**Stealthphone Information Security System**

**List of products and functions**

Table of contents:

[**Stealthphone Information Security System** 1](#_Toc421116541)

[**List of products and functions** 1](#_Toc421116542)

[Mission of the document 4](#_Toc421116543)

[1. Теrms and definitions 5](#_Toc421116544)

[1.1. Crypto terms 5](#_Toc421116545)

[1.2. Brands and helping definitions 6](#_Toc421116546)

[MTT company products and solutions 9](#_Toc421116547)

[2. Solutions for individual using and personal information security 10](#_Toc421116548)

[2.1. StealthPhone Software PKI 10](#_Toc421116549)

[2.2. Secure Android 13](#_Toc421116550)

[2.3. Stealthphone VPN 13](#_Toc421116551)

[3. Solutions for the information security systems of small and medium businesses 15](#_Toc421116552)

[3.1. StealthPhone Software 15](#_Toc421116553)

[3.2.1. Encryption keys hardware generator 22](#_Toc421116554)

[3.3. Secure Android 22](#_Toc421116555)

[3.4. Stealthphone VPN 22](#_Toc421116556)

[4. Solutions for security of the information systems of corporations 24](#_Toc421116557)

[4.1. Stealthphone Hard 24](#_Toc421116558)

[4.1.1. Stealthphone CryptoDisk 32](#_Toc421116559)

[4.2. Stealthphone Office Gate 33](#_Toc421116560)

[4.3. Secure Android 34](#_Toc421116561)

[4.4. Stealthphone VPN 35](#_Toc421116562)

[4.5. StealthPhone Key 35](#_Toc421116563)

[4.5.1. Hardware key generator 35](#_Toc421116564)

[4.6. Certification authority 35](#_Toc421116565)

[4.7. Server platform 35](#_Toc421116566)

[4.8. FileHider 35](#_Toc421116567)

[5. Solutions for state information systems security 36](#_Toc421116568)

[5.1. Server platform 36](#_Toc421116569)

[5.2. Certification authority 36](#_Toc421116570)

[6. Services 37](#_Toc421116571)

[6.1. Consultations on information security 37](#_Toc421116572)

[6.2. Trainings on information security 37](#_Toc421116573)

# *Mission of the document*

This document is designed for the internal use of employees of “Mobile Trust Telecommunication” (hereafter “MTT”). The present document is intended to solve the following issues:

1. Make a clear conception about MTT company products and solutions which now are on the different stages of engineering and development;

2. Unify terms and brand names used inside the company;

3. Consolidate the main technical data on products and solutions of MTT company to create user manuals, guidance on administration, technical specifications, marketing materials and other documents.

# *Теrms and definitions*

## Crypto terms

**Encryption** — data conversion in order to hide it from the unauthorized people, meanwhile giving access to it to the authorized users.

**Decryption** — the process of modifying of an encrypted text into a clear text.

**Encrypted text** — an encrypted message.

**Crypto algorithm** (cipher) – a mathematic function used for encryption and decryption.

**Encryption system** — a system which can produce data encryption and decryption.

**Encryption key** —a secret information used for data encryption and decryption.

**Symmetric encryption algorithms** — a way of encryption when the same crypto key is used for encryption and decryption. These algorithms, also known as the algorithms with a private key or one key algorithms, require a sender and a recipient to agree the key they use before starting a secure message transfer. Security of the symmetric algorithm is defined by a key. The key compromising means that anyone can encrypt or decrypt messages. While transferred messages have to be secret, the key should be kept private.

**Asymmetric encryption algorithms** (algorithms with a public key) — the algorithm where an encryption key differs from a decryption key. In asymmetric algorithms the decryption key cannot be calculated using the encryption key. Every subscriber has its own public and private key.

**Public key** — an encryption key in asymmetric algorithms. This key is not secret; it is transferred via the open communication channels and is used to encrypt messages.

**Private key** — a decryption key in asymmetric algorithms. This key is secret, only a particular subscriber can decrypt a message encrypted using his public key.

**Stealthphone information security system** (Stealthphone system) — the system which allows subscribers exchange information confidentially. Stealthphone information security system includes: Stealthphone Software, Stealthphone Hard with Stealthphone Sync software application, Stealthphone Key generation and distribution program (can be optionally completed by a hardware key generator), SIP server and license server.

**TEMPEST** (Transient Electromagnetic Pulse Emanation Standard) — the international standard for transient electromagnetic pulse emanations of the operating radio electronic equipment. The technology of testing via TEMPEST standard minimizes the risk of secret information disclosure if it is captured and analyzed using the different technical means of side electromagnetic radiation. Notion TEMPEST also includes standards for equipment, measuring and control instruments.

## Brands and helping definitions

**Stealthphone Hard** – is software and hardware complex for information encryption using Stealthphone Touch hardware encryptor or Stealthphone Tempest connected via Bluetooth channel to the mobile phone with installed Stealthphone Sync application, which can encrypt any kind of the transferred data (voice, SMS, MMS, e-mails, documents and files) in mobile phones and computers.

**Voice over GSM** - the technology for encrypted voice transfer via standard GSM channels of voice signal transfer.

The key point is that an encrypted voice signal is transferred via a standard GSM communication voice channel. Voice over GSM uses eCall technology (data transfer over voice signal- Data over voice channel GSM). Encryption and decryption are performed in a hardware encryptor. The encryptor using Voice over GSM technology is connected to mobile phones as a usual Bluetooth head set. This technology can be used for encrypted voice transfer not only via GSM channel but also via VoIP (SKYPE).

