The structure of the secure cross-platform VoIP service for business customers

Sergei Kryltcov[1][0000-0002-2137-0487], Alexei Machovikov[2][0000-0002-6306-2060], Pavel Tcvetkov[3][0000-0002-3049-7893]

[1] Department of General Electrical Engineering, Saint-Petersburg Mining University, 199106 St. Petersburg, Russia;
kryltcov@outlook.com
[2] Department of Informatics and Computer Technology, Saint-Petersburg Mining University, 199106 St. Petersburg, Russia.
amakhovikov@spmi.ru
[3] Department of Informatics and Computer Technology, Saint-Petersburg Mining University, 199106 St. Petersburg, Russia.
pscvetkov@spmi.ru

Abstract. The paper addresses issues of development of secure and reliable Voice over IP solution and delivering it to the corporate customers. During the study, key requirements to the VoIP solution suitable for business sector were indicated. Two major disadvantages of existing proprietary solutions for business sectors were noted – lack of control over transmitted information and both hardware and software vendor lock-in. On the other hand, open-source solutions are not yet versatile enough to meet constantly growing business requirements for the voice and messaging services. Therefore, the new VoIP software solution was developed to meet indicated requirements for business sector. The unique feature of the solution and possibility to deploy whole client-server architecture of the VoIP solution entirely on the customers equipment, therefore providing minimal latency and full control over the voice and messaging traffic. The solution is currently undergoing tests in Russia and Canada. Preliminary results of the tests show ease of deploy and high quality of the VoIP service, that indicates such infrastructure as viable solution for the business sector.

Keywords: VoIP, Unified Communications, Telecom.

1 Introduction

The information revolution let to the significant changes in both economic situation and business processes within enterprises. Profit-making activities of the companies has been greatly shifted to the sales and service sector of economy. In such circumstances, the value of information for the business increases as well [2].

The voice calls are traditional way to exchange the information between the company employees. For several decades, the straight-forward approach to organize voice calls was a regular telephone line. However, as business becomes more and more

distributed, the prices of telecommunications service providers (TSP) for the use of telephone line between remote offices becomes too high. The Voice over Internet Protocol (VoIP) – one of the services that emerged as a result of the Internet development [3]. It allows to transmit voice traffic over the Internet Service Providers (ISP) instead of TSP, which allows to greatly reduce prices for communications. Nowadays, term «VoIP service» also often referred to both voice and video conferencing and text messaging and therefore it often mixes with «unified communications» term [5].

The aim of the paper is to present the viable infrastructure to meet business requirements for VoIP service. These requirements were indicated during the study and will be discussed in the Section 2. Section 3 will cover the structure of proposed solution in details as well as issues of service quality, development and delivering to the customers. Section 4 contains details of particular implementation of the proposed solution, including thorough description implemented functionality and installation process.

2 Requirements for the modern VoIP solution in business sector

Currently, there are three main trends in the development of VoIP communications.

1. Communication systems, initially intended for use in the corporate sector. A distinctive feature of these systems is the provision of communication services inseparable from equipment and services from the vendor, which leads to very high costs for providing corporate communications. Another feature of these systems is the low focus on the integration of other platforms (for example, clients for mobile devices operating under a specific operating system).
2. Communication systems for the mass consumer. A distinctive feature of these systems is the focus on the greatest reach of the audience, which is usually achieved by cross-platform client software simultaneously with the most simple configuration / deployment of the system. The server part of such systems is always located at the company-developer of the system, or its partners, which is an essential disadvantage on the part of security.
3. Communication systems with open source. A feature of this type of system is the ability to refine the necessary functionality and structure of corporate communications for the needs of a particular company. To service such systems requires high qualification of personnel, which leads to high maintenance costs. In addition, it should be noted weak support for mobile devices among key players in this area of the communications market.

Before the development of the VoIP solution, the set of requirements for the VoIP service in the business sector was determined, as well as analysis of existing solutions was performed. All indicated requirements may be divided in two groups: quality of connection and ease of deploy and access.

