Final Report

001

03.01.2012

Version 1

Team 3

	Name	Title	Date	Signature
Prepared By	K.Ç. Bardakçı İ.Akpolat M.Değirmenci H.H. Kahraman O.Avcı A.B.Akbay	SW Engineer SW Engineer CFO PDM HW Engineer HW Engineer	31.12.2011	
Controlled By	H.H. Kahraman	PDM	02.01.2012	
Approved By	A.B.Akbay	CEO	03.01.2012	

Table of Contents

1. Executive Summary

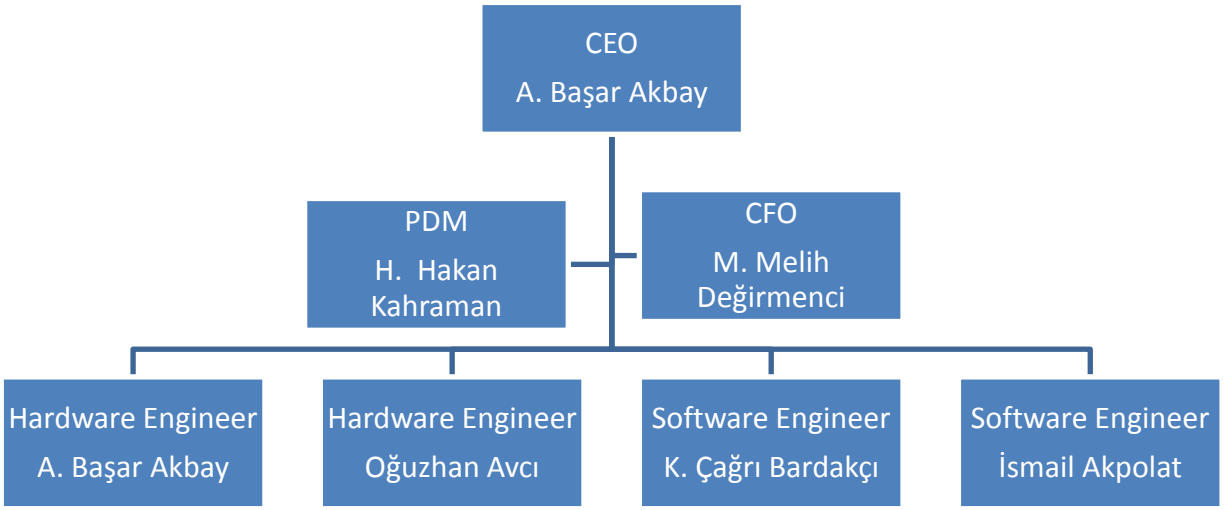
Secure Communications Center (SCC) Associates has been founded by 6 shareholders in order to provide secure messaging on mobile phones and location tracking. The main aim of the company is to produce innovative and secure messaging system combined with location tracking in the smart phones' accessories market that can meet the demand.

The target customer of our company is especially military and police maybe any other customers like company that want to use location tracking system with high security. Considering the importance of secure communication issues and customer's need to use or buy the equipment, the company would be able to sell its products directly to customers and make profit.

Aim of the Secure Communications Center (SCC) Associates is to have the most of the share in the secure communication system on smart phones market in Turkey. The product we are planning to produce helps to military and police service via both secure messaging and location tracking. This product can be called as a messenger program being run on smart phones (Android operating systems) and having the feature of enabling users to see the positions of each other on a map. All the information shared within the group is encrypted. Via this product, providing secure communication to the users is the main target. The benefits of the product are known but security problem hadn't been considered by any other producers. However, when we produced it with feature that satisfies security, customers will be tend to buy the product.

The power of innovative thinking and serious research of the market is done by the establishers of the company to establish Secure Communications Center (SCC) Associates. Considering the capabilities of the company, the innovative product that is designed, Secure Communications Center (SCC) Associates aims to dedicate itself to serve for the military and police service according to their needs. According to demands of companies, customers or institutions, the needs may differ like more powerful encrypting system or any other features which can be implemented on our product. Basically, our product is flexible to any further development since the codes and design are completely controlled by our engineers.

2. Company Organization



CEO of Project

Abdullah Başar AKBAY is the CEO of the company because he brought the all member together and knows complete information about each production process of our product. He is in charge for all operations and decisions taken in the company. He decides about the product development and investment plans and analyzes the final reports. He is responsible for the general progress of the project. The responsibilities of the CEO are set by the organization's board of directors. Typically, the CEO has responsibilities as a communicator, decision maker, leader and supervisor. The communicator role includes the press and the rest of the outside world, as well as between employees. The decision-making role contains high-level decisions about policy and strategy. As a leader, the CEO advises the board of directors, motivates them.

Hardware

We have two hardware engineers in our team whose names are Oğuzhan Avcı who is hardware director and Abdullah Başar Akbay. They are responsible to produce hardware of the Secure Communications Center (SCC) by combining mobile phone to a cryptographic device which encodes the data sent from the mobile device. This device should be designed small enough to be portable. The connection between the cryptographic device and mobile phone is done through Bluetooth technology.

Software

We have two software engineers in our team whose names are İsmail Akpolat who is software director and Kemal Çağrı Bardakçı. They are responsible to design software of the Secure Communications Center (SCC) whose user interface which displays the locations of the other users on a map is designed. Also it enables the user to send and receive encrypted messages. The encrypted information is transmitted to the other users via a HTTP Server application. Moreover, they will deal with creating a logo and a webpage for the company.

Quality Control and Product Development Manager

Hilmi Hakan Kahraman is the Quality Control and Product Development Manager of the company. His main jobs are to manage the quality control process before,during and after production, to procure of correct raw materials with due consideration to compliance to revelant production standarts, to make coordination the relations between the sales,production,quality control departments and the customers in an optimum manner, to maintain safe working places in the laboratory and to give the formulations to production and to back up production manager for production processes.

CFO of Project

The Financial Director of Secure Communications Center (SCC) Associates is Mehmet Melih Değirmenci who takes the responsibility of financial decisions in the company. He manages the financial risks of the business. The Financial Manager takes decisions about the business; develops a business plan, a financial plan and a marketing plan. He is responsible for everything about the financial aspects of the company. In the future, the company may need to do the accounting management separately so these positions are considered for any future needs.