**Stealthphone Sync** —an application for a mobile phone (tablet) needed for using Stealthphone Touch hardware encryptor or Stealthphone Tempest.

**Stealthphone Software** — a software encryptor. Software for a mobile phone (tablet) which emulates the work of hardware encryptor.

**Stealthphone Software PKI**— a software encryptor. Software for a mobile phone (tablet) which emulates the work of hardware encryptor and uses asymmetric encryption on public keys. Users authentication is performed through the Certification Authority.

**Secure Android** – a mobile phone on the Android platform with the pre settings performed by MTT company for a stronger seсurity of user information.

**Stealthphone VPN** – a technology providing non-disclosure of IP address, meta data and a complete impersonation of a subscriber, which makes possible to get anonymity in the Internet network.

**StealthPhone Office Gate** – software and hardware solution providing a secure access to the office network (telephone, followed by IP) from smartphones using StealthPhone Software program and StealthPhone Hard hardware generator.

**Crypto disk** – software designed for data encryption on a personal PC using Stealthphone Hard while connection via USB.

**SIP-server** — a server providing the opportunity to transfer subscriber voice data, encrypted by Stealthphone Hard or Stealthphone Software, via IP network.

**License server** — a server which allows conduct registration and identification of Stealthphone network subscribers.

**Сrypto chat server** — a XMPP server which allows Stealthphone network subscribers exchange encrypted data on-line using crypto chat or crypto conference.

**Billing center** —a server responsible for a profile managing (creation, blocking, deletion and change), funds control, service rating, the automatic subscribers invoicing and payments reception.

**Certification authority** (CA) – a software product which is a subsystem of the information security system, Stealthphone software and hardware complex (Program Apparatus Complex, PAC)

The mission of CA is managing asymmetric crypto keys and user digital certificates to ensure a secure information exchange between users as well as their identification.

**Stealthphone Key** — computer software designed to generate and distribute encryption keys and PIN codes of Stealthphone network subscribers. Stealthphone Key program is used by the Stealthphone network administrator.

**Hardware encryption key generator** —a device for generation encryption keys which work is based on the physical random numbers generator. It ensures high quality of the generated keys with a high degree of randomness. The hardware encryption key generator is used together with Stealthphone Key program.

**Stealthphone Keyloader** — computer software Stealthphone network subscribers can use to download encryption keys to Stealthphone Hard hardware encryptors themselves.

**Stealthphone Email** (settings for Microsoft Outlook) — computer software designed for encrypted email messages exchange between computers and mobile phones of Stealthphone network subscribers. Encryption is performed by Stealthphone Hard hardware encryptor connected to a computer via USB.

**Crypto network** (Stealthphone network) — a group of subscribers with the same Stealthphone network identifier. Encryption keys of all subscriber connections of a one crypto network belong to the only one key matrix; therefore information exchange is possible only between the subscribers of this crypto network. A number of subscribers in one crypto network can range from 2 to 10000.

Every subscriber can only be in one crypto chat. Encrypted calls, SMS, MMS, emails exchange, chat and crypto conference are possible only between the subscribers of one crypto network.

**Crypto network identifier** — a unique identifier which consists of 8 symbols (figures and English letters from A to F inclusively). Stealthphone network administrator gets the crypto network identifier in a form of a file from MTT company.

**Encryption key of a pair connection** — key for encryption and decryption of voice or data (SMS, MMS, email messages, chat) used while connection between two subscribers.

**Crypto number** —a unique identification number of a subscriber in crypto network. Crypto number is assigned to every subscriber by the Stealthphone network administrator.

**SIP number** —an identifier assigned to a crypto network subscriber, where the other crypto network subscribers can call.

**Crypto chat**— encrypted messages exchange between two subscribers of Stealthphone network. Crypto chat allows two subscribers to exchange files and text messages.

**Crypto conference** —encrypted messages exchange between two and more Stealthphone network subscribers.

**Secrecy level** — level from 1 (the highest) to 10 to distinguish the opportunity of confidential messages exchange between subscribers. The secrecy level is assigned to every subscriber by Stealthphone network administrator.

**Stealthphone network administrator** — a person responsible for generation and distribution of encryption keys and PIN codes of Stealthphone network subscribers.

# *MTT company products and solutions*

MTT company presents the products for information security in mobile phones, tablets an personal computers. For convenience and in order to meet demands of any clients there are 2 ways of information security, using software and hardware solutions.

Information security system is based on VoIP technologies and presents the IP telephony with a strong and super strong data encryption (based on hardware and software encryption)

MTT company presents products and solutions for the personal information security and protection of corporate and state information systems.

# Solutions for individual using and personal information security

## StealthPhone Software PKI

Stealthphone Software PKI – is a software product for mobile devices on the basis of iOS, Android, Windows Phone and BlackBerry platforms. Stealthphone Software PKI uses the asymmetric encryption key and is designed for the personal information security.

1. **Functional capabilities:**

Stealthphone Soft PKI information security system provides crypto security of the following information in mobile phones and tablets:

1. Voice.
2. Data:
* SMS.
* MMS (in the next versions).
* Email. Sending and getting messages are possible using MTT company mail server or the any other server (Gmail, Mail, Yandex etc).
* Crypto chat (text messages and files exchange between two subscribers) and crypto conference (text messages exchange between two and more subscribers).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Functionality on different platforms** | **iOS** | **Android** | **Windows Phone** | **BlackBerry** |
| Voice calls encryption using audio codec AMR-WB and the service quality control; |  |  |  |  |
| 1. Encrypted text messages exchange (crypto chat) between users and control of the message delivery and its successful decryption by a recipient.
 |  |  |  |  |
| 1. Encrypted text messages exchange for a group of users taking part in a crypto conference
 |  |  |  |  |
| 1. Encrypted SMS messages exchange
 |  |  |  |  |
| 1. Encrypted files exchange between users with control of delivery and successful decryption
 |  |  |  |  |
| Exchange by encrypted emails with attachments via SMTP and POP protocol |  |  |  |  |
| Encryption of files from the programs of third-party developers for secure transfer via the network |  |  |  |  |
| Storage of not big texts in a form of notes in an encrypted way |  |  |  |  |
| Data storage in an encrypted form in a phone memory |  |  |  |  |

1. **Supported operation systems and devices**: Android, iOS, Blackberry, Windows Phone 8.

