STEALTHPHONE

INFORMATION SECURITY SYSTEM

MOBILE TRUST TELECOMMUNICATIONS

STAY INVISIBLE IN THE DIGITAL WORLD

Anatoly Klepov

General Director of Mobile Trust Telecommunications with more than 40 years of experience in the field of cryptography. Cryptographic algorithm developed by Anatoly Klepov was certified by Swedish Kungliga Tekniska Hogskolan (KTH) Royal Institute of Technology

Johan Hastad, the leading cryptographist who analyzed the algorithm, acknowledged that the algorithm cannot be broken in less than the age of the universe.

South African Communication Security Agency also analyzed Mr. Klepov's cryptoalgorithm and acknowledged its endurance.

https://www.facebook.com/GroupMTT

https://www.linkedin.com/company/mobile-trust-telecommunications

https://twitter.com/mtt_group

Mobile Trust Telecommunications AG

Usterristrasse 11
8001 Zurich, Switzerland
Tel: + 41 44 21 03 743
E-mail: info@mttgroup.ch
URL: www.mttgroup.ch

INFORMATION SECURITY SYSTEM FOR MOBILE DEVICES AND PCs

A UNIQUE TECHNOLOGY DEVELOPED BY MOBILE TRUST TELECOMMUNICATIONS (MTT)

INFORMATION SECURITY SYSTEM FOR MOBILE DEVICES AND PCs

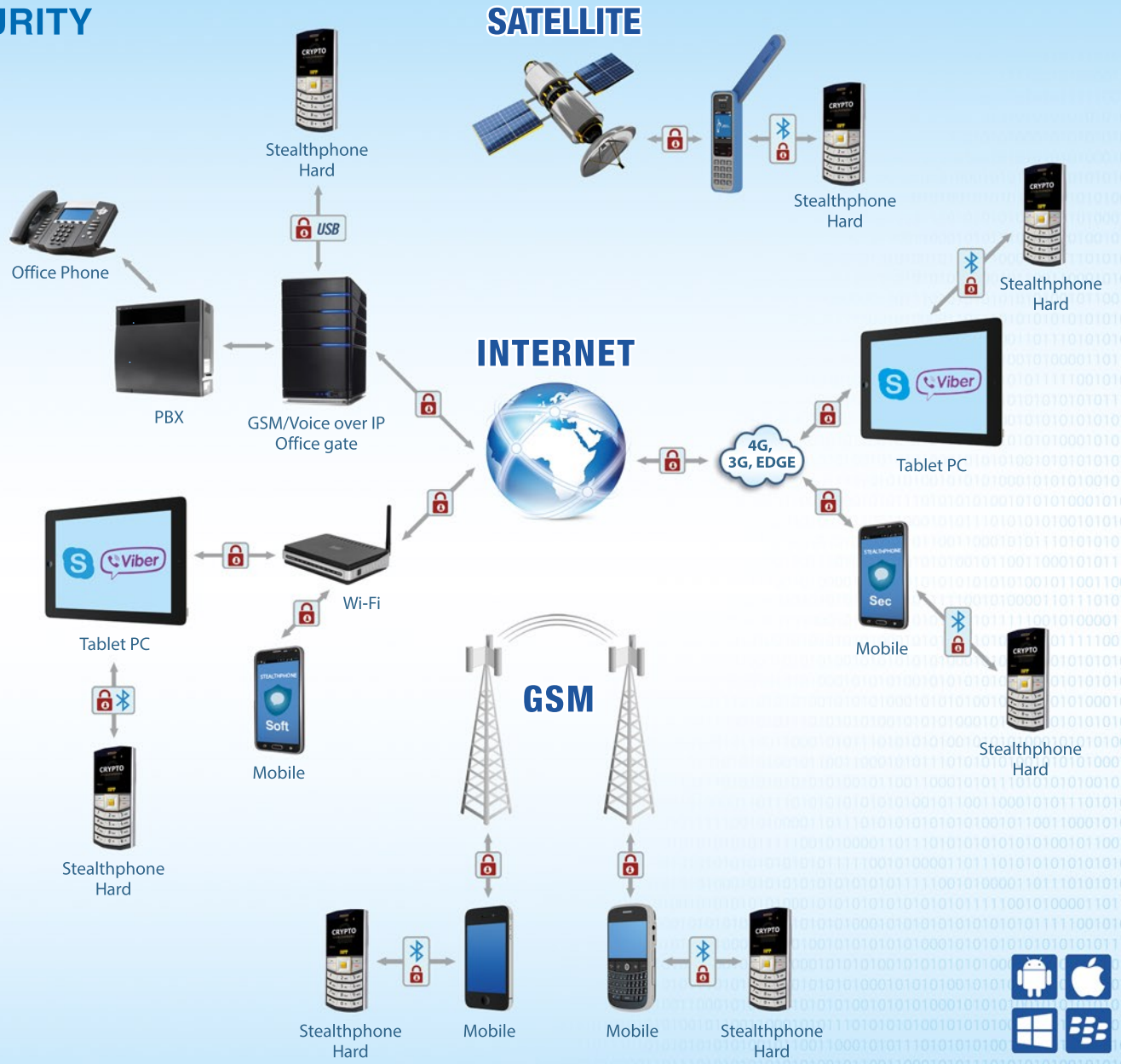
- Calls
- E-Mails
- SMS/Chat
- Notes, documents
- Money transaction
- Credit card PIN-code
- Skype, Viber
- Facebook, Twitter, LinedIn
- BYOD