3. Corporate Identity Designs

Figure 1- LogoType1

Security Communications Center

Figure 2 – Logo Type 2

Security Communications Center

Figure 3 – Logotype 3

Figure 4 – Logo Type 4

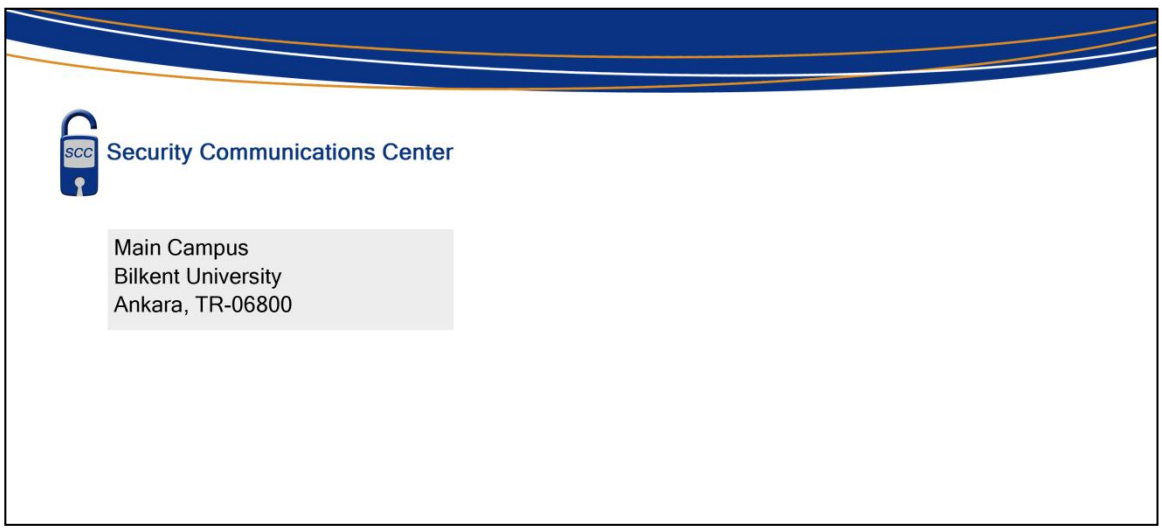


Figure 5 – Envelope

Figure 6 – Business Card

Figure 7 – Business Card Back

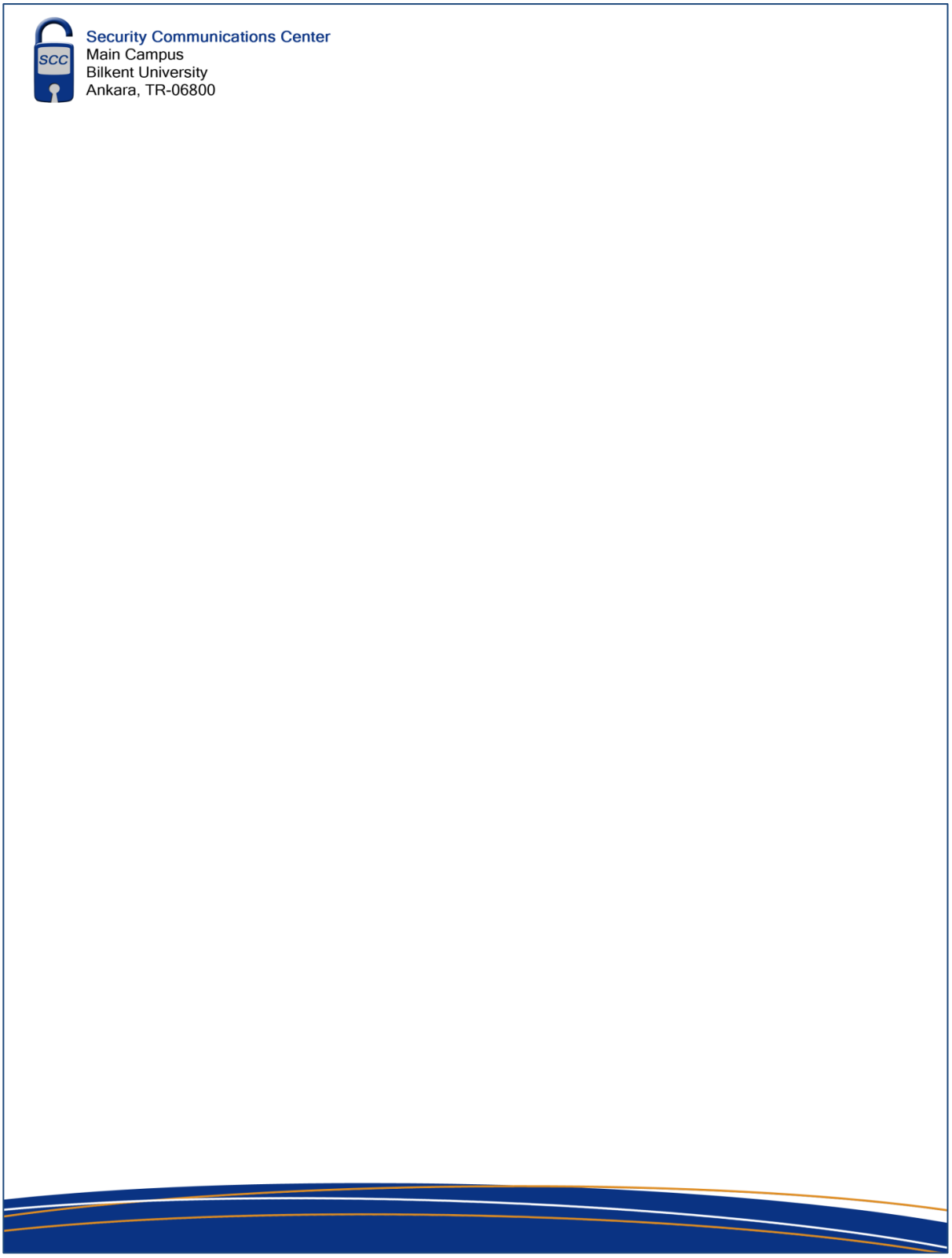


Figure 8 - Letterhead

Security Communications Center
Main Campus
Bilkent University
Ankara, TR-06800

Security Communications Center

18.12.2011

Didem Ozan

Asafa Ltd.

Dumlupınar Bulvarı

No:252

Ankara 06530

Dear Ms. Didem,

The first shipment of equipment from Asafa Ltd. has arrived. We are delighted with every piece. Therefore, we are decided to make our initial purchase larger than anticipated. I am attaching our purchase order no. 889945 for additional goods totaling list price $450.000.

Since you already have a copy of our Procurement Guidelines, I shall not attach them to this order. As before, we will establish a letter of credit. Please inform me of shipping dates.

Sincerely,

Mehmet Melih Değirmenci

Chief Finance Officer

Figure 9 – Prepared Letterhead

3.1.Corporate Identity

Every successful technological company knows what deficiencies of their market are. For Apple, lack of mobility in music players was striking deficiency to snatch the large market share. Our company mainly concurred with this logic as well and determined to satisfy the deficiency of security in the trendy market smartphones' accessories specifically in messaging and location tracking system.

Aim of the Secure Communications Center (SCC) Associates is to have the most of the share in the secure communication system on smart phones market in Turkey. The product we produce helps to military and police service via both secure messaging and location tracking. Any other companies who care about security are potential customers as well. Via this product, providing secure communication to the users is the main target. The benefits of the product are known but security problem hadn't been considered by any other producers. That differentiates us from others.

3.2.Company Name

"Secure Communications Center"

Our company is named "Secure Communications Center" shortly SCC. The name inspired by our distinctive characteristic secure. Since we are in communication sector and emphasizing security, the name should be firm and faithful. Initials type is considered as appropriate for the name.

3.3.Product Name

"Cher Ami"

Our product is named "Cher Ami" bird accepted as fourth heroic animal in history which has remarkable story behind it. Also, metaphorical features exist between the heroic bird and our product. Briefly, during World War I, On October 3, 1918, Charles Whittlesey and more than 500 men were trapped in a small depression on the side of the hill behind enemy lines without food or ammunition. However, with the help of pigeon Cher Ami, they accomplished to survive. First of all, both our product and Cher Ami bird used for communication even high level secure chips symbolize the distinguishing of

Cher Ami's security. As Cher Ami accomplished to provide communication between two groups, our Cher Ami aims to connect even more people to each other as well. If Cher Ami could not be secure enough, most probably 200 hundred people would die just because of lack of secure messaging. Similarly, as Cher Ami proved to be trustworthy, our product's one of the main characteristics put forward is trustworthiness. Since Cher Ami died and cannot be cloned, for secure messaging SCC's Cher Ami is the only option that is available for everyone. Additionally, Pigeon was very trendy and portable during World War I just as smart phones are in the same conditions today.

3.4.Company Logotype

The logo of our company is designed as shown on Figure 1, 2 and 3. We aimed to design a company logo which is simple and manages to display the main features of the company. It is obvious that we combined smart phone, key and key hole which symbolizes security. The open key symbol implemented just because of it suits nicely. When we close the key, it looks like almost keychain. Therefore, we preferred the open one. We also tried to use orange color but we did not appreciate it. In the logos and any other documents we used Microsoft Serif Sans type. Also we used same colors for both logos and blue-shape in the documents. The name of the company is also drawn on the screen. The blue is the prominent feature of logo because this color implies the security. Rectangle shape means safety and technology as well. Lastly we decided to use clean envelope for the front side of the envelope. We have designed four different types of logo in order to be used on letterhead, business cards and envelopes. These logos are displayed on the following pages.

3.5.Marketing Plan

Marketing Plan report has been prepared on the purpose of outlining the strategies of the Security Communications Center (SCC) Company in order to market our new and innovative information technology product "Cher Ami". Marketing Plan report is regarded as a crucial part of establishing our management operation strategies. It constitutes the utmost crucial part of our Business Plan together with the Organizational and Financial Plans.

Marketing Plan begins with a latest definition of product Cher Ami as a part of introduction. It has been decided that two different versions will be serviced in order to reach larger customer groups. Primary version will be only a software application which enables users to see their location and send messages to each other on Internet channels which are designed according to SSL 3.0 and TLS secure web communications protocols. Premium version also includes additional physical equipment which encrypts all the shared data in addition to the software package of the primary version.

Main feature of our product is its security. Therefore, we have focused on the customer groups who give uttermost importance to their communication security. At the end our analysis we have defined two target markets: governmental agencies and civilians who cares about their business or private communication security. Profiles of these customer groups and buying decision mechanisms are scrutinized. The steps of our analysis and its results are expressed in Target Market part of the marketing report.

According to the latest stage of our design and latest choices of the components, possible cost interval for the total cost of the items which will be used in the production of the hardware are analyzed. Other factors such as transportation, storage and production costs are also discussed. Together with the results of the cost analysis; critical for the revenue model, price ceiling and floor, pricing methods and strategies are examined. Results of these evaluations are given in the Price part of the report.

Under Distribution Channels subheading, the natures of the marketing channels to deliver our product to customers are discussed. As it has been stated above, we have targeted governmental and civil markets which are heavily separated characteristics which also reflect into distribution channels. Selected distribution channels are clarified in this part with their advantages over other possible choices and constraints comparing to other alternatives.

Successful advertising and public relations have vital importance for us. SCC is an emerging company with an innovative in the large information technology market; therefore, we need to determine promotion strategies. Our brochure samples, national and international exhibitions and fairs which can enable us to publicize our company and product in the sector, advertising strategies on Internet and mass media are discussed under Promotion subheading.

We could not find another product which services the same features that Cher Ami have. However, it is possible to find different secure communication companies. These competitors, their products & services are presented under Competition part. Furthermore, we have also expressed their positions in the market, prices, and features in comparison with Cher Ami.

Lastly, in sales strategy part, we are going to analyze especially who will do the selling. This question is answered partly in distribution channels by explaining how we choose the seller and how we decided it. Technical and logistic support will be clarified. After sale, technical guarantee service will be provided by our company.

4. Developments in The Project

4.1. Product Overview

Secure Messaging and Location Tracking project can be called as a messenger program being run on smart phones (Android operating systems) and having the feature of enabling users to see the positions of each other on a map. All the information shared within the group is encrypted.

In this project, a portable cryptographic device, which encodes the data sent from the mobile device, will be designed. Public key encryption algoritm will be used. The connection between the cryptographic device and mobile phone is done through Bluetooth technology.