**iOS:** IOS 7
**Android:** Android c 2.3 до 4.3 (except 4.2)

**BlackBerry:** Blackberry OS 6, OS 10
**Windows Phone:** Windows phone 8
**Supported networks:** 3G, 4G, EDGE, CDMA, WiFi

1. **Encryption system:** Data encryption is performed using a symmetric algorithm and one- time session keys of 256 bit length deleted after each communication session.
2. **Key distribution system.**

Public key distribution system (Public Key Infrastructure).

**For user:** while a secure connection all the processes on key generation, encryption and decryption go invisibly for users with the indication of a process (encryption, decryption and verification). In case the certificate of a second participant of communication is not valid, the notifications about impossibility to continue a secure connection will appear in the program interface. *MTT company does not have access to subscribers encryption keys.*

**General operating principles of PKI:** PKI is based on using crypto system with a public key and several main principles:

1. a private key is known only to its user;
2. the certification authority creates a public key certificate, therefore certifying this key;
3. nobody trusts each other but everybody trusts the certification authority;
4. the certification authority confirms or disconfirms that a public key belongs to a given person who possesses a corresponding private key.

**PKI main components:**

* Certification authority (CA) is the main structure which forms digital certificates of the subordinate certification centers and end users. CA is the main managing component of PKI:
1. it is a trusted third party
2. it is the server which manages certificates.
* Public key certificate (often just a certificate) — user data and public key signed by CA. When CA issues a key, it confirms that the person named in the certificate owns a private key corresponding to this public key.
* End users – application or system users who are certificate owners and use the public key managing infrastructure.

**PKI algorithm:**

* + - 1. Client application generates public and private key.
			2. Client application generates a request for the certificate. The user application form and public key are included in the request.
			3. The request for a certificate is signed with a private key and sent for verification to CA.
			4. CA checks the license and signature.
			5. If the data is correct, CA verifies the application form and the public key with its private key.
			6. The signed certificate is returned to the user
			7. Now both users can perform a secure data exchange or make a secure phone call. A one-time encryption session key is generated on the users public keys.
			8. Decryption goes on the private user keys.



Scheme 1. Infrastructure scheme of Stealthphone Soft PKI

1. **Solution components** (see Scheme 1):
2. **Client part:**
3. Stealthphone Software PKI installed on users devices.
4. **Server part**
5. Certification authority
6. Billing center
7. XMPP server (сrypto chat server)
8. **Support service**
9. Technical support service for users (Моscow)
10. Call-center (Switzerland)
11. **General description**

After purchasing the subscription for Stealthphone Soft PKI software, a private office on MTT website is provided to a subscriber. Information about his agreement (subscription) status, his data for CA and connections statistic is displayed in the private office.

Voice or text data of the first subscriber are encrypted in Stealthphone Soft PKI and transferred to the second subscriber using a mobile phone (tablet).Voice, crypto chat, crypto conference and email messages are transferred via the Internet (via Wi-Fi or mobile internet of a cellular network) and SMS and MMS messages are transferred via cellular network. The received data is decrypted using Stealthphone Soft PKI of the second subscriber.

As can be seen from the above, voice and data are encrypted in Stealthphone Soft PKI of the first subscriber, decrypted by the encryptor of the second subscriber and are transferred in the encrypted form between 2 mobile phones. Every subscriber needs to have the pre installed Stealthphone Soft PKI software encryptor on his smart phone for confidential connection.

1. **Compatibility with other products.**

An open question.

1. **Cost of subscription services:** approximately $17 per month
2. **Рroduct development.**

Demo version of the product (limited period of work - 7 days) can be included into the pre-installing basis packet to the supported mobile phones of partners.

Possible partners: network operators, producers of mobile devices, developers of mobile OS.

## Secure Android

Secure Android – smartphone with the operation system developed by MTT company on Android OS basis. Smartphone antivirus software is installed on the smartphone.

Necessary to do on this product:

1. Find a smartphone supplier. One of the options is Google Nexus devices, which are available for buying. Google company – Android developer – provides all OS source codes and the utility for firmware integration
2. Find an antivirus software supplier for pre installation to the phone
3. Adjust Stealthphone Software PKI to a product for the best work on the chosen Android version.
4. Expand functionality of the basic Android using security instruments against unauthorized access and user data encryption.

## Stealthphone VPN

Stealthphone VPN –product for security of IP address and user meta- data

The system is designed to arrange the virtual private network (VPN) and provide VPN service to StealthPhone network subscribers. The main mission of the system is non-disclosure of IP address and meta-data and a complete impersonation of a subscriber data in order to get anonymity in the Internet network. Communication is performed via networks with less or unknown trust level (for example, via public networks). Trust level of a constructed logical network does not depend on the trust level of the basic networks due to using cryptographic instruments (encryption, authentication, public key infrastructure and instruments for protection against repeating and changes transferred via the logic messages network).