STEALTHPHONE INFORMATION SECURITY SYSTEM IS DESIGNED FOR:

- State organizations
  (army, police, governmental organizations, etc.)
- Corporations (banks, financial organizations, medical, legal companies, etc.)
- Small and medium business
- Individual users

For the first time in the world the Swiss company Mobile Trust Telecommunications (MTT) has created STEALTHPHONE information security system on the basis of hardware encryptor STEALTHPHONE HARD, which provides the guaranteed information security for mobile phones and computers.

Confidential information can be transferred in an encrypted mode via STEALTHPHONE IP network as well as via external communication networks (GSM, Skype / Viber, satellite, landline) thanks to “Crypto voice over GSM”, a unique technology developed by MTT company.



STEALTHPHONE INFORMATION SECURITY SYSTEM FOR MOBILE PHONES

Confidential information security in mobile phones is provided by means of super strong hardware encryptor STEALTHPHONE HARD.

STEALTHPHONE HARD is a handheld device designed for:

- Encryption of voice transferred via GSM networks, IP-telephony systems (Skype / Viber), satellite and landline communication networks

- Voice and data encryption (e-mail, instant messages, sms, files, cryptochat, cryptoconference) transferred over STEALTHPHONE IP servers

- Data encryption inside the device (on the embedded SD card of STEALTHPHONE HARD and in the memory of a mobile phone)

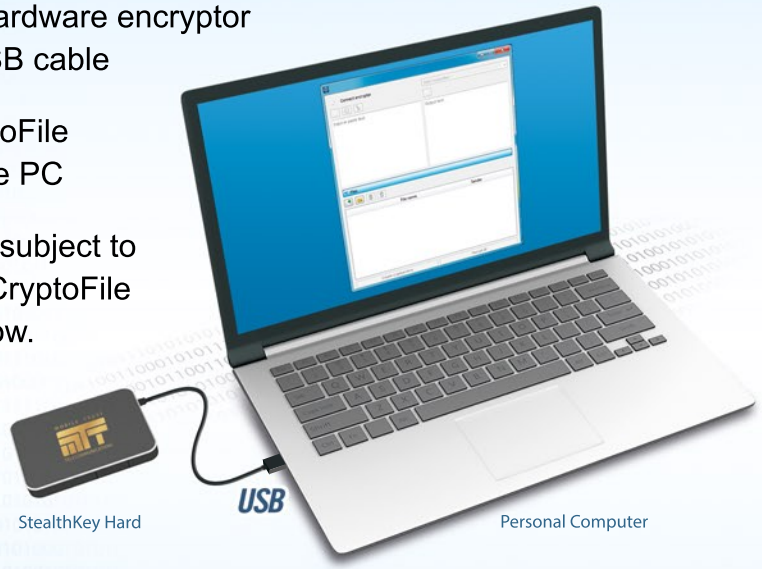
STEALTHPHONE HARD is compatible with mobile phones operating under Android, IOS, Windows phone and Blackberry.

STEALTHPHONE INFORMATION SECURITY SYSTEM FOR COMPUTERS

CRYPTOFILE – is the option of STEALTHPHONE HARD that allows you to encrypt files on your computer.

It is necessary to do the following to encrypt data using CryptoFile:

1. Connect the hardware encryptor to a PC via USB cable
2. Start the CryptoFile program on the PC
3. Move the files subject to encryption to CryptoFile program window.



Information is transferred to the encryptor from the CryptoFile program, then, already encrypted, it is transferred back to CryptoFile and is stored in the PC in an encrypted mode.

With the help of CryptoFile you can easily transfer confidential information in an encrypted mode using any usual way – email message, social networks (Facebook, Linkedin, etc.), Google Talk, ICQ and so on.

CRYPTODISK - is an option of STEALTHPHONE HARD that enables to encrypt logic drives on your computer.