A user interface, which displays the locations of the other users on a map, is designed. The location information is read from the integrated GPS chip inside the smart phone. Obtained coordinates are interpreted and users are demonstrated on the map with symbols. This user interface also enables the user to send and receive encrypted messages via this application. Together with the location information, the

plaintext is sent to the cryptographic device via Bluetooth. Encrypted information is transmitted to the other users via a HTTP Server application.

The received and transmitted messages are stored during the session. Last few locations of the users are also stored internally in the program in case of a GPS or Internet connection loss. In such unexpected emergency cases, other users who still have the connection can reach the last location of the user who has lost his connection.

4.2. Software Development

The project has two main ingredients which are software and hardware. In the software part as its proposed GUI part of the application is mainly completed. In addition to give an idea of flow of events between database and application, some data read-write operations are done in local host using Sqlite Database that is default database installed in android mobile phones. Application will be run on an emulator from a laptop. Since application is will not be shown via mobile phone GPS locations will not be caught instead few people with random GPS locations will be shown for illustration purposes.

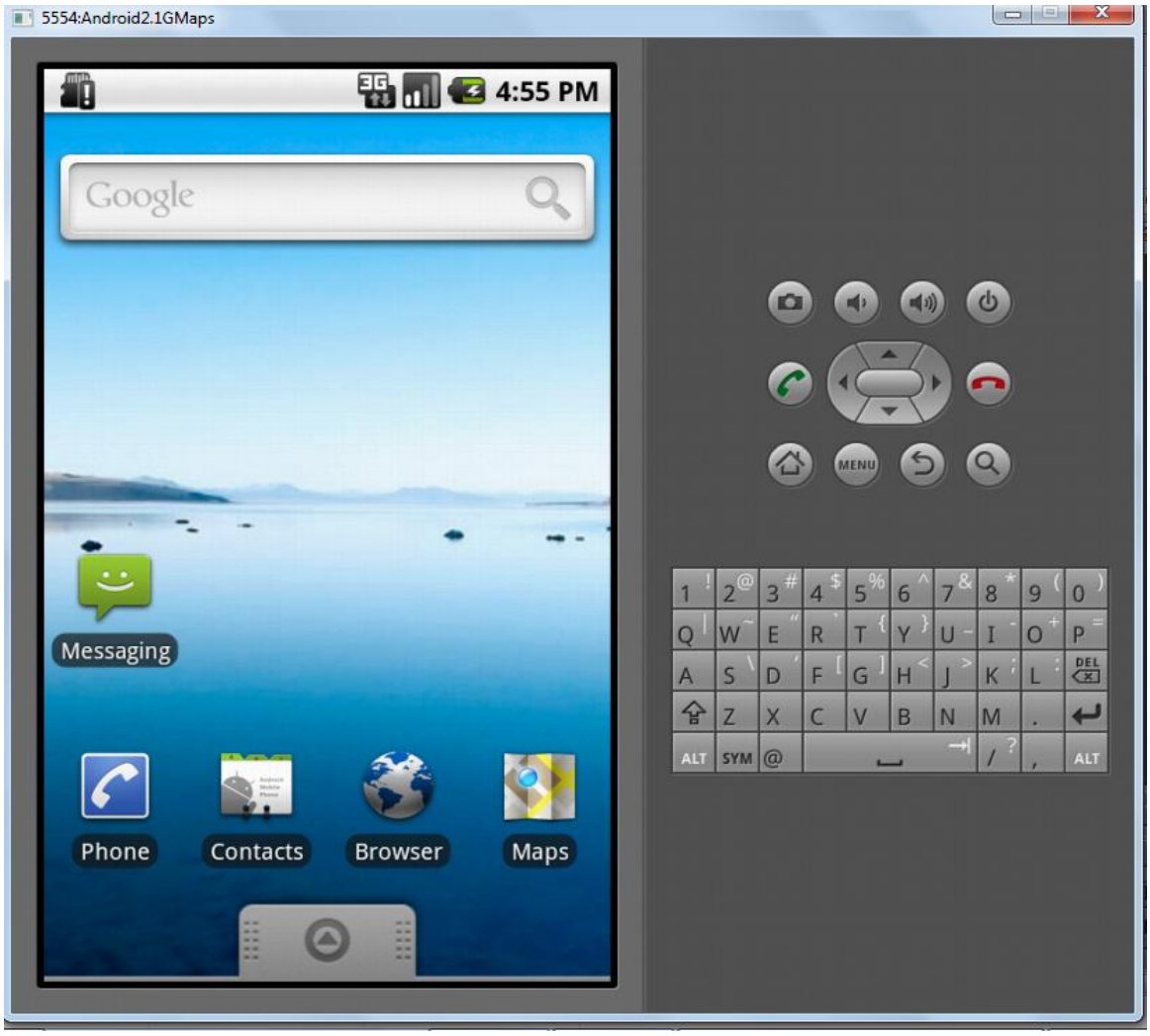


Figure 10 – Screenshot of Emulator

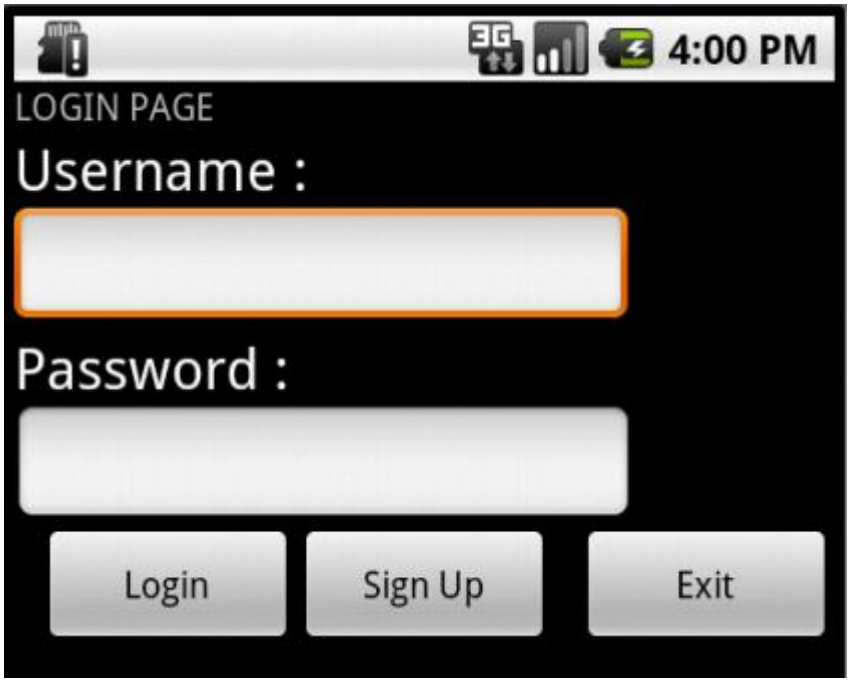


Figure 11 – Screenshot from Login Page

At the beginning of the application users encounter with Login Page as shown in figure above. Users are able to login, sign up or quit the application. If a user is not registered into system while tapping sign up button he is directed to Signup Page. If user's username and password is match in other words username-password combination exists in database user successfully login to system and forward to Map Page.

Figure 12 – Screenshot from Signup Page

In signup page user are asked to fill out name, surname, username, password, age, gender, e-mail and address information besides they need to add a profile photo to be used in the system. To be able to show in demo information can be taken from text boxes and hold, data is hold in Sqlite Database in localhost at the moment. Currently no character type and length checking is done for name, surname, username and for such kind of information in which some inspection is necessary.

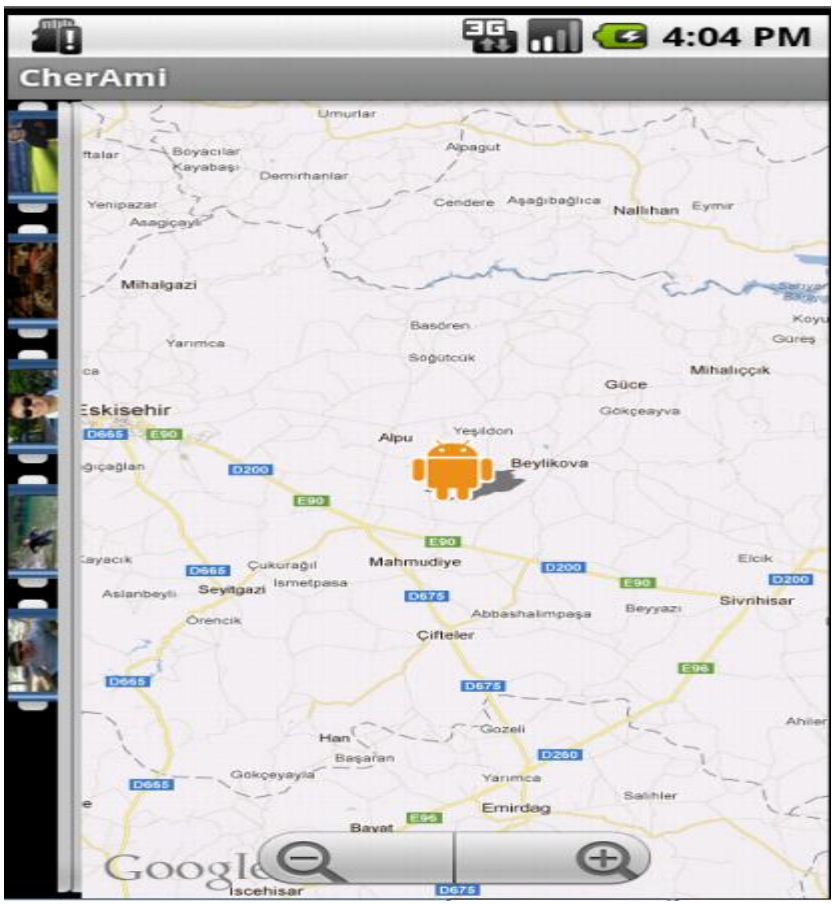


Figure 12 – A screenshot which includes application map

After successfully login into system, own GPS location of user is centralized on the map and with orange colored figure he is represented. In the meantime, name of the application is CherAmi and it's written at the top of all pages in the application except login page.