# Solutions for the information security systems of small and medium businesses

1. StealthPhone Software
	1. StealthPhone Key – software for encryption keys generation and distribution
		1. Encryption keys hardware generator
2. Secure Android
3. Secure VPN

## StealthPhone Software

Stealthphone Software – a software product for mobile devices on the basis of iOS, Android, Windows Phone and BlackBerry platforms, which exploits the symmetric encryption key and is designed for security of the information systems of small and medium businesses.

1. **Functional capabilities:**

Stealthphone Software information security system provides crypto security of the following information in mobile phones and tablets:

1. Voice.
2. Data:
* SMS.
* MMS
* Email. Sending and getting messages are possible using MTT company mail server or any other server (Gmail, Mail, Yandex etc).
* Crypto chat (text messages and files exchange between two subscribers) and crypto conference (text messages exchange between two and more subscribers).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Functionality for different platform** | **iOS** | **Android** | **Windows Phone** | **BlackBerry** |
| 1. Voice calls encryption using audio codec AMR-WB and the service quality control; |  |  |  |  |
| 1. Encrypted text messages exchange (crypto chat) between users and control of the message delivery and its successful decryption by a recipient.
 |  |  |  |  |
| 1. Encrypted text messages exchange for a group of users taking part in a crypto conference
 |  |  |  |  |
| 1. Encrypted SMS messages exchange
 |  |  |  |  |
| Exchange by encrypted emails with attachments via SMTP and POP protocol |  |  |  |  |
| Encryption of files from the programs of third-party developers for secure transfer via the network |  |  |  |  |
| Storage of not big texts in a form of notes in an encrypted way |  |  |  |  |
| Data storage in an encrypted form in a phone memory |  |  |  |  |

**2. Supported operation systems and devices**: Android, iOS, Blackberry, Windows Phone 8.

**iOS: Syncle IOS 7
Android:** Android from 2.3 to 4.3 (except 4.2)

**BlackBerry:** Blackberry OS 6, OS 10
**Windows Phone:** Windows phone
**Supported networks:** 3G, 4G, EDGE, CDMA, WiFi

1. **Encryption system:** Symmetric keys combined with Diffie-Hellman protocol are used to generate a session key
2. **Key generation system.**

When this solution is employed, encryption keys are generated by users themselves or by Stealthphone network administrator. Encryption keys are generated using Stealthphone Key program and encryption keys hardware generator (hardware key generator is additional option). To encrypt different kinds of data between a pair of subscribers its own key is generated for every kind of connection (voice,SMS, chat, data, email). MTT company does not have access to the encryption keys of users.

***Key distribution procedure***

Key distribution procedure consists of 3 stages:

**1. MTT company carries out preparation.** As a result of preparation, Stealthphone network administrator is given the file of network identifier and Stealthphone Key program.

**2. Key generation and distribution is** performed by Stealthphone network administrator using Stealthphone Key program. Stealthphone network administrator forms and transfers encryption key files for remote users.

**3. Encryption key loading to Stealthphone Hard or Stealthphone Software** can be performed as the Stealthphone network administrator as a subscriber himself:

* Stealthphone Key program is used by the administrator for key loading.
* To download keys subscribers use Stealthphone Keyloader program ( see Stealthphone Hard user manual for more details). To download keys a subscriber should have encryption key file, encryptor PIN code and Stealthphone Keyloader program.
1. **Product components:**
2. **Client part:**
	1. Software for Stealthphone Software mobile device
	2. StealthPhone Key generation and distribution program
	3. Encryption keys hardware generator (оptionally)
3. **Server part ( Аncort):**
	1. License server
	2. SIP server
	3. Crypto chat server
	4. Mail server
4. **User support**
5. User technical support



Scheme 2.Stealthphone Software infrastructure solution

1. **General description**

Stealthphone network administrator is suggested for this solution. The administrator determines a list of crypto network participants, the number of the symmetric keys every subscriber has and their distribution, deleting compromised keys. In this solution distribution is carried out by copying the list of keys to the smartphone of every crypto network participant. Keys are transferred and stored in a mobile device in the encrypted key container.

***Operation principles***

Voice or text messages of the first subscriber are encrypted in Stealthphone Soft and transferred using a mobile phone (tablet) to the second subscriber. Voice, crypto chat, crypto conference and email messages are transferred via the Internet (via Wi-Fi or the mobile internet of provider) and SMS and MMS messages are transferred through the cellular network. The received data is decrypted using Stealthphone Soft of the second subscriber.

olk

As can be seen from the above, voice and data are encrypted in Stealthphone Soft of the first subscriber, decrypted by the encryptor of the second subscriber and are transferred in the encrypted form between 2 mobile phones. Every subscriber needs to have the pre installed Stealthphone Soft software encryptor on his smart phone for confidential connection.

***Advantages***

* **Separate encryption key matrix for every kind of connection**

Separate encryption key matrixes are used in Stealthphone information security system for every kind of data (voice, SMS, MMS, crypto chat and email messages). Therefore, 5 encryption key matrixes are used in Stealthphone system, which increases the level of crypto security while confidential data exchange.

* **It is not possible to decrypt the transferred voice and data even if a mobile phone is lost or stolen.**

Malicious people will not be able to get access to the data stored in Stealthphone Soft, if a mobile phone is lost or stolen, as encryption keys are stored in Stealthphone Soft in the encrypted form.

Every Stealthphone system subscriber has his own unique set of keys for connection with other subscriber. Therefore, if one encryptor is lost or stolen, it will not have any effect on the security of other subscribers. Encryption keys of connections with this subscriber can be deleted by other Stealthphone network subscribers from their encryptors. Set of keys is formed by Stealthphone network administrator using encryption key generator. It can be easily changed if it is necessary and the compromised keys can be deleted from the base of encryption keys.