2.1 Quality of connection

Security and privacy
To achieve the privacy of conversations and therefore secure the exchange of voice and text data between subscribers, it is mandatory to encrypt all exchanged packets with strong algorithms. To prevent security through obscurity scenario, existing standards in encryption without known vulnerabilities should be preferred. However, exceeding encryption of the data may degrade the performance of end-user and server devices as well as to reduce the flow of useful traffic within the connection bandwidth. It also should be noted that encryption algorithm must comply with the local and state laws for encrypted data. Most of available VoIP solutions meet the encryption requirements, as it became the telecom standard.
However, in the case of flowing VoIP traffic through the remote third-party gateways (e.g. vendors servers), it is not unusual situation, that whole traffic may be decrypted at the third-party site, therefore providing full access to transmitted information, regardless the encryption.
Quality of codecs
While flowing from the one end-user device to another, the voice and video information should be coded at the sender device and decoded (reconstructed) at the recipient site. This process is handled by the use of voice and video codecs, that will usually limit the bitrate of the transmitted information and affect the quality of reconstructed speech and video information. While there are usually limitations on the connection bandwidth especially if the data transmitted over the mobile broadband connection, the codecs should adapt the bitrate of the voice and video traffic to provide reliable conversations. Requirements to used codecs are also met by the most of VoIP solutions, due to long story of codecs evolution.
Latency
The quality of voice conversations strongly depends on the latency, which means time between the sending of encoded and encrypted data from one end-user device and receiving the data on the another one. While latency strongly depends on the location of subscribers and performance of the network link between them, it is also affected by the infrastructure of VoIP solution. For example, while both subscribers are in the same building, some VoIP solutions mostly with client-server architecture might forward the traffic to the vendor's gateways, that may be located in hundreds and thousands of kilometers away from subscribers. Typical example of such situation are the supernodes of Skype infrastructure [1]. The requirements to minimization of latency are met in a greater degree for solutions with peer-to-peer architecture or when server might be allocated at the customers site.

2.2 Ease of access and deployment

Accessibility on handheld device
Another important trend is the ubiquity of mobile phones. The IDC Quarterly Mobile Phone Tracker claimed that total of 344.3 million smartphones have been shipped worldwide during first quarter of 2017 [7]. This indicates the mobile phone as a key

device to deliver voice, video and messaging services to the business customers. Therefore, the VoIP solution should be available at the variety of handheld devices. While most of huge vendors have support of these devices via vendor applications for most popular mobile operating systems (OS) – Android, iOS, open-source solutions, e.g. Asterisk, are experiencing lack of the support [4].

Cross-platform

Companies often have IT infrastructure based on devices working under different OS, depending on business requirements, technical and financial decisions, et cetera. In such circumstances, the VoIP solution should be able to support the diversity of both client and server devices, which usually requires VoIP solution to be cross-platform [5].

Ease of deployment

If the VoIP solution allows to place it at the customers site, it is necessary to provide ease of its deployment, as it may require hiring additional staff with narrow specializations to maintain the VoIP system functionality. At the same time, good vendor's support of the solution as well as complete documentation may lead to reduced costs of solution deployment.

2.3 Existing solutions

The closest in terms of functionality to the proposed system are the messengers Cisco Unified Communications Manager and Microsoft Lync Server. However, they are expensive and require the deployment and support of highly qualified professionals who have received special training, which is unacceptable for small companies. Our project does not have these drawbacks.

As a rule, various IT companies are engaged in the implementation of such projects. To the previously mentioned Skype, WhatsApp, Telegram, Viber, Cisco Unified Communications Manager and Microsoft Lync Server, the Signal Private Messenger, Chadder, Wickr Me, Threema and many others may be added. The number of which is increasing every year.

As mentioned earlier, all existing and currently developed projects have one of two drawbacks, or both. The first is the excessive cost and the need to attract third-party specialists to manage the server. The second is the lack of control over the server part of the system. In other words, it is not known where all the information from the server actually is. The proposed solution is devoid of both shortcomings.

3 Proposed solution

The innovative components of the proposed system include, firstly, individual elements of software, such as audio codecs and encryption algorithm. Secondly, the location of the servers of the proposed system can be selected by the customer. That is, it is possible to block access to third parties (including the developers of the proposed system) to servers, which significantly distinguishes the proposed system from existing analogs. It is also possible to install the system on a cloud server.

