (at least 128-bit which is the most powerful form of encryption available in browsers today [9] becomes the new standard on web browsers [10]) encryption used to generate an encryption key.
- The encryption/decryption time shall not be large. It should be smaller than a 1s.
- Hardware module should generate public and private keys when the user is log on to the network. After generation of the keys, private key should be kept in the hardware and public key should be sent to smartphone to be published.
- Hardware component shall store the public keys of the other users during a session. It uses these public keys in encryption processes.

Software Specifications

- The size of the software will not be greater than 10mb.
- A message will contain maximally 300-characters in the message window. An example of a message window can be seen in figure-1.



Figure 1 – Message Window

- In the group conference mode, the number of people will be constrained maximally to 5 – 10 people.
- The application will enable the users to see others' location on the map starting from the 10 meters distance. Nevertheless, the users will have the option of scaling with 100 meters, 1 kilometer, 10 kilometers, etc. to only track the people in the range of those distances from the user as it is seen in figure-2 (Users' photo, longitude and latitude information -by assuming the user's position as zero point- also can be seen when their location is clicked).

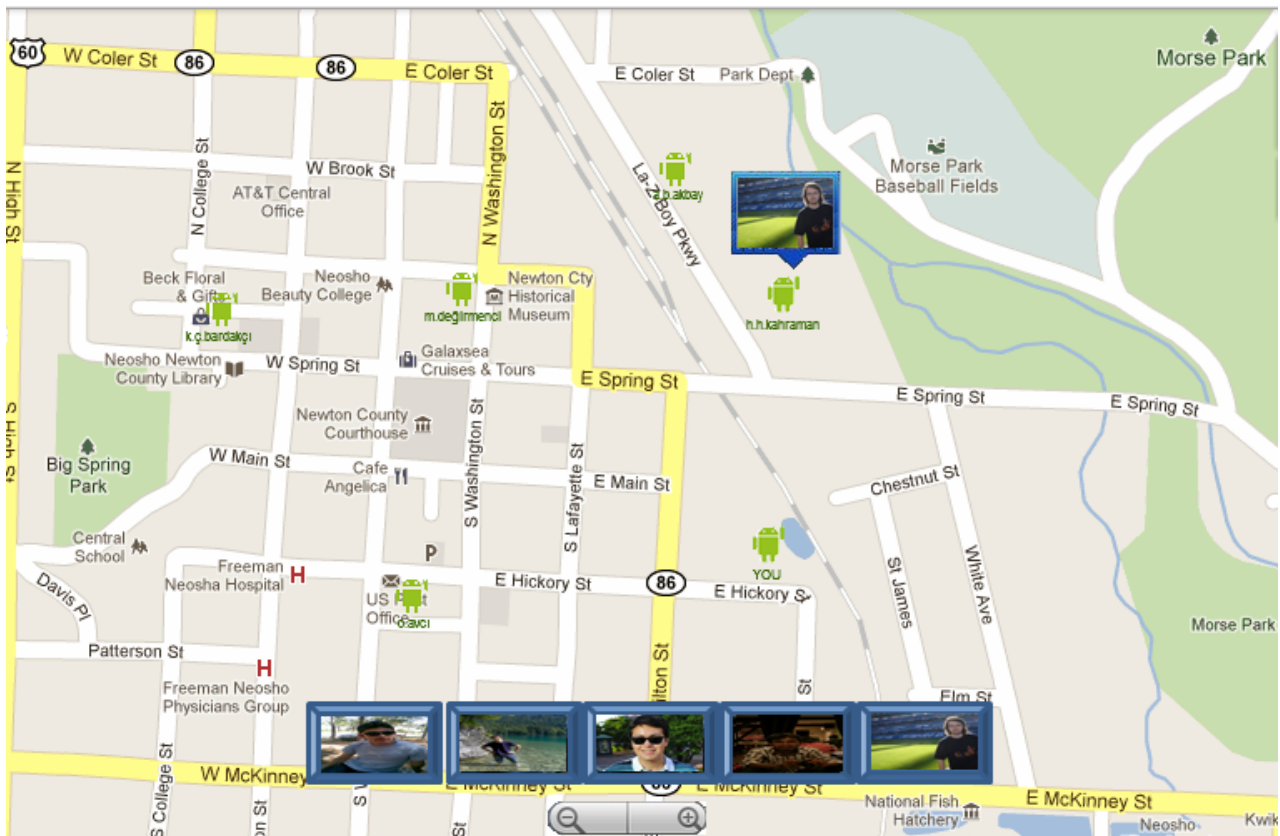


Figure 2 – An example of extended map screen.

- If the battery of the encryption device is run out, encryption will be done directly using smart phone until the battery is recharged.
- Estimated locations which are supplied from cell towers will have a precision of 100 meters in urban areas and 1 kilometer for rural areas.
- A group consists of 10 person maximum.
- Whether a person is online or offline will be indicated with different colors.
- Last 10 locations of users will be hold in database and users will be able to see location of others even if they are offline.
- There will be five different screens in application including login screen, map-message screen, add-join group screen, option screen, help screen (Some of them are shown in figure-3).