* **Possibility for subscribers to generate encryption key themselves**

In Stealthphone information security system subscribers can generate encryption keys themselves using hardware or software key generator.

Hardware generator provides the strongest crypto security and its work is based on measuring parameters of the physical processes.

Subscribers can check quality of the created keys themselves.

* **Money saving while voice calls**

As in other IP telephony services (Skype, Viber), encrypted voice is transferred via the Internet in Stealthphone system. Thanks to using IP telephony, subscribers can significantly cut costs on calls in roaming during their business trips or holidays.

Using a unique vocoder in Stealthphone Soft allows saving voice quality while transfer with the speed of 4,8 Kbit per second. This solution makes possible to significantly cut the volume of the transferred data if to compare with other IP telephony services, therefore cutting costs on the services of data transfer.

***Protection against attacks***

* **Protection against the attack “man in the middle”**

«Man in the middle» — the attack method when an intruder, having connected to the communication channel between subscribers, wiretaps and actively interferes in the data transfer, deleting and changing it or giving the false information. Subscribers in this situation don’t know they are being attacked.

For security against wiretapping using the method «Man in the middle» in the beginning of the encrypted conversation the security code of 5 figures is displayed on the screen of a mobile phone. The same code should be displayed on the screen of the other subscriber.

An example of the security code. A new code is created every time.

In the beginning of every conversation a user should match the security code on his mobile phone screen with the code of the second subscriber. If the security codes of the first and the second subscribers are different, the subscribers are being attacked with the method “man in the middle”. In this case it is necessary to stop the conversation and make the second voice call to a subscriber again until the codes are the same.

* **Security against interference into the encrypted conversation**

A third person cannot interfere into the encrypted conversation as it happens with the usual phone connection, because the operation principle of Stealthphone system guarantees the consistency of the transferred information.

1. **Compatibility with other products and solutions of MTT company**

In addition to StealthPhone Software product the following products and solutions can be purchased:

Encryption keys hardware generator;

Stealthphone Hard hardware generator;

Solution for security of the office network Stealthphone Office Gate;

Solution for security Stealthphone VPN;

Secure Android.

1. **Price:**
USD 500–1000 for a license
2. **Product development.** Product demo version (limit for the period of work is 7 days)

**Possible partners:** network operators, producers of mobile devices, developers of mobile OS

* 1. **Stealthphone Key**

Stealthphone Key – a software product for encryption keys generation. It is a part of Stealthphone Soft and Stealthphone Hard solutions.

**Functional capabilities**

Stealthphone Key program is designed to:

* create and administrate the data base of Stealthphone network subscribers;
* generate, edit and distribute the encryption keys of Stealthphone network subscribers;
* download the encryption keys to Stealthphone Hard and StealthPhone Software encryptors;
* conduct encryption keys export and their later transfer to the remote subscribers so they could download the keys to Stealthphone Hard and Stealthphone Software encryptors themselves.

**System requirements**

To install and use Stealthphone Key program is needed the computer which meets the following requirements:

|  |  |
| --- | --- |
| Оperation system | * Windows XP and Windows 7 (32-bit and 64-bit).
 |
| Free space on hard disk | * Stealthphone Key program takes about 50 МB on hard disk.

Size of the database depends on the number of subscribers.Note: Data base for10 000 subscribers takes about 16 GB on the hard disk. |

**Key distribution procedure**

Key distribution procedure consists of 3 stages:

**1. MTT company carries out preparation.** As a result of preparation, Stealthphone network administrator is given the file of network identifier and Stealthphone Key program.

**2. Key generation and distribution is** performed by Stealthphone network administrator using Stealthphone Key program. Stealthphone network administrator forms and transfers encryption key files for remote users.

**3. Encryption key loading to Stealthphone Hard or Stealthphone Software** can be performed as the Stealthphone network administrator as a subscriber himself:

* Stealthphone Key program is used by the administrator for key loading.
* To download keys subscribers use Stealthphone Keyloader program ( see Stealthphone Hard user manual for more details). To download keys a subscriber should have encryption key file, encryptor PIN code and Stealthphone Keyloader program.

Key distribution is displayed on the picture below:



**Additional options**

In addition to Stealthphone Software encryption key hardware generator can be purchased.

### Encryption keys hardware generator

Encryption keys hardware generator is an additional option of Stealthphone Key program.

Physical random numbers generator based on noise diode is used in the generator. It provides high quality of the generated keys, which have a high degree of randomness (in contrast to the software realization, where pseudo random numbers are generated). Exploiting hardware key generator also allows confining possibility that some computer viruses make effect on them.

**Functional capabilities of the encryption key generator:**

* Possibility of key generation using a physical random numbers generator;
* Possibility of key editing and their check for complying the quality characteristics;
* Possibility of work with a big number of keys;
* Possibility to create the own library.

**General description**

Hardware encryption key generator is connected to PC with the pre installed software product Stealthphone Key via USB. Hardware generator managing is conducted in the interface of Stealthphone Key software generator.

## Secure Android

Secure Android – smartphone on the Android basis with the pre installed software product and antivirus security.

Necessary to do on this product:

1. Find a smartphone supplier. One of the options is Google Nexus devices, which are available for buying. Google company – Android developer – provides all OS source codes and the utility for firmware integration
2. Find an antivirus software supplier for pre installation to the phone
3. Adjust Stealthphone Software PKI to a product for the best work on the chosen Android version.
4. Expand functionality of the basic Android using security instruments against unauthorized access and user data encryption.