3.1 Basic principle

The system's operating principle is based on transmitting verbal and text information between the front-end applications installed on smartphones of your customers. Interaction between the system components is implemented using unique algorithms. While the information is transmitted via the network, it is secured using methods covered by relevant all-Union State Standards and uniquely designed solutions.
Once the software components (including server-side application) are purchased, the system will be created and operated only by the customer. Every communication network created by customer is unique. Any eavesdropping or retrieval of information that circulate on the net is nearly impossible.

The system includes:

1. Dedicated or cloud server running Linux / Microsoft Windows operating systems, with the server application installed on it. Installation and support of the server can be carried out by the customer or the developer.
2. Smartphones of any manufacturer with client applications installed on them.
3. A personal computer running Microsoft Windows operating system with an application installed on it for system administration.

System's features are as follows:
The owner holds total control over all the system components, they decide on where the system's elements are located. The owner also selects the process of creation and operation of the exclusive communication network.
The system will by no means interact with public communications networks and any other organized communication systems and networking devices via which information can be retrieved (authorized or unauthorized).
The owner can individually set up all parameters of communication network (location of the server-side application, subscriber list, connection matrix, etc.), as well as front end applications for smartphones of network subscribers.
The uniquely designed (non-standard) solutions are used to improve the communication quality and information security.

3.2 Structure of the software package

To fully meet indicated requirements, a new VoIP solution has been designed and implemented. The proposed system contains both package for deployment on the customers site and system to generate unique deployment package for a specific customer, which allows to tune system features and pricing policy.

During communications, all information between the Client and Server software is encrypted with strong algorithm, which complies with the Russian cryptographic

standard GOST 28147-89. Audio information is also encoded with developed codec, which allows to alter session bitrate depending on the quality of communication channel.

The proposed solution was built according to client-server architecture, as it allows to increase accessibility and control of service by the customer. However, compared with the most available client-server VoIP solutions, the package contains whole infrastructure, which allows to fully secure the traffic within the system as well as to minimize latency of communication. The package with proposed system contains several modules to provide customers with ease of deployment, access and maintenance.

Administration Console

The Administration Console (AC) is used to generate preferences files for both server and client software. It provides following functionality.

1. AC generates startup script for the server with preset IP address and port, which will be used to communicate with clients.
2. AC is used to setup matrix of contacts, which determines which users can communicate with each other. The matrix of contacts is stored as database and then being uploaded to the server.
3. AC used to generate QR codes for users' devices, that is used for software client on the mobile phone to connect to the server.

Server

The Server application is a binary file uniquely built for specific customer, which is available for both Windows and Linux hosts. On both OS families Server does not require installation and may instantly run as soon as database files are generated by the AC. Server listens for TCP connection on the configured port for authentication requests. After successful authentication, Server establishes TCP session with client to maintain short messages exchange and calls initialization and UDP session to exchange voice traffic. The Server app may run on public IP as well as to be configured for network address translation.

Proxy-server

Proxy server is the application, providing gateway between Server and Client. It is usually used to prevent compromising of the Server public IP.

Client for mobile phones

The Client is the application currently available for iOS and Android devices. It may be downloaded directly from the Google Play and Apple App Store. The Client application has minimalistic interface, however providing all necessary functionality to maintain messaging, voice calls and conferencing.

4 Integration, installation and implemented functionality of proposed solution

To prove the concept of proposed solution, the particular VoIP system was implemented according to structure, presented in the section 3. The system is named HiddenNet and is being currently rapidly developing by the paper authors. To demonstrate the fulfillment of criteria presented in section 2 of the paper, the integration of the HiddenNet system in the particular network as well as its functionality will be discussed in detail.

To set up the HiddenNet network, customer should start the AC application. To ensure privacy of the conversations, customer should enter information known only to him, to locate the server in an area selected by him and known only to him, as well as information on your network subscribers with whom he is willing to communicate:

- Public IP address of the server-side application;
- Public port of the server-side application;
- Local IP address of the server-side application (if the server is located outside NAT);
- Local port of the server-side application (if the server is located outside NAT);
- The network subscriber list and individual subscribers' PIN codes used to unlock the front-end application;
- Network subscribers connection matrix.