To encrypt data using CryptoDisk it is necessary to do the following:

1. Connect the hardware encryptor to a PC via USB cable
2. Start the CryptoDisk program on the PC
3. Create one or more crypto containers on the PC using the CryptoDisk program.

When creating a crypto container in the STEALTHPHONE HARD a unique key is created automatically. PIN-code (a number of 8 to 20 digits) is used to secure access to crypto container.

If needed, the immediate deletion of encrypted information is performed within 3-5 sec.

STEALTHPHONE INFORMATION SECURITY SYSTEM FOR COMPUTERS

CRYPTO E-MAIL – is an option of the STEALTHPHONE HARD that enables to secure emails transferred via Microsoft Outlook program.

To secure e-mail using Crypto E-mail option it is necessary to do the following:

1. Install STEALTHPHONE E-mail plug-in for Microsoft Outlook
2. Connect the STEALTHPHONE HARD to PC via USB
3. Run Microsoft Outlook program on PC

Your counterpart gets an encrypted message and decrypts it using only one button.

OPERATING STEALTHPHONE HARD IN CRYPTO VOICE OVER GSM MODE

Crypto voice over GSM is a unique technology of the Mobile Trust Telecommunications (MTT) company, which has no rivals in the world. Crypto Voice over GSM technology allows making encrypted calls even without the Internet access. When there is no access to the Internet, Crypto voice over GSM provides guaranteed security of your telephone conversation from wiretapping. Your voice is encrypted and transferred to another subscriber via regular Voice GSM channel. Voice signal is encrypted in STEALTHPHONE HARD and transferred in an encrypted mode via Bluetooth to a mobile phone.

YOUR TELEPHONE IS SECURE AGAINST WIRETAPPING BY INTRUDERS

No additional software is needed. Voice encryption is performed using a separate device – STEALTHPHONE HARD, which every subscriber has to have. When the Internet access is available, the STEALTHPHONE HARD can be switched from Crypto Voice over GSM to Crypto Voice over IP mode.

USING STEALTHPHONE HARD IN CRYPTO SKYPE, CRYPTO VIBER MODE

CRYPTO SKYPE, CRYPTO VIBER – is a technology for secure transfer of your voice in an encrypted mode over the Internet network using IP telephony programs: Skype, Viber.

During regular conversations via Skype and Viber information goes through many servers in the Internet network. Your conversation can be intercepted at any time and wiretapped by malicious persons.

If you use STEALTHPHONE HARD, your conversation via Skype and Viber guaranteedly cannot be wiretapped, as your voice goes through the servers located in the Internet previously encrypted.

To make an encrypted call, the STEALTHPHONE HARD is connected to a mobile phone as a normal Bluetooth headset.

You don’t need to install any additional programs on your mobile phone or computer to make secure conversations – you use a usual Skype, Viber interface.

STEALTHPHONE HARD FOR SECURITY OF VOICE TRANSFERRED VIA EXTERNAL NETWORKS

USING STEALTHPHONE HARD FOR SECURITY OF VOICE TRANSFERRED OVER SATELLITE AND ANALOG TELEPHONE NETWORKS

During regular conversations over satellite or analog networks, a voice signal can be intercepted in any time and wiretapped by malicious persons.

If you use STEALTHPHONE HARD, your conversation guaranteedly cannot be wiretapped, as your voice signal goes through the satellite communication channels and analog networks in previously encrypted mode.

To make an encrypted call, the STEALTHPHONE HARD is connected to a satellite or analog phone as a regular Bluetooth headset.

You don’t need to install the additional programs on your satellite or analog phone.

STEALTHPHONE HARD FOR SECURITY OF VOICE AND DATA (E-MAIL, INSTANT MESSAGES, SMS, FILES, CRYPTOCHAT, CRYPTOCONFERENCE) TRANSFERRED OVER OWN STEALTHPHONE'S IP SERVERS

CRYPTO VOICE OVER IP TECHNOLOGY

Provides voice and data encryption as well as its transfer via the Internet using own Stealthphone IP network. Internet connection is executed via 3G, 4G, CDMA or Wi-Fi.

STEALTHPHONE HARD secures your data making it available only to your counterpart using another STEALTHPHONE HARD device. Data is transferred to our company's servers in an encrypted form.

In order to provide secure phone conversations for your company, you can use both STEALTHPHONE SOFT solution and STEALTHPHONE HARD (maximum level of security for top managers of your company). They are fully compatible.

STEALTHPHONE HARD employs the noise suppression function of a mobile phone microphone.

It is possible to use our servers as well as purchase your own communication servers in our company for the maximum security.