## Stealthphone VPN

Stealthphone VPN –product for security of IP address and user meta- data

The system is designed to arrange the virtual private network (VPN) and provide VPN service to StealthPhone network subscribers. The main mission of the system is non-disclosure of IP address and meta-data and a complete impersonation of a subscriber data in order to get anonymity in the Internet network. Communication is performed via networks with less or unknown trust level (for example, via public networks). Trust level of a constructed logical network does not depend on the trust level of the basic networks due to using cryptographic instruments (encryption, authentication, public key infrastructure and instruments for protection against repeating and changes transferred via the logic messages network).

# Solutions for security of the information systems of corporations

1. StealthPhone Hard
	1. StealthPhonе Temptest
	2. StealthPhone Touch
	3. Work in GSM mode
	4. StealthPhone CryptoDisk
	5. StealthPhone – software for encryption keys generation and distribution
		1. Encryption keys hardware generator
2. StealthPhone Office Gate

## Stealthphone Hard

Stealthphone Hard –a security solution for the information systems of corporations. The solution provides a super strong level of encryption due to using hardware encryptor.



1. **Cryptographic parameters**
* Symmetric encryption algorithm (MTT company’s development) with a key length of 256 bit
* Asymmetric encryption algorithm based on the elliptic curves with a key length of 384 bit.
* Possibility of embedding additional encryption algorithms
* Embedded physical random number generator for creating crypto keys
* A specialized crypto operational system managing the work of device
* Specialized software for key generation and recording to the device
* One-time session keys (are generated in the beginning of a session and are guaranteed to be erased at the end of the session)
* Calculating a session key for voice encryption using Diffie-Hellman method combined with full key matrix.
* Calculating a session key for encryption of SMS and Email using full key matrix.
* Protection against unauthorized access:
* Device – using a password from 8 to 20 figures
* Bluetooth – using PIN code from 4 to 20 figures
* Crypto SD card – using a password from 8 to 20 figures
* Speed of encryption – 5 МBit/sec
* Authentication of subscribers in the mode of encryption of telephone conversation
* Protection against the attack “Man in the middle” (MITM) while voice encryption
* Control of wholeness of the transferred encrypted data
* Using secured IPSec protocol in the tunnel mode for connection of Stealthphone with a specialized SIP server
* Immunity to computer viruses
* Key erasing and blocking of crypto services in case the device is lost or stolen
1. **Functional capabilities:**

Stealthphone Hard information security system (hardware encryptor) provides crypto security of the following information in mobile phones and tablets:

1. Voice.
2. Data:
* SMS.
* MMS
* Email. Sending and getting messages are possible using MTT company mail server or any other server (Gmail, Mail, Yandex etc).
* Crypto chat (text messages and files exchange between 2 subscribers) and crypto conference (text messages exchange between 2 and more subscribers)
* Files when Stealthphone encryptor is connected to PC via USB
* Voice over GSM – encrypted voice data transfer via a standard voice channel of the mobile operator
1. **Supported operation systems of a mobile phone for Stealthphone Sync software application:** Android 2.3-4.3 (except 4,2), iOS 7, Blackberry OS6 and OS10, Windows Phone 8
2. **Supported operation systems:** Android, iOS, Blackberry, Windows Phone
3. **Supported networks:** GSM, 3G, 4G, EDGE, CDMA, WiFi
4. **Encryption system:** Symmetric keys combined with Diffie –Hellman protocol are used to generate a session key.
5. **Key distribution system.** When this solution is employed, encryption keys are generated by users themselves or by the Stealthphone network administrator. Encryption keys are generated using Stealthphone Key program and encryption keys hardware generator (hardware key generator is additional option). To encrypt different kinds of data between a pair of subscribers its own key is generated for every kind of connection (voice, SMS, chat, data, email). *MTT company does not have access to the encryption keys of users.*
6. **Solution elements:**

Client and server components on the side of a client:

1. Stealthphone Touch or Temptest hardware encryptor
2. Software for Stealthphone Sync mobile device
3. StealthPhone Key program for key generation and distribution
4. Hardware encryption key generator (optionally)
5. License server
6. SIP server
7. Crypto chat server
8. Mail server
9. Теchnical support (On the side of MTT).



Scheme 3. Stealthphone Hard infrastructure solution

1. **General description**

***Key distribution procedure***

Key distribution procedure consists of 3 stages:

**1. MTT company carries out preparation.** As a result of preparation, Stealthphone network administrator is given the file of network identifier and Stealthphone Key program.

**2. Key generation and distribution is** performed by Stealthphone network administrator using Stealthphone Key program. Stealthphone network administrator forms and transfers encryption key files to remote users.

**3. Encryption key loading to Stealthphone Hard or Stealthphone Software** can be performed as the Stealthphone network administrator as a subscriber himself:

* Stealthphone Key program is used by the administrator for key loading.
* To download keys subscribers use Stealthphone Keyloader program ( see Stealthphone Hard user manual for more details). To download keys a subscriber should have encryption key file, encryptor PIN code and Stealthphone Keyloader program.

***Operation principle***



As can be seen from the above, voice and data are encrypted in Stealthphone Soft of the first subscriber, decrypted by the encryptor of the second subscriber and are transferred in the encrypted form between 2 mobile phones. Every subscriber needs to have his own encryptor for confidential connection. It can be either Stealthphone Hard, providing a stronger encryption or Stealthphone Soft software encryptor.

**Voice over GSM operation mode**

Stealthphone Hard in Voice over GSM mode – a unique operation mode of Stealthphone Hard when hardware encryptor provides information crypo security while voice transfer via a standard voice channel of mobile GSM connection.