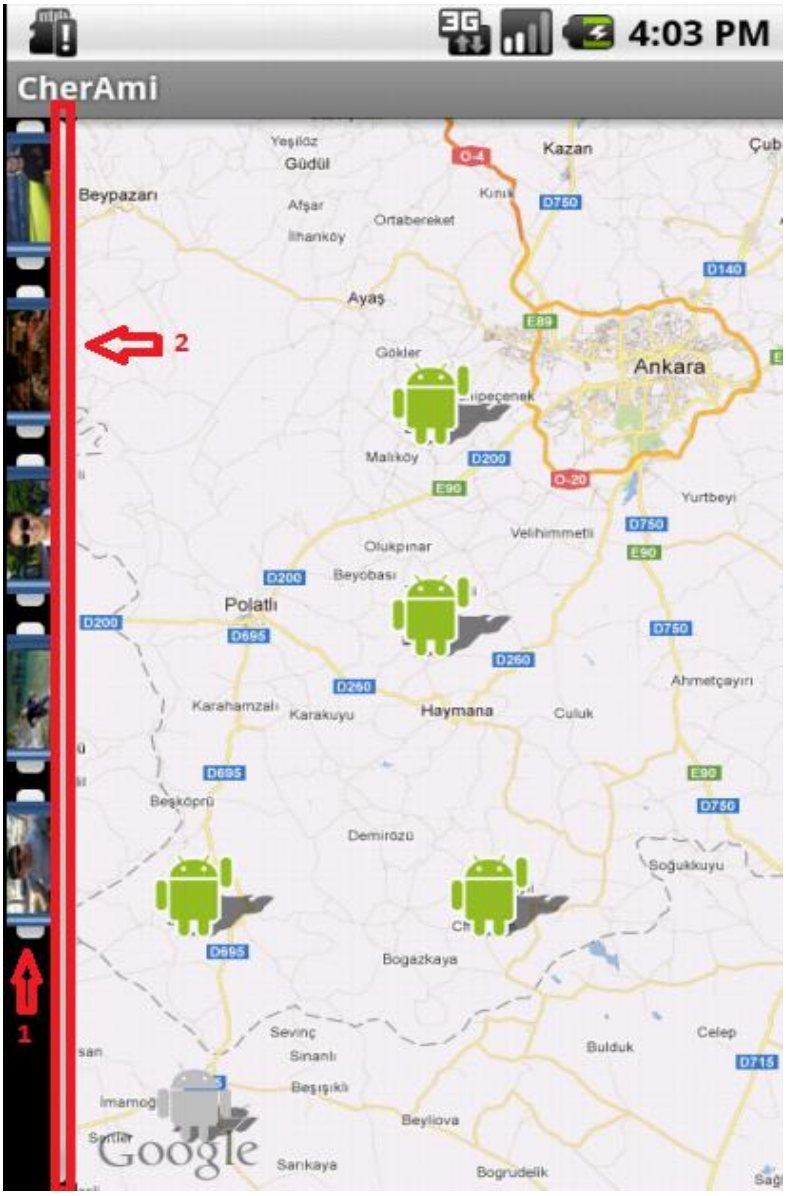


Figure 13 - Another screenshot which includes application map

Figures with other than orange color represent other users. Green colored figures are online users and gray colored figures are offline ones. Users are able to focus on a friend by clicking any pictures located at the left side of the screen (1). While focusing on a friend, program also optimizes zoom settings to clearly show requested person. By clicking thin button located next to pictures at the left most, message screen is opened (2) which will be represented after following figure.

Figure 14 – A screenshot of Map Page from distance

Using zoom in and zoom out buttons, users are able to adjust distance until allowed level.

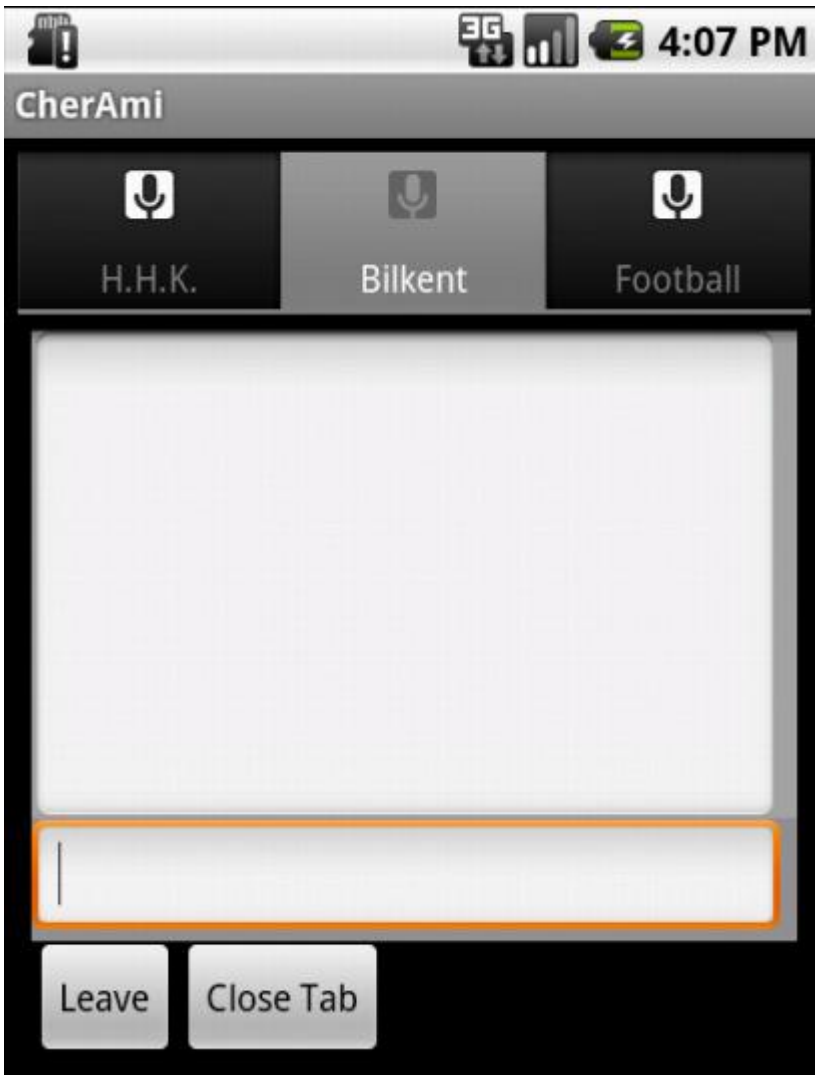


Figure 14 – Screenshot from Message Screen

User will be able to communicate securely via messages from the page indicated in above figure with a friend or friends within a group if he joined any group before. Since currently no mobile phone connection between different users is established user is not able to send messages. User is able to select to whom he want to speak through opening different tabs. Tabs are represented with names which can be a name of friend or group name. In addition user can terminate communication any time by tapping close tab button at the bottom of the screen.