Once these data are entered, one should create the communication network database file which is encrypted using a self-generated key. The following files are also self-generated:

- Batch files used to start the server-side application;
- Batch files used to stop the server-side application;
- Individual settings files for front-end applications of network subscribers.

After that, the following files will be copied to a folder in a dedicated or cloud-based server:

- EXE file of the server-side application;
- Communication network database file;
- Key file used to close a communication network database file;
- Batch file used to start the server-side application;
- Batch file used to stop the server-side application.
- The server-side application is started by a Batch file for starting the server-side application.

4.1 System requirements

The communication network is created quickly and easily, however, there are prerequisite for the stability and smooth operation of HiddenNet, as follows:

- The HiddenNet server-side application should be installed on a dedicated or cloud-based server powered by 32- or 64- bit Linux or Microsoft Windows operating systems with a stable broadband balanced Internet connection. One should ensure an anytime access to the server using a public IP address and port which enables the incoming TCP connections and UDP datagrams.
- The HiddenNet front end applications should be installed on smartphones powered by Android 4.0 and up or Apple iOS, which can be connected to the Internet using 3G, CDMA, LTE or Wi-Fi technologies.
- The HiddenNet system administration application should be installed on a personal computer or laptop powered by Microsoft Windows connected to a local Wi-Fi network.

4.2 Administration console application installation and functionality

After the purchase and download of the application, a folder with the AC software is automatically downloaded, which allows customer to independently deploy a mobile encryption network with the parameters customized for him.

The folder contains the following components:

- an executable file for the Windows operating system (admin.exe);
- key information files (admin.key) and client database (admin.crk).

To start AC, the admin.exe file should be started in the folder, where the AC software archive has been unpacked after downloading from the manufacturer's website. A message will appear on the screen that the key file was successfully created. To continue, customer should press the "OK" button.

On the next screen customer should fill in the fields of the "External (Internet) address" block of settings:

- IP - the IP address of the server allocated to you.
- Port - the port allocated to you for use.

If the server is on the network behind NAT, customer must check the corresponding "Server by NAT" checkbox and additionally specify the internal IP address port. Further, you customer has two options:

- first – if the server is running Linux, customer needs to click the ".sh-file (Linux)" button, then the shell_linux folder will be created in the archive folder;
- the second - if the servers is running Windows OS, customer needs to click the ".bat - file (Windows)" button, after which the shell_windows folder will be created in the archive folder.

At the next stage, the customer needs to determine the subscribers (customers) of the network by processing to the "Clients" tab. The "Name" and "PIN-code" fields (any, but not less than 6 symbols) of the "Client identification" block should be filled by the

customer. Subsequent click on the "New" button will create the server startup command files.

After that, all subscribers (clients) of customer's network are displayed in the list. In order to delete a subscriber (customer), customer must select the subscriber (client) from the list and click the "Delete" button. In order to show the QR code of the subscriber (customer), it is necessary to select the subscriber (customer) from the list and click the "Show code" button. In order to save the customer's QR code, customer must select the subscriber (customer) from the list and click the "Save code ..." button.

The "Database Information" block displays the current and maximum number of subscribers (clients).

After determining all the subscribers of customer's network, in the "Contacts" tab one needs to configure the contacts of all subscribers (customers) of the network. To do this, customer must select the subscriber (client) from the drop-down list and mark the checkboxes of those with whom he can communicate and which will be displayed in his smartphone in the contact list. To speed up the work, to select all or clear all the subscribers from the list, there exist corresponding buttons.

After customer have defined (created) all the subscribers of the network and configured their possible contacts, one needs to click the "Save" button, then click the "Create a network ..." button and in the popup window on the computer select the user folder where the QR codes of the clients will be stored.

The user interface of developed AC software is shown in the Fig. 1.

4.3 Server installation and functionality

Using the AC application, customer must install the Server with created database and preferences files of the network on any selected, dedicated or cloud computing resource (server) running 32- or 64-bit Linux or Microsoft Windows operating systems that has a stable broadband symmetric Internet connection. The server must be provided with permanent access to the public IP-address and port, which allows to receive incoming TCP-connections and UDP-datagrams.