While voice encryption in GSM mode, encrypted voice is transferred from one subscriber to another via GSM channel of a mobile provider. Therefore Stealthphone Hard allows encrypt voice while a usual phone conversation.

The phone conversation starts in a usual mode without encryption. While a not encrypted conversation is conducted, a subscriber can speak using Stealthphone Hard as well as a mobile phone. Voice encryption can be activated by one of subscribers in any time of a telephone conversation and the second subscriber’s encryptor will automatically be switched to the voice encryption mode. After encryption is activated, conversation is possible only using Stealthphone Hard as a telephone receiver as the encrypted voice of another subscriber will be heard through a mobile phone.

Stealthphone Hard encrypts subscriber’s speech and sends it in the encrypted mode via Bluetooth channel to a mobile phone.

Encrypted speech is transferred via GSM channel of the mobile operator to a mobile phone of the second subscriber and then via Bluetooth channel - to his encryptor, where decryption is carried out.

Only the subscriber who is being talked to can decrypt speech as its own encryption key is provided for every subscriber connection.



As can be seen from the above, voice and data are encrypted in Stealthphone Soft of the first subscriber, decrypted by the encryptor of the second subscriber and are transferred in the encrypted form between 2 mobile phones. Every subscriber needs to have the pre installed Stealthphone Soft software encryptor on his smartphone for confidential connection.

***Advantages***

* **Super strong encryption**

Voice and all the transferred data (text, graphical, video, etc) are encrypted and decrypted in Stealthphone Hard.

The encrypted data is transferred via Bluetooth to a mobile phone (tablet) of a subscriber and via the Internet (mobile operator network or Wi-Fi access point) to another subscriber. While using Stealthphone Hard for data encryption in a computer, Stealthphone Hard is connected to the computer via USB cable.

Encryption carried out in Stealthphone Hard excludes interception of not encrypted speech and possibility of information leak due to the fault of a mobile operator or SIP server administrator.

Stealthphone Hard encryptors are invulnerable for viruses as they work under their own unique operation system control.

* **Separate encryption key matrix for every kind of connection**

Separate encryption key matrixes are used in Stealthphone information security system for every kind of data (voice, SMS, MMS, crypto chat and email messages). Therefore, 5 encryption key matrixes are used in Stealthphone system, which increases the level of crypto security while confidential data exchange.

* **It is not possible to decrypt the transferred voice and data even if a mobile phone is lost or stolen.**

Malicious people will not be able to get access to the data stored in Stealthphone Soft, if a mobile phone is lost or stolen, as encryption keys are stored in Stealthphone Soft in the encrypted form.

Every Stealthphone system subscriber has his own unique set of keys for connection with other subscriber. Therefore, if one encryptor is lost or stolen, it will not have any effect on the security of other subscribers. Encryption keys of connections with this subscriber can be deleted by other Stealthphone network subscribers from their encryptors. Set of keys is formed by Stealthphone network administrator using encryption key generator. It can be easily changed, if it is necessary and the compromised keys can be deleted from the base of encryption keys.

* **Possibility for subscribers to generate encryption key themselves**

In Stealthphone information security system subscribers can generate encryption keys themselves using hardware or software key generator.

Hardware generator provides the strongest crypto security and its work is based on measuring parameters of the physical processes.

Subscribers can check quality of the created keys themselves.

* **Money saving while voice calls**

As in other IP telephony services (Skype, Viber), encrypted voice is transferred via the Internet in Stealthphone system. Thanks to using IP telephony, subscribers can significantly cut costs on calls in roaming during their business trips or holidays.

Using in Stealthphone Soft a unique vocoder based on the specialized voice processor by Texas Instruments allows saving voice quality while transfer with the speed of 4,8 Kbit per second, compared with the voice quality while transfer with speed 9,6 Kbit per second. This solution makes possible to significantly cut the volume of the transferred data if to compare with other IP telephony services, therefore cutting costs on the services of data transfer.

***Protection against attacks***

* **Protection against the attack “man in the middle”**

«Man in the middle» — the attack method when an intruder, having connected to the communication channel between subscribers, wiretaps and actively interferes in the data transfer, deleting and changing it or providing the false information. Subscribers in this situation don’t know they are being attacked.

For security against wiretapping using the method «Man in the middle», the security code of 5 figures is displayed on the screen of a mobile phone in the beginning of the encrypted conversation. The same code should be displayed on the screen of the other subscriber.

05073

Outcoming call

subscriber 2

An example of the code. A new code is created every t ttime timetime

* In the beginning of every conversation a user should match the security code on his mobile phone screen with the code of the second subscriber. If the security codes of the first and the second subscribers are different, the subscribers are being attacked with the method “man in the middle”. In this case it is necessary to stop the conversation and make the second voice call to a subscriber until the codes are the same.
* **Speech-like noise**

A malicious person can remotely activate the microphone of a mobile phone and wiretap speech and all sounds near the mobile phone. For protection against such wiretapping, switch on the function “Speech-like noise” in Stealthphone Sec. Then during the encrypted conversation a speech like noise will be produced from the dynamic of your mobile phone (tablet). A malicious person will hear only a speech-like noise and not the conversation and other sounds near the mobile phone when he tries to wiretap.

MTT company research showed that the dynamic spectrum of a mobile phone microphone is broader than the spectrum of a dynamic. Therefore, for a reliable suppress of voice harmonics it is necessary to put a mobile phone with Stealthphone Sec application into a thick case. In this case a subscriber can be sure that all conversations near the mobile phone are reliably secured against wiretapping through the microphone of a mobile phone.