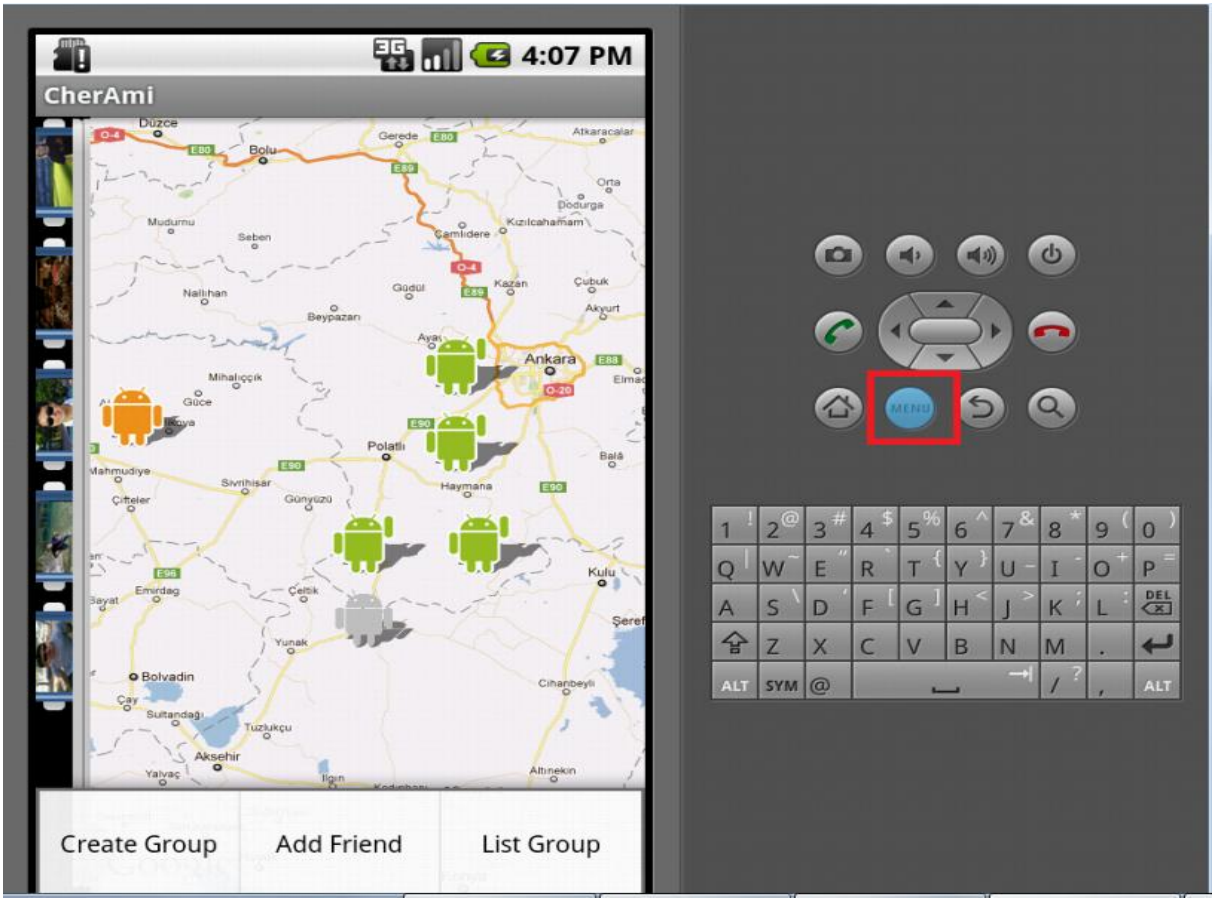


Figure 15 – A screenshot from application to show menu

At any time while Map Page is open user can open menu by pressing menu button which is surrounded with a red rectangle. At the moment create group, add friend, list group options are available. When a user create group he will be the only person in that group until some join into that group and he will be the manager of that group who will have permission to delete group. Group has name and logo if developers let it to be. Users add friend from this menu while entering name and surname of their friends. Friend request will be shown on the counter side as notification and if request is accepted by other user, both users are assigned as friends. Add friend option is currently not available. List group option lists groups that user created or joined. After tapping list group option user is encountered with new dialog which lists names of groups he belongs to as indicated in the figure below.

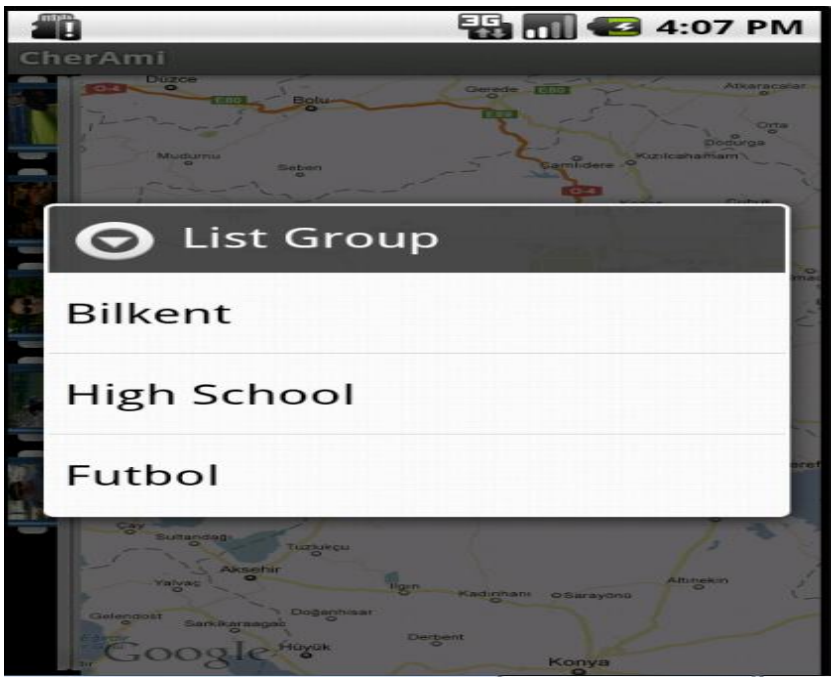


Figure 16 – Screenshot of list of groups that user belongs to

After selecting a group from group list user is directed to inside of that menu. Meanwhile when user is in these two pages, he is not allowed to interact with Map Page to sustain progress in healthy way. User is able to add group members to his message page and start communication by tapping messaging button. He can leave from screen by using close button or quit from group with the respective button. If user is also the creator of that group, group is deleted forever.

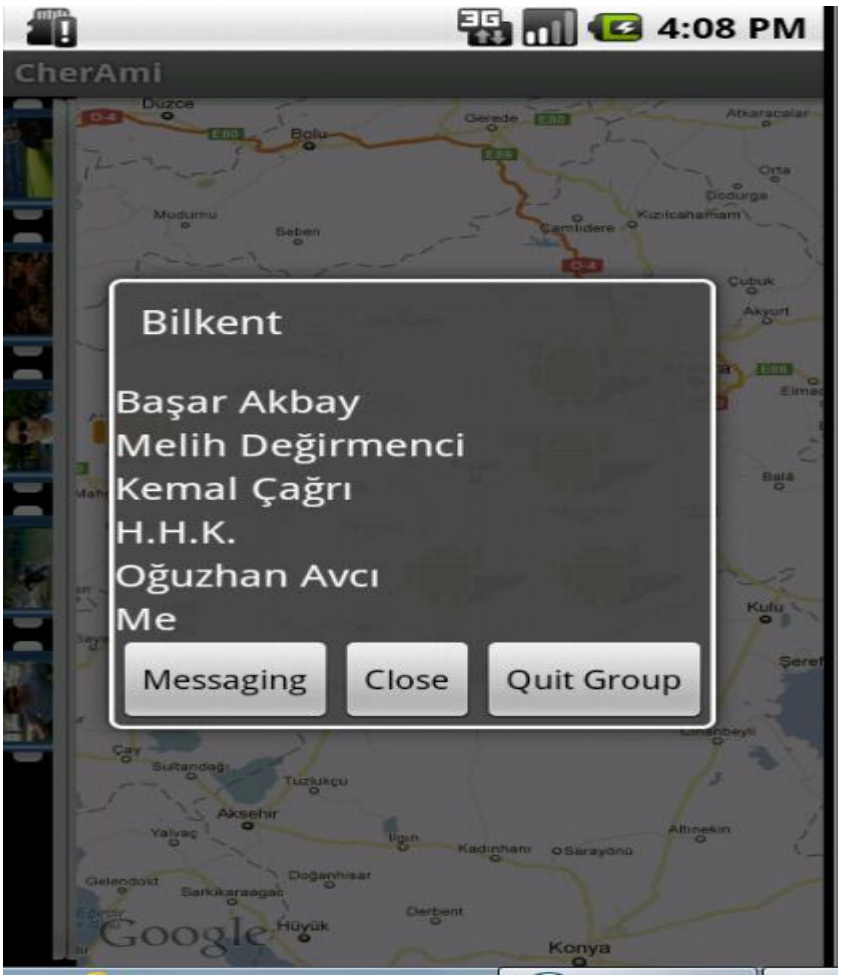


Figure 17 – Screenshot from inside of an example group

5.3. Hardware Development

In the hardware we have two important parts Bluetooth connection with android mobile phones and encryption in a Bluetooth device. Encryption on hardware left to the second semester. For hardware part, we will show that connection we have established between Bluetooth device and laptop in demo. Bluetooth device of Texas Instruments will be used which is represented in the figure below.

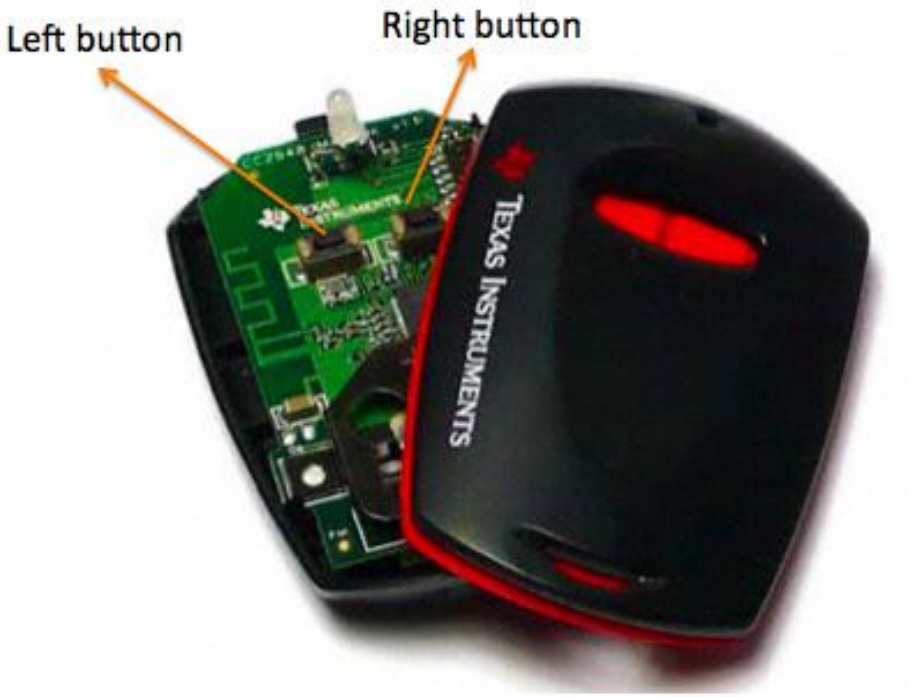


Figure 17 - CC2540 Bluetooth Key fob

Device uses COM5 port to send and receive data from laptop. We developed GUI component to done our job easier. Available COM ports are selected from combo box then connect button is pressed start connection. It takes some time to create connection. After connection is established, if key notification is open application receives input that came from Bluetooth device if not it's not possible for Bluetooth device to interact with the application. Key notification can be on and off via pressing buttons key notify on and key notify off buttons respectively as indicate in the figure below.