Figure 3 – User interface of application

Quality Function Deployment

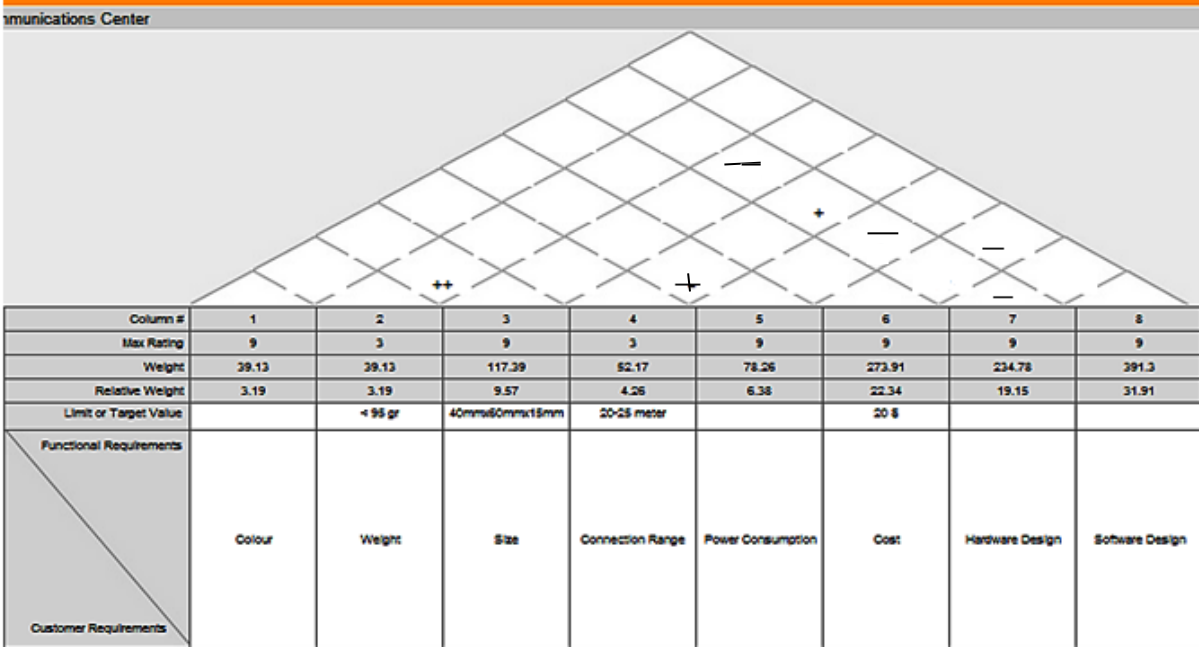


Figure 4 – Top Roof of QFD

As we can see the roof of the House of Quality, weight has strong positive correlation with size. Hardware design has strong negative correlation with cost, size and power consumption which indicates that with better hardware and software designs, cost, size and power consumption can be reduced without any reduction in performance of the system. Hardware design has also positive relation with connection range. In addition to these, software design has negative correlation with cost. Size and weight are much correlated parameters. In general, if a size of a component increases, its weight also increases. Connection range and power consumption are negatively correlated, since an increase in the connection range requires sending Bluetooth signals with higher power levels. Naturally, an increase in the power consumption can be expected.

References

- [1] “*Plantronics 903/R US BackBeat Headphones*” <http://www.amazon.com/Plantronics-903-US-BackBeat-Headphones/dp/B001TK3AC0> Last Accessed on 25.11.2011
- [2] “*Samsung HM1500 RODIN Clip On Bluetooth Handsfree*” <http://www.amazon.co.uk/Samsung-HM1500-RODIN-Bluetooth-Handsfree/dp/B003FST6HW> Last Accessed on 25.11.2011
- [3] “*Jabra Bt2035 Bluetooth Headset*” <http://www.hama.de/00104808/jabra-bt2035-bluetooth-headset> Last Accessed on 25.11.2011
- [4] “*Nokia N8*” <http://www.amazon.com/Nokia-Touchscreen-Featuring-Navigation-Camera-U-S/dp/B003ZX7RL4> Last Accessed on 25.11.2011
- [5] “*Samsung Galaxy Mini S5570*” http://www.gsmarena.com/samsung_galaxy_mini_s5570-3725.php Last Accessed on 25.11.2011
- [6] “*Rogadis BSH18 Stereo Bluetooth Kulaklık*” www.hepsiburada.com Last Accessed on 25.11.2011
- [7] “*Samsung HM1100 Bluetooth Earphone*” www.hepsiburada.com Last Accessed on 25.11.2011
- [8] “*Design Guide for Altera FPGA Power Management Systems*” http://www.digikey.com/Web%20Export/Supplier%20Content/STMicroelectronics_497/PDF/FPGA_Altera.pdf?redirected=1 Last Accessed on 25.11.2011
- [9] “*Understanding encryption levels*” <http://www.opera.com/support/kb/view/593/> Last Access 25.11.2011
- [10] “*What is the Difference Between 40-bit and 128-bit Encryption?*” <http://compnetworking.about.com/od/networksecurityprivacy/l/aa011303a.htm> Last Accessed on 25.11.2011