When the microphone of a mobile phone (tablet) is switched on, voice harmonics are directed to its antenna and make effect to the signal eliminated by the antenna. Malicious people using special technical equipment can take the signal from antenna and separate voice harmonics, therefore getting speech record.

Speech-like noise function protects subscribers using Stealthphone Hard against wiretapping their speech through taking out a directed microphone signal from the mobile phone antenna. The signal with speech-like noise goes to the microphone and it is not possible to separate speech out of it.

* **Security against interference into the encrypted conversation**

A third person cannot interfere into the encrypted conversation as it happens with the usual phone connection, because the operation principle of Stealthphone system guarantees consistency of the transferred information.

1. **Compatibility with other products and solutions of MTT company**

In addition to StealthPhone Software product the following products and solutions can be purchased:

Encryption keys hardware generator;

Stealthphone Hard hardware generator;

Solution for security of the office network Stealthphone Office Gate;

Solution for security Stealthphone VPN;

Secure Android.

1. **Price:**
2. **Product development.** For ensuring product availability in different regions, StealthPhonе Hard needs to have a far-reaching distribution network (partners-distributors networks) and networks of the system integrators-partners specializing in the information security.

### Stealthphone CryptoDisk

Stealthphone CryptoDisk – an additional option of Stealthphone Hard, hardware and software solution which provides data encryption on a hard disk in computer using Stealthphone Hard connected via USB.

* + - 1. **Functional capabilities:**

Stealthphone CryptoDisk software allows storing encrypted data in a file container or a portable USB drive.

The file container can be assembled in the Windows system as a virtual disk. While data recording to this disk, the data is encrypted through Stealthphone Hard hardware encryptor connected to a PC via USB cable and is saved to the file container in already encrypted form. While data reading from the virtual disk, files are decrypted on Stealthphone Hard device.

In a similar way, after data encryption on a USB drive - while data recording to this USB drive, the data is encrypted through Stealthphone Hard hardware encryptor connected to a PC via USB cable and is saved to the USB drive in already encrypted form. While data reading from the encrypted USB drive, files are decrypted on Stealthphone Hard device.

* + - 1. **Product components**
			2. Stealthphone CryptoDisk application
			3. Stealthphone Hard
			4. **System requirements:**
1. Windows Server 2003;
2. Windows XP x86;
3. Windows Vista x86;
4. Windows Vista x64;
5. Windows 7 x86;
6. Windows 7 x64;
7. Windows 8;

## Stealthphone Office Gate

**Stealthphone Office Gate** –software and hardware solution for secure information exchange between corporate local network (telephone IP) and remote subscribers using Stealthphone Software or Stealthphone Hard solutions.

Voice and data security is carried out while information transfer via open channels between Stealthphone Office Gate and a subscriber using Stealthphone Software or Stealthphone Hard. The data is transferred in a not encrypted way within the office network.

1. **Functional capabilities:**

Stealthphone Office Gate information security system provides crypto security of the following information in mobile phones and tablets:

1. Voice.
2. Data:
* SMS.
* Email.
* Crypto chat (text messages and files exchange between two subscribers) and crypto conference (text messages exchange between two and more subscribers).
* Files.
1. **Supported operational systems:** \*nix
2. **Supported networks:** Wi-Fi, Internet
3. **Product components:**
4. SIP server OfficeGate
5. Entirely implemented solution Stealthphone Hard or Stealthphone Software.



1. **General description**

***Stealthphone OfficeGate operation algorithm***

* + - 1. An outside subscriber of Stealthphone corporate crypto network makes a secure call to the office using Stealthphone Hard or Stealthphone Software solution;
			2. The call goes to Stealthphone OfficeGate server where it is decrypted and transferred to the office ATS in the open way.

A back call from the office to the outside subscriber of the corporate crypto network is made in a reversed order.

1. **Соmpatibility with other products.**

In addition to StealthPhone Software the following products and solutions can be used:

Solution for Stealthphone VPN security;

Secure Android.

1. **Price:**

## Secure Android

[Secure Android](#_Secure_Android) (see division «Solution for information systems security of small and medium businesses»).

## Stealthphone VPN

[Stealthphone VPN](#_Stealthphone_VPN) (see division «Solution for information systems security of small and medium businesses»).

## StealthPhone Key

[StealthPhone Key](#_StealthPhone_Key) (see division «Solution for information systems security of small and medium businesses»).

### Hardware key generator

Hardware key generator (see division «Solution for information systems security of small and medium businesses»).

## Certification authority

Certification authority (see division «Solution for state information systems security»).

## Server platform

Server platform (see division «Solution for state information systems security»).

## FileHider

**FileHider** is an application enabling you to hide confidential information (even encrypted) on a digital media.

The application hides the files using stenography method, i.e. randomly injecting bytes of files to be hidden into a container file. The process changes the container file insignificantly without affecting the file size and structure, therefore enabling you to use the container file as usual.

You may use audio, video, and image files as containers.

# Solutions for state information systems security

## Server platform

At customer’s wish, MTT company can prepare a server platform including the following components:

* SIP server
* Mail-server
* Crypto chat server
* Billing server.

## Certification authority

**Certification authority (CA)** – a software product which is a subsystem of StealthPhone hardware and software information security system.

The mission of CA software solution is managing asymmetric crypto keys and user digital certificates for their identification and secure information exchange between users.

CA is a party whose honesty is unquestionable and whose public key (CA certificate) is known to the participants of crypto network. The task of CA is to confirm the authenticity of encryption public keys using digital signature.

**СA components:**

1. Data base server
2. Software product for producing, storage and managing user keys

# Services

## Consultations on information security

## Trainings on information security