Setting up the server working under Linux OS.

Installation process for the Linux server will be shown on the CentOS 6 Linux distribution example. In the archive folder, customer must select the files admin.crk, admin.key and server executable to copy them to the shell_linux folder.

For further work customer needs the SFTP client many of which are available for different operation systems. In the paper, the open-source project WinSCP was used to manage files on the remote server. To connect to the remote server, customer needs to fill the following fields of the SFTP client:

- Transmission protocol - SFTP (automatically selected);
- Host name - the IP address of the server you have selected (selected by customer);
- Port - 22 (automatically filled);
- Username - the login customer created when buying a server;
- Password - the password customer created when buying a server.

After filling all fields, customer needs to click the "Login" button. Then, on the server, customer needs to go to the home folder and copy the shell_linux folder from the computer with configure AC software. After that, all files inside shell_linux folder, should be granted with the read/write/execute rights for the user, which will run the server software (usually it is root or system account).

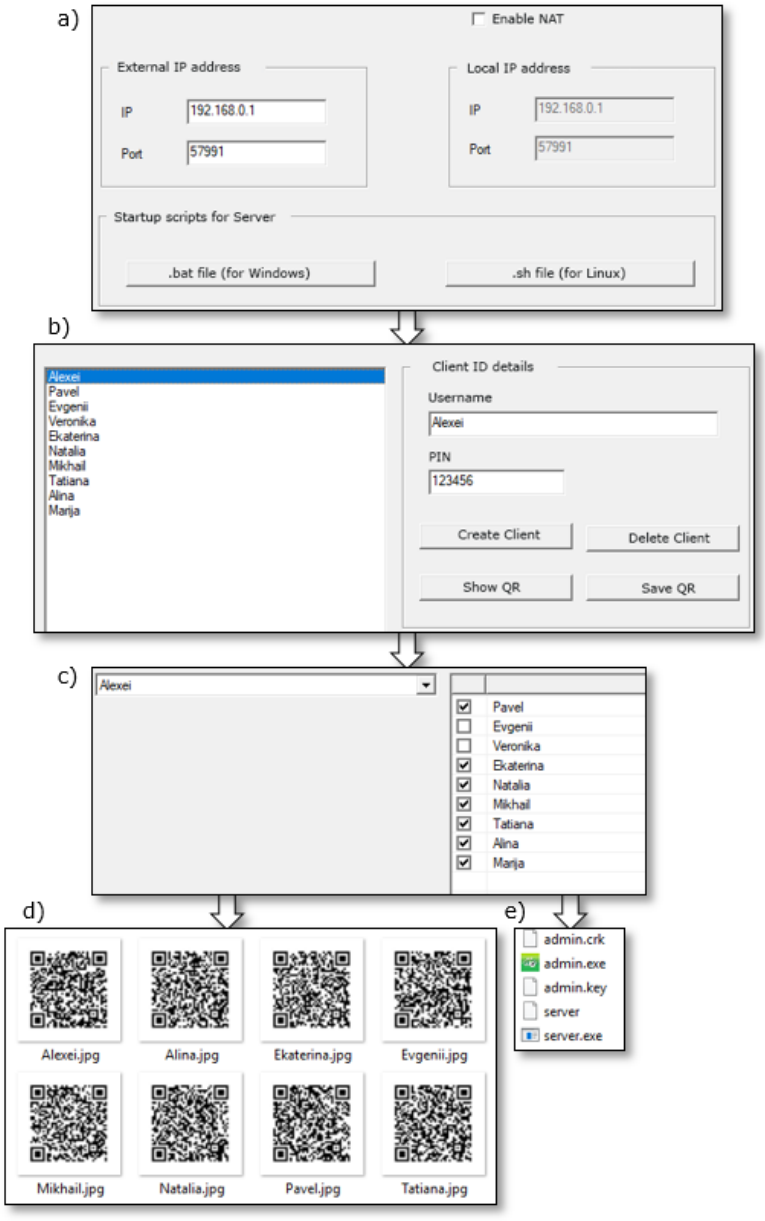

Fig. 1. – User interface of the Administration Console during step-by-step configuration. Server preferences – a); user creation – b); communication matrix – c); generated QR codes with preferences for handheld devices – d); generated database files for the server – e).