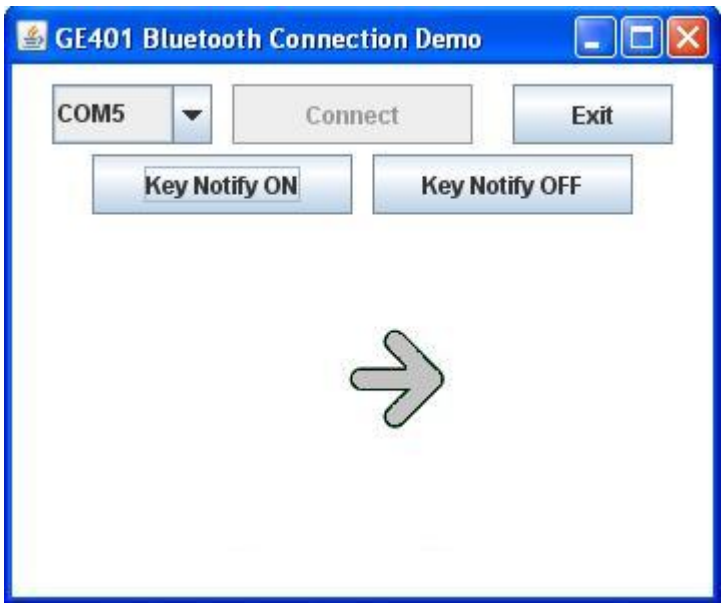


Figure 18 – One second after right button released and also initial state

Whether left button is pressed or right button is pressed is indicated by arrows. Green arrows indicate that left or right button is pressed soon (0 – 1 sec) and gray arrows indicate that at least 1 sec is passed after a button is pressed. At the beginning of the application arrow which is directed to right with gray color is shown. If user presses right button, it becomes green and the text “right button pressed” is also shown below that arrow. Same procedure applies for left button also. Screenshots from application GUI is represented in figures below.

Until the writing of this report, a decisive development in the implementation of RSA Algorithm has not been achieved. Some modules such as modular addition, modular multiplication and modular exponentiation which will have take place in the construciton of the algorithm has been written and simulated. However, these codes and results have not been included in this report. After some more developments, technical details related with the RSA Algorithm implementation will be provided in the EE Progress Report.

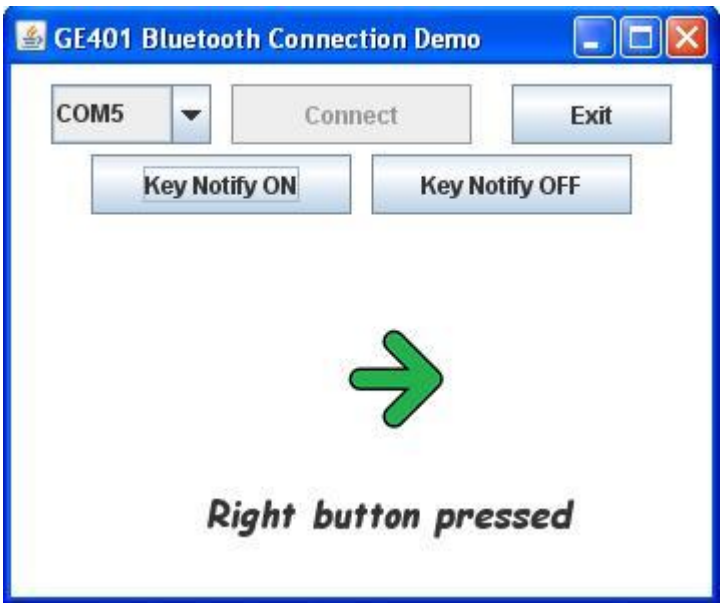


Figure 19 - When right button is pressed

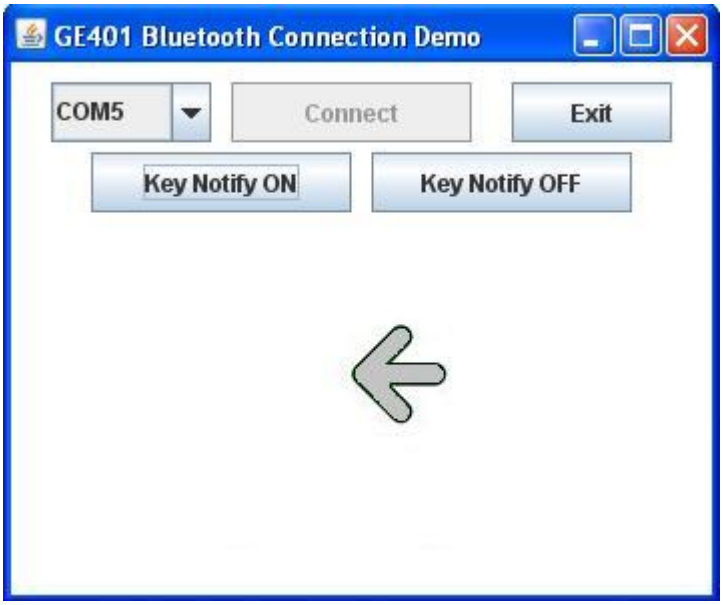


Figure 20 – One second after left button released

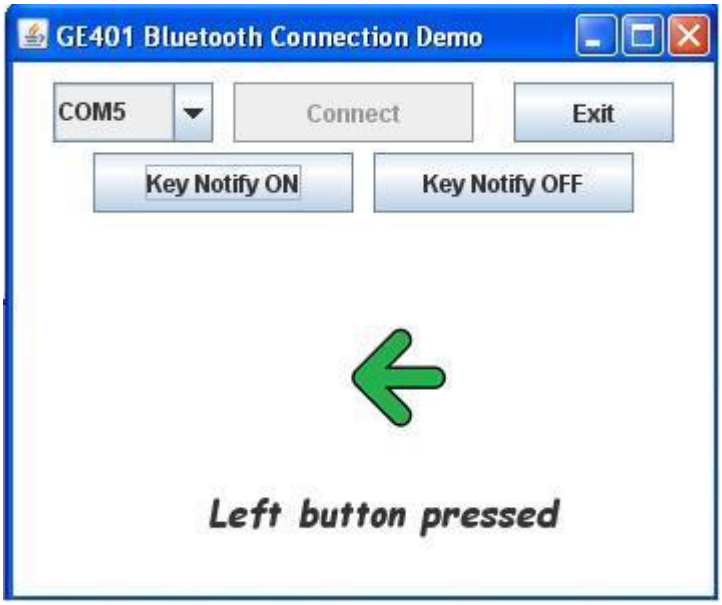


Figure 15 - When right button is pressed

5. Professional and Ethical Issues

In this report, the company's intellectual property and professional development policy has been explained. Intellectual property policy comprises both the protection of the intellectual property which are produced by SCC and avoidance of the violation of the secondary companies' or persons' rights. The SCC gives utmost importance to the professional development of its employees to enhance the quality of the work performance and outputs of the company. Furthermore, SCC believes in that enabling its employees to participate in activities and provide them necessary educational where the conditions are mutually agreeable for both sides are responsibilities of the company for its employees.

5.1 Intellectual Property Policy

The term "Intellectual Property" stands for the outputs of creative endeavor in literary, artistic, industrial, scientific and engineering fields, which can be identified and protected under legislation relating to patents, plant breeders rights, trade marks, copyright, and design rights. Of the different forms of intellectual property, patents for new technology are of prime interest to scientists and engineers, although copyright can also be important (for example, for the protection of computer software). Secure Communications Center (SCC) is Turkish R&D&I (Research-Development-Innovation) company authorized to find effective and secure solutions relating to communication systems since September 2011. This document reflects the decisions that have been made to promote effective utilization management and exploitation of Intellectual Property and determine outline of how the policy should be consulted. The motivation behind ethical issues report is to designate our company's Intellectual Property Infringement Policy which emanates from the innovative and developing structure of our company. Since our company produces an original and newly created commodity, the Intellectual Property rights of it should be well defined and protected (from illegal usage of any SW&HW related solutions and to be used illegally by other institutions/companies). The outline and visualization of the activities related to Intellectual Property Rights and Intellectual Creation Cycle manifested by SCC in October 2011 will be reported in this document.

5.1.1 Software IP Policy Decisions

Although there are several types of Intellectual Property, SCC concerns center on two of them: patent and copyright. When the definitions for both of them are analyzed, computer programs fall into gray area

between these two types of Intellectual Property such that: programs that are a part of any new and useful process (machine, manufacture, etc.) are eligible for patent management and programs that contain minimally original terms are eligible for copyright management.