ENCRYPTION KEY GENERATION AND DISTRIBUTION IN THE STEALTHPHONE INFORMATION SECURITY SYSTEM

Encryption keys should be loaded on STEALTHPHONE HARD or to STEALTHPHONE SOFT before it is used.

Encryption keys are generated and distributed using STEALTHPHONE KEY SYSTEM.

An authorized person – Stealthphone network administrator - controls STEALTHPHONE KEY SYSTEM.

STEALTHPHONE INFORMATION SECURITY SYSTEM is resistant to the loss or theft of private devices of STEALTHPHONE network subscribers.

ADVANTAGES OF STEALTHPHONE KEY SYSTEM:

- Encryption keys for every subscriber are created by Stealthphone network administrator and stored only in STEALTHPHONE HARD
- STEALTHPHONE KEY HARD hardware random numbers generator is used to generate encryption keys

STEALTHPHONE CRYPTO OFFICEGATE

STEALTHPHONE OFFICEGATE is recommended for use in state organizations and big corporations.

STEALTHPHONE OFFICEGATE is a solution for corporate clients, which provides a secure access to the office telephone network (IP, digital or analog phones) for subscribers of STEALTHPHONE INFORMATION SECURITY SYSTEM. Voice security function is implemented on the basis of STEALTHPHONE HARD.

STEALTHPHONE OFFICEGATE presents a crypto gateway, which provides encrypted voice connection between network subscribers using STEALTHPHONE HARD or STEALTHPHONE SOFT and office telephone network subscribers, who use IP, digital or analog phones.

Several OFFICEGATE systems can be installed within one STEALTHPHONE NETWORK (for example, in different offices of a company). In this case encrypted calls may be made not only between the office and a mobile phone of a STEALTHPHONE NETWORK subscriber, but between several offices as well.

Connection can be established over both IP and GSM channels.

STEALTHPHONE OFFICEGATE FUNCTIONS:

- Receipt of encrypted incoming calls from STEALTHPHONE NETWORK subscribers, decoding and transfer to the office telephone station in a clear form
- Making outcoming encrypted calls from any office phone of the office station to mobile phones of STEALTHPHONE NETWORK subscribers
- Making encrypted calls between two offices of the company (if several OFFICEGATE systems are available)

CRYPTOROUTER MTT-GW

CRYPTOROUTER MTT-GW is a device designed for security of secret and confidential information transferred between different offices of your corporation over the Internet network.

CRYPTOROUTER MTT-GW is a super strong crypto hardware security device which combines several technologies – crypto security, firewall, etc.

Advantages and the main functions of CRYPTOROUTER MTT-GW:

- Traffic routing;
- Crypto security of communication channels;
- Integrity control of the transferred information;
- VPN-server for remote clients access;
- Firewall and network segmentation;
- Separate service data channels;
- Intrusion detection and prevention system.

SERVER PLATFORM

SERVER PLATFORM is a communication component of the STEALTHPHONE INFORMATION SECURITY SYSTEM which includes:

- SIP- server. Provides transfer of the encrypted voice between Stealthphone network subscribers over the Internet network (Voice over IP)
- E-mail server. Provides encrypted email messages exchange
- JABBER-server. Provides encrypted instant messages exchange with support of transferring encrypted files of any format

Advantages of the MTT company's server platform:

- Easy and quick registration of clients on SIP-, Mail- and Jabber servers
- Easy and convenient configuration and server service
- Storage of statistics on clients work with the platform and provision of full and secure access to the statistics for clients
- High quality technical support of clients

BYOD

When employers use their own mobile devices in work purposes, it poses risk to the leakage of confidential information outside the organization.

It can lead to financial losses for the corporation.

Using hardware encryptor STEALTHPHONE HARD with STEALTHPHONE SEC or STEALTHPHONE SOFT programs installed on your mobile phone, you can distinguish the access to personal and corporate information of employees having implemented BYOD (Bring Your Own Device) technology.

Today 89% heads of IT departments in small and medium companies all over the world support BYOD.

BYOD security measures:

- Providing reliable passwords on all devices
- Antivirus protection
- Prevention of data leakage
- Removal of confidential data if the device is lost or stolen
- Control of all applications

SOFTWARE SOLUTION OF STEALTHPHONE SECURITY SYSTEM FOR MOBILE PHONE

STEALTHPHONE SOFT

STEALTHPHONE SOFT application for mobile phones is a software solution emulating functions of STEALTHPHONE HARD while operating in own Stealthphone IP network.

It is possible to use STEALTHPHONE SOFT application and STEALTHPHONE HARD simultaneously in one network as they are fully compatible.

STEALTHPHONE SOFT PROVIDES ENCRYPTION OF:

- Voice
- Sms messages
- Instant messages, files
- E-mails