To provide the auto start on system reboot, the /etc/rc.d/rc.local file should be edited on the server. The path to the Server startup scripts should be edited to the end of the file. By default, required text looks as follows: sh /home/shell_linux/server_start.sh.

The final step is to configure the firewall. The iptables is default firewall under the CentOS. The typical configuration, which is enough for secure utilization of the HiddenNet system is shown below:

```
1. :INPUT ACCEPT [0:0]
 2. :FORWARD ACCEPT [0:0]
 3. :OUTPUT ACCEPT [0:0]
 4. -N LOGGING
 5. -A INPUT -i lo -j ACCEPT
 6. -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
 7. -A INPUT -p tcp --dport 12345 -j ACCEPT
 8. -A INPUT -p udp --dport 12345 -j ACCEPT
 9. -A INPUT -j LOGGING
10. -A OUTPUT -o lo -j ACCEPT
11. -A OUTPUT -m state --state ESTABLISHED -j ACCEPT
12. -A OUTPUT -p tcp --sport 22 -m state --state ESTABLISHED -j ACCEPT
13. -A OUTPUT -p tcp --sport 12345 -m state --state ESTABLISHED -j ACCEPT
14. -A OUTPUT -p udp --sport 12345 -j ACCEPT
15. -A OUTPUT -j LOGGING
16. -A LOGGING -m limit --limit 2/min -j LOG --log-prefix "IPTables-Dropped: " --
    log-level 4
17. -A LOGGING -j DROP
18. COMMIT
```

Here the configured port of the Server application is supposed to be 12345.

Now customer may restart the server. To do this, customer may enter the ‘reboot’ command in the WinSCP terminal interface and click the "Run" button. After reboot, the server starts automatically.

Setting up the server working under Windows OS (in case the computing resource (server) is running 32-bit or 64-bit Microsoft Windows operating systems). In the archive folder, customer needs to select the files admin.crk, admin.key and server.exe and copy them to the shell_windows folder. Then, in the shell_windows folder, customer should run the script sever_start.bat. If necessary, customer should tune the Windows Firewall to allow server to listen ports and accept connections.

After launching, a console window with the following information appears on the user's screen:

– information about the IP address and port;

– information about the status of the server startup.

To stop the server and exit the application, the "q" button should be pressed.

4.4 Designed mobile application

To get started with the mobile application, it needs firstly to be downloaded and installed on customer's mobile device (smartphone) in the usual way – from the online markets of corresponding operating systems or via direct download of .apk/.ipa files for the Android/iOS devices.

After installing the application, customer needs to start it and enter the QR code scanner mode. Then it is necessary to scan the QR code of the subscriber generated by the AC application. After a successful scan, the "OK" button will appear on the screen.

After that it is necessary to enter the PIN-code, which was defined for the corresponding subscriber when it was created in the AC application, and proceed to the authorization. After authorization, the Contacts tab is displayed. The application consists of 4 tabs:

– Contacts;
– Messages;
– Journal;
– Management.

The **Contacts tab** is presented as a list of all contacts of the user with the ability to quickly dial and send a message to any user in the list. The structure of the tab display:

– User icon:
  - Users on the network are displayed with a green icon;
  - Users not on the network are displayed with a white icon;
– User name.
– The "Messages" icon is opposite each user. When pressed, a dialog with the user opens.
– Log icon - opposite each user. When pressed, a call and a conversation with the selected subscriber are made. To end the call, you must click the "Hang Up" button. When an incoming call is made, two "Accept call" and "Snooze" buttons are available to the subscriber.

Unread messages appear in red in the Contacts tab in the Messages icon. Missed calls are displayed in red in the Contacts tab in the Journal icon.

The Messages tab is presented as a list of all dialogs with subscribers. The structure of the tab display:

– Status of the last message:
  - Outbox-the "Messages" blue icon;
  - Inbox - the "Messages" icon is green;

- New.

– Subscriber's name;
– Date and time of the last message.

When customer select a subscriber from the list, a dialog window opens.