Standards or Regulatory Work – SCC ensures that Intellectual Property (IP) generated from such work does not allow one particular supplier to establish a monopoly in supplying Software (SW) programs, functions and algorithms required to meet the standard or regulation;

Improvements to Health and Safety – As a result of SCC's mission, the entertainment and security benefits stemming from software-based (funded) activities must be promoted and exploited in preference solely to the commercial exploitation of that work;

Dissemination of Information -- The complete divulgence of information generated by SCC SW team is a requisite in order to have transparent successive decisions and/or IP policy addressed or regenerated.

Aggregation of Work – Since the computer programs are not only some big modules but are part of an aggregation of work taken in charge by a number of developers (actually they are also providers) and the IP is best exploited at the aggregate level, SCC ensures its freedom to use alternative sources of supply for related part of a hardware programming or a pure software program and to make IP from earlier programs freely available especially in Android market and as some other open source hardware development programs or algorithms (for Bluetooth connection and FPGA programming).

Developer and/or Provider Resources – SW developers and/or providers do not have the resources to preserve and make use of IP that is established, or may refuse to take ownership.

5.1.2 Hardware IP Policy Decisions

The hardware parts of the Cher Ami include Bluetooth Transceiver module, FPGA Chip and power supply circuit. Power supply is driven by the National Instruments LM3370 Dual Synchronous Step-Down DC-DC Converter with Dynamic Voltage Scaling Functions. FPGA Chip is chosen from Altera Semiconductors Cyclone Family. Bluetooth transceiver module is Texas Instruments CC2540 2.4GHz Bluetooth Low Energy System-on-Chip Solution. The interfaces are designed according to the information provided in the user manuals and datasheet of the manufacturers. These designs have been provided in the EE Progress Report, Preliminary Design and Subassembly Specifications Report. These designs are actually the recommended settings and are applied into the Cher Ami project.

At the end of January 2012, the Hardware group plans to implement the project on the development kits level. In the implementation of the Bluetooth connection, Texas Instruments CC2540 mini development kit will be used. The reception and transmission processes are being driven using Java software written by the developers of TI CC2540 mini development kit. At this level, SCC Hardware engineers used this code and modified it for development. This code is a part of the kit for new developers and provided for the customers of the development kit which is SCC in this case. Therefore, hardware engineers do not regard benefiting from these codes in order to increase the knowledge and experience as an unethical act or the violation of the Texas Instruments' rights. Furthermore, copyright of this software is certainly covers the unauthorized usage as a violation. However, copyright laws cannot protect the algorithms, the logic behind the code. In the development of the driving codes and (circuits if it necessary) for Bluetooth transceiver, the open documents of Texas Instrument corporation will be used. If they prohibit the direct usage or protect the software; SSC Hardware engineers regard these documents as sources to develop their own codes. As it has been indicated before, copyright laws do not prevent the deduction and the

application of the algorithms if the company allows developers to examine the software. However, if the software or the algorithm is patented; it certainly prevents its unlicensed usage. This is not a very common situation; however, it may be encountered. In such cases, the violation of the laws will be certainly avoided and intellectual property will be well respected by simply not using such software or buying them.

RSA Cryptology algorithm will be implemented on the FPGA Chip as the decryption / encryption block. MIT's RSA Algorithm patent expired in 2001[1]. Therefore, examination and implementation of the algorithm is open for everyone. However, the algorithm itself is not solely sufficient for the efficient implementation. SCC hardware engineers have to work on the additional algorithms for spatially and temporally efficient and sufficient working of the product. This requires extensive literature survey. Indeed, this process has been continuing from the definition of the product at the beginning of the semester. Primary sources are the papers which have been published in academic journals. Such references are indicated in the technical documents such as EE Progress Report and Preliminary Report. These are open sources and can be used freely for commercial applications. They do not include the software codes; but, the descriptions and presentations of the algorithms. In addition, it is possible to find VHDL codes for the implementation of RSA algorithm. In general, these codes are written by educational or noncommercial purposes. Therefore, they cannot be used directly. Some of them have GNU license which strictly prohibits the commercial usage. However, similar to the Bluetooth drivers, these codes can also be regarded as examples and they are only subject to the analyses.

In Turkey, selling cryptographic devices is subject to some rules. It has been issued in the *"Kamu Kurum ve Kuruluşları ile Gerçek ve Tüzel Kişilerin Elektronik Haberleşme Hizmeti İçinde Kodlu veya Kriptolu Haberleşme Yapma Usul ve Esasları Hakkında Yönetmelik"* [2]. Turkish Law requires share of the

cryptology algorithms with Turkish Information Technologies Authority from the companies which provide security communication products. The related part of the regulation is given in the appendix A (In Turkish). As the law requires, the final encryption algorithm and the technical features of the device will be shared with the Turkish Information Technologies Authority.

The Cher Ami project hardware component cannot be regarded as an invention. Therefore, protection of the SCC's rights on the hardware component through granting patent is not regarded as the most suitable way. However, the Bluetooth driving codes and the RSA implementation algorithm can be protected under copyright rights.

5.2 Professional Development Policy

SCC highly cares about the professional development of its employees. In the accordance with its motto of the pursuit of the excellence, SCC regards professional development as an opportunity for its employees to increase the abilities and technical/nontechnical background of its staff. Furthermore, SCC needs employees who believe in the necessity of improving him/herself in order to meet the evolving requirements of the market and the organization. SCC is aware of that professional development is highly correlated with the personal job satisfaction, realizations of the missions and improvements of the current quality.

Under the decree of the Chief Executive Officer, employees can attend technical or nontechnical conferences, seminars, workshops and short courses. SCC will be fully responsible for all costs; if, this program is decided as necessary for a staff member for a particular skill or feature. SCC highly encourages research works of its employees and highly promotes to write academically valued papers related with the employee's job description. The same policy also applies on the attendance to formal studies or participation in industry visits, subject meetings, courses and programs.

When the employee desires to involve in a professional development activity which is not required or is decided that the particular skill is not necessary for the employee by the CEO of the company, SCC efforts to provide the following possibilities under the discretion of the CEO:

- SCC is open to discuss temporary or permanent rearrangement of the working hours.
- SCC may permit the usage of its facilities and equipment if this does not cause any delay or problem in the regular work stream and they are free during such a usage.

Proposals for professional development

Employees shall be encouraged as part of the performance review process to take an active role in their own ongoing professional and career development and to apply their learning to its most effective use.

6. The Expected Impact of Project

6.1. Possible Impacts of the Project at a Global Scale

With this project, we aim to make the world, the countries and the people communicate more comfortably by providing a device that will ensure a reliable and secure communication. The users of the device will be able to communicate in a group whose members will be determined by themselves in any place in the world without any wiretapping concerns. As the project will be available globally, all people in the world will be our potential customers. Furthermore, this project will have a potential significance for military applications in different countries. For instance, in secret operations, our device will enable secure communication among its users, in this case, which happens to be the soldiers. Moreover, our product is also a promising technology for constabularies of countries. Our device will also have functionalities for daily use as well. Individuals will be able to locate and track the users of their

customized groups.

6.2. Possible Economic Impacts

Each year trillions of dollars are spend on military and security services. By the help of our project, the operations conducted by the military and police forces will have more accurate results with less effort allocated for secure communication and location tracking. For instance, our country, Turkey, has approximately 10 billion dollar budget for Ministry of Defense for 2012. After the project is started being used, it is expected that there will be considerable amount of decrease in the expenses concerning military operations. Then the funds that will be saved from this gain, can be reflected to the public services of the country, e.g., health, education and transportation services.

6.3. Environmental Impacts

While designing our device, we tried using components, which last longer with low power consumption. For example, we chose to use Texas Instruments' Bluetooth low energy technology in order to lessen the overall power consumption; hence we designed our hardware with respect to Texas Instruments' CC2540 Bluetooth Low Energy Chip.

6.4. Societal Impacts

It is usually very difficult to keep track of excessive amount of people while travelling, particularly in the airports, it is a hustle to locate everyone's location. By the help of our product, this problem will vanish resulting in making people travel more often safely without any concern. Furthermore, with our device, parents will be able track their children's location from anywhere on their smart phones easily.

7. Conclusions

It is achieved to use Google Maps API in our program to show gps location on map. However, in order to use Google Maps API on android, Google forces to get a certificated key. This certificated key is free for development usage. This certificated key is acquired via g-mail account. The Bluetooth module is also in action and it is tested by generating GUI for it. By means of this GUI two leds on the Bluetooth is controlled by a computer program. RSA Cryptology algorithm is also implemented partly but not fully. It is apparent that this algorithm will cause a lot of work for encryption algorithm developers for FPGA. The hardest part of the project seems to be the connection part which will enable us to send raw data and get encrypted data.

For software part user icons, login screen, message dialog box, some other menus and some visual items have been added. Add/join group menu interface is available but it will not be applicable until next semester because the network part is only locally established. Message dialog box will be seen on the screen but not functional. Distance between two different users will be calculated and can be seen on the screen.

Towards the end of May 2012, it is planned to establish network communication module of the system, create database and integrate the software with hardware components.

How the software and hardware developments are enhanced step by step in detail by means of documentation is observed. We possess the chance of evaluating whether what we have planned is correct and reachable. The steps which will be done until the end of project are analyzed and determined.

Expected Difficulties in the Project Development Process:

Difficulty: Gps data may come later than expected time.

Solution: Gps data is planned to be sent in every 10 seconds. Time delay is acceptable.

Difficulty: Battery of encryption device is run out

Solution: Data will be encrypted via software based encryption method.

Difficulty: Battery of smart phone of a user is run out

Solution: His location can be determined by looking last 10 locations of that user.

Difficulty: Gps data may not be accurate enough. Gps may not work properly in every place.

Solutions will be produced until program is released

8. Appendices

8.1. Changes in the Product Definition (if any)

There are no reasonable changes in the product definition, requirements or specifications for now. Only some unknown and unclear points are clarified, such as GUI decisions of software part and algorithm decisions for encryption device.

8.2. Other Appendices

İKİNCİ BÖLÜM

Kodlu veya Kriptolu Elektronik Haberleşme Hizmetleri İçin Başvuru, Değerlendirme, İzin İşlemleri, Emniyet ve Muhafaza Tedbirleri

Başvuru

MADDE 5 – (1) 5809 sayılı Kanunda belirtilen istisnai kurumlar haricindeki tüm kamu kurum ve kuruluşları ile gerçek ve tüzel kişiler bu Yönetmelik hükümlerine aykırı olmamak kaydıyla kodlu ve/veya kriptolu haberleşme yapabilir.

(2) Kodlu veya kriptolu haberleşme cihaz/sistem ithal veya imal edilmesi üretici tarafından yapılır. Üretici, imal veya ithal edeceği cihaz/sistemlere izin alabilmesi için;

a) İzin başvuru yazısı,

b) Kurulması planlanan haberleşme sisteminin türü (kara, deniz, hava, uydu) ve sistem özellikleri dikkate alınarak talep sahibi tarafından doldurulup imzalanmış iki nüsha ilgili Kurum Başvuru Formu,

c) Kullanılan kripto tekniği/cihazı ile ilgili belgeler ve kullanılacak elektronik haberleşme sisteminin teknik özellikleri,

ç) Kripto algoritması ve anahtarı, anahtar üretme, dağıtma ve yükleme modülü/cihazı, bu amaçla kullanılan tüm yazılım/donanım, gerektiğinde şifrenin çözülmesine imkân tanıyan yazılım ve/veya donanım,

d) İki adet cihaz numunesi, var ise opsiyonel yazılımlar/donanımlar, aksesuarlar, ihtiyaç duyulması halinde bu cihazların testinde kullanılacak özel aparatlar,

e) Gerçek ve tüzel kişilerden; Ticaret Odası belgesi, Sanayi Odası belgesi, Ticaret Sicil Gazetesi örneği, dernek tüzüğü veya bunlara benzer bir faaliyet belgesi,

f) Gerçek ve tüzel kişileri temsile yetkili kişilerin imza sirküleri,

g) Tüzel kişileri temsile yetkili kişiler ile gerçek kişilerin adli sicil belgesi,

ğ) 24/3/2007 tarihli ve 26472 sayılı Resmî Gazete'de yayımlanan Telsiz ve Telekomünikasyon Terminal Ekipmanları Yönetmeliği (1999/5/AT) kapsamında yer alan cihazlar için aynı Yönetmeliğin Ek-2'sinde belirtilen teknik dosya içeriği,

ile birlikte Kuruma başvurur.

Değerlendirme

MADDE 6 – (1) Kodlu veya kriptolu elektronik haberleşme hizmeti cihaz/sistem üreticisinin başvuruları; telsiz sistemleri bakımından 17/7/2009 tarihli ve 27291 sayılı Resmî Gazete'de yayımlanan Telsiz İşlemlerine İlişkin Usul ve Esaslar Hakkında Yönetmeliğe, cihaz/sistemlerin piyasaya arzı, dağıtımı, piyasada bulunması ve hizmete sunulma aşamalarında ise Telsiz ve Telekomünikasyon Terminal Ekipmanları Yönetmeliğine (1999/5/AT) göre değerlendirilir.

(2) Üretici veya üretici firmayı temsilen imza yetkisini haiz kişilerin adli sicil kayıtlarında Devletin ülkesi ve

milletiyle bölünmez bütünlüğüne, Cumhuriyetin temel ilkelerine ve devletin güvenliğine karşı suçlar, Anayasal düzene ve bu düzenin işleyişine karşı suçlar, milli savunmaya karşı suçlar, Devlet sırlarına karşı suçlar ve casusluk, zimmet, irtikâp, rüşvet, hırsızlık, dolandırıcılık, sahtecilik, güveni kötüye kullanma, hileli iflas, ihaleye fesat karıştırma, edimin ifasına fesat karıştırma, suçtan kaynaklanan malvarlığı değerlerini aklama veya kaçakçılık veya 12/4/1991 tarihli ve 3713 sayılı Terörle Mücadele Kanunu kapsamındaki suçlardan mahkûm olma durumu var ise yapılan başvuru reddedilir.

(3) Kamu kurum veya kuruluşları ile gerçek ve tüzel kişilerin yurtdışından yolcu beraberinde veya kesin dönüşte getirilen veya bireysel olarak ithal edilen veya posta ile gelen kodlu veya kriptolu haberleşme cihaz/sistemlerine, bu cihaz/sistemlere ait kod veya kripto anahtarlarının Kuruma teslim edilmesi halinde, kullanma ve kurma izni verilebilir. Kurumdan izin alınmadan yapıldığı tespit edilen kodlu veya kriptolu haberleşmeler iletişime kapatılır ve ilgililer hakkında suç duyurusunda bulunulur.

(4) Üretici tarafından yapılacak başvurularda ilgili mevzuata uygun görülmeyen kodlu veya kriptolu cihaz/sistem başvuruları reddedilir.

(5) Kurum tarafından ihtiyaç duyulması halinde kodlu veya kriptolu elektronik haberleşme sistemlerine ilişkin olarak bu konuda ihtisaslaşmış kuruluşlarla işbirliği yapılabilir.

(6) Yabancı devletlerin Türkiye'deki diplomatik temsilciliklerine münhasıran kendi hükümet merkezleri ile haberleşme yapmak veya kendi iç güvenlik amaçlarıyla kullanmak üzere karşılıklılık esaslarına bağlı olarak kodlu veya kriptolu elektronik haberleşme sistemi kurma ve işletme izni ile ilgili her türlü işlemler Dışişleri Bakanlığı tarafından değerlendirilir.

(7) Kamu kurum ve kuruluşları tarafından kullanılan kodlu veya kriptolu haberleşme sistemlerinde tasarımı ve üretimi Türkiye'de yapılan milli kripto cihazlarının kullanılması esastır.

İzin

MADDE 7 – (1) Kodlu veya kriptolu elektronik haberleşme hizmeti başvuruları Kurum tarafından değerlendirilir. Başvurunun kabul edilmesi durumunda kod veya kripto Kuruma teslim edilir ve üreticiye izin verilebilir.

(2) Herhangi bir işletmeci tarafından işletilen elektronik haberleşme sistemi altyapısı kullanmayan bina, depo, garaj gibi lokal alanların içerisinde kodlu veya kriptolu haberleşme yapan sistemlere izin alınmasına gerek yoktur.

(3) Üretici, kamu kurum ve kuruluşları ile gerçek ve tüzel kişiler, sahip olduğu kodlu veya kriptolu elektronik haberleşme sistemlerine ilişkin olarak Kurumdan izin almadan cihaz/sistemlerin teknik özelliklerinde donanım ve yazılım bazında herhangi bir değişiklik ve tadilat yapamaz. Yapılacak her türlü değişiklik ve tadilat işlemleri Kurum onayı ile yapılabilir. Cihaz/sistemlerin teknik özelliklerinde herhangi bir değişiklik ve tadilat yapıldığının tespit edilmesi halinde cihaz/sistem iletişime kapatılır ve ilgililer hakkında suç duyurusunda bulunulur.

Emniyet ve muhafaza tedbirleri

MADDE 8 – (1) Kodlu veya kriptolu elektronik haberleşme cihaz/sistem kuran ve işleten kamu kurum ve kuruluşları ile gerçek ve tüzel kişiler, sistemlerinin yetkisiz kimselerin eline geçmesini ve yetkisiz kişilerce kullanılmasını engelleyici muhafaza tedbirlerini alır.

(2) Üreticiler tarafından Kuruma teslim edilecek olan kodlu veya kriptolu elektronik haberleşme cihaz/sistemlerine ait kod veya kripto algoritması ve anahtarları Kurum tarafından muhafaza edilir.

9. References

[1] Patent US4405829 - Cryptographic Communications System ... - Google Patents." *Google*. Web. 02 Jan. 2012. http://www.google.com/patents?vid=4405829

[2] http://www.tk.gov.tr/mevzuat/yonetmelikler/dosyalar/Kripto_Yonetmeligi.pdf.

[3] Intellectual Property and Software - Software and Intellectual Property Rights." *DoD Journal of Software Technology*. Web. 02 Jan. 2012. <http://journal.thedacs.com/issue/45/110>.

DESCRIPTION		ADDITIONAL DESCRIPTION		PART NO
APPROVAL	PREPARED BY	LANGUAGE	DATE 03.01.2012	UNIT
DOCUMENT TYPE	PAGE 40	TOTAL PAGE 40	REVISION	LOGO