Log tab is presented as a list of all user calls. The structure of the tab display includes call status, user name, date and time of the call. To call the user, customer should click on his name in the list.

Manage tab consists of 5 items of application settings:

– SMS life time;
– Clear all;
– Reset the application;
– Stop the application;
– About the program.

When customer clicks on the item, he can set the SMS life time. The following time intervals are available: 10 minutes, hour, day, week, unlimited.

Clear history functionality. The “Clear All” button displays the following message: "Logs and messages will be deleted. Continue?". By clicking the "Yes" button, all data will be deleted with the exception of any possibility of reading or removing information on them. By clicking the "No" button, the user will be returned to the "Management" tab.

Reset application. If customer clicks on "Reset application", the system will display the following message: "The configuration will be deleted, then the program will end. Continue?”. By clicking the "Yes" button, the application data will be reset, the application is closed and any contact with the network server is excluded. To authenticate (re-enter the network), the user will have to re-fill the "IP" field and read the previously proposed QR code (or the new one generated by the Administrator), followed by the input of the previously proposed PIN (or the new PIN generated by the Administrator). By clicking the "No" button, the user will be returned to the "Management" tab.

If customer clicks "**Stop application**", the system displays the following message "Are you sure?". After accepting, the application will be closed. For authorization, the user will have to enter a PIN code. By clicking the "No" button, the user will be returned to the "Management" tab.

When customer clicks on "**About**" the user can view the data about the program.

The example of created interface of the mobile client running under iOS is shown in the Fig. 2.

4.5 Service delivery to the customers

To distribute VoIP solution among the customers, the Distribution System (DS), which builds package with Server, Proxy-server and AC software, was implemented. It has administrative web-interface, which allows to operate with database, determining system features and downloads for customers. DS monitors purchases of the VoIP

system and provides customers with download of purchased package with the system software.

Front-end applications are downloaded and installed to subscribers' smartphones in the usual way. Then they will be automatically connected to the system administration application and will load the individual settings files. Once the user preinstalled pin-code is entered, the front-end client application is connected to the system server, from where the contact list of this subscriber will be loaded. Should a wrong pin-code be entered three times, all the data of the front-end application shall be automatically deleted from the smartphone and it will be completely disabled.

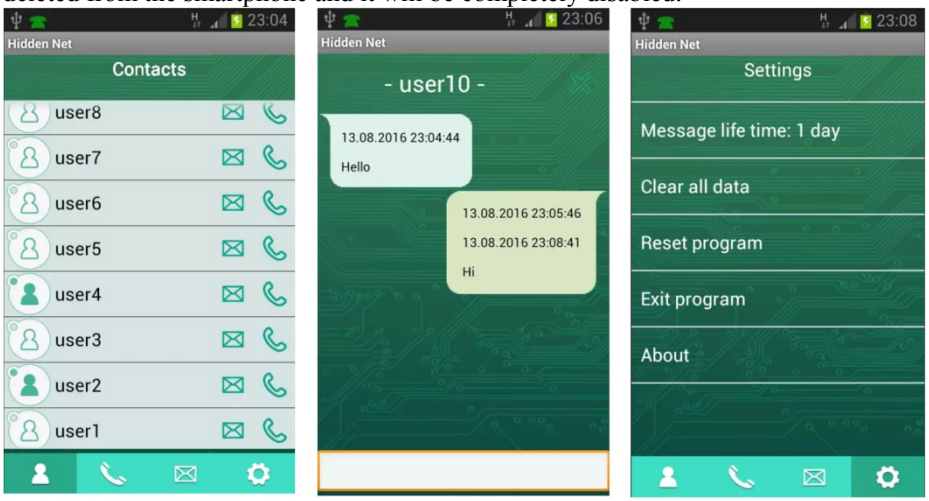

Fig. 2. – User interface of the Client application operating under iOS device.

We assume two main directions of commercialization of the solution.

- The first is corporate information security.
- The second is the development of a communication system for state structures at a price.

The developed system does not provide a fee for the use of the network, for technical support (any problems in the operation of the system are eliminated by the team resources), and for renting the servers in case of placing the system elements on the customer's servers (the choice of the location of the elements of the system is determined by the customer).

The cost of the system is the annual rent for its use and is dependent on customer's requirements. The examples of subjects, influencing the cost for customer are as follows:

- Length of the cryptographic key. In some countries the key length is strictly limited to 32 or 64 bits by the state laws. In such situation customer may purchase the system with reduced key length. However, recommended length is 256 bit, which leads to about 10^{77} of combinations required for brute-force attack on the key.

– Maximum number of subscribers. This allows to distinguish pricing policy between the small and large companies, as required scope of work to support companies of different sizes is either different.

4.6 Current status of project and further development

The HiddenNet solution is currently in the stage of rapid development. Currently there is a functioning client for devices on Android and iOS. The algorithm for encryption of transmitted information is based on GOST 28147-89 has been developed and implemented. An audio codec was developed at a speed of 26 kbps, having the same quality and computational costs as the G711 codec at 64 kbit/s. Voice communication and text messaging are fully operational.

Now the HiddenNet project is undergoing testing stage in Russia and Canada. The whole system has been deployed at several enterprises. The positive feedback has been obtained and requests for additional functionality allowed to formulate aims for the further development of the system:

1. Realization of the possibility of file transfer. It is an indispensable attribute of any modern communication system.
2. Creating a multi-client. The implication is that one user can participate in several secure networks. This function can be in demand if a person works in several companies that use our system.
3. Development of flexible settings for organizing a multi-level hierarchy of the contact list. For example, if used within a company, individual hierarchy levels may be departments, offices, departments.
4. Automation of deployment tasks described sections 4.2-4.3.

5 Conclusions

The paper presented structure of the VoIP solution suitable for customers in the business sector. Particular implementation of the system concept named HiddenNet is described in the details, demonstrating the fulfillment of ease-of-use and security criteria, formulated during the work. The proposed system has been delivered to the customer as the whole client-server solution, therefore providing customer with full control over communications, excluding involvement of the third-parties. The proposed solution utilizes strong encryption algorithms that comply with GOST 28147-89 cryptography standard. At the same time, the system is a cross-platform solution and does not require narrow specific knowledges to deploy the system. The system is undergoing tests in Russia and Canada, which preliminary results show, that proposed structure of the VoIP solution meets indicated requirements of the business sector and may be used as a viable architecture for VoIP software.

6 Acknowledgements

The paper is based on research carried out with the financial support of the grant of the Russian Science Foundation (Project No. 14-38-00009, The program-targeted management of the Russian Arctic zone development). Peter the Great St. Petersburg Polytechnic University.

References

1. Bonfiglio, D., Mellia, M., Meo, M., Rossi, D., & Tofanelli, P. (2007, August). Revealing skype traffic: when randomness plays with you. In ACM SIGCOMM Computer Communication Review (Vol. 37, No. 4, pp. 37-48). ACM.
2. Goldibina, L.A., Orlov, P.S. (2017) BIM Technology and Experience of Their Introduction into Educational Process for Training Bachelor Students of Major 08.03.01 «Construction». Journal of Mining Institute (Vol. 224, pp. 263-272). DOI: http://dx.doi.org/10.18454/pmi.2017.2.263
3. Goode, B. (2002). Voice over internet protocol (VoIP). Proceedings of the IEEE, 90(9), 1495-1517.
4. Montoro, P., & Casilari, E. (2009, July). A comparative study of VoIP standards with asterisk. In Digital Telecommunications, 2009. ICDT'09. Fourth International Conference on (pp. 1-6). IEEE.
5. Palmieri, M., Singh, I., & Cicchetti, A. (2012, October). Comparison of cross-platform mobile development tools. In Intelligence in Next Generation Networks (ICIN), 2012 16th International Conference on (pp. 179-186). IEEE.
6. Shah, N. A., Hugg, E. B., & Chestnut, K. L. (2003). U.S. Patent No. 6,606,647. Washington, DC: U.S. Patent and Trademark Office.
7. Worldwide Smartphone Growth Goes Flat in the First Quarter as Chinese Vendors Churn the Top 5 Vendor List, According to IDC. wwwidccom. 2017. Available at: http://www.idc.com/getdoc.jsp?containerId=prUS41216716. Accessed July 11, 2017.