STEALTHPHONE

INFORMATION SECURITY SYSTEM

MOBILE TRUST

TELECOMMUNICATIONS

STEALTHPHONE HARD (BM-700)

CRYPTOGRAPHIC FUNCTIONS

- Voice encryption
- SMS / E-MAIL encryption
- Cryptochat / cryptoconference
- Storage of encrypted information on Stealthphone built-in SD card
- Encryption of data stored on PC
- Stealthphone Token

STEALTHPHONE HARD (BM-700)

Display:
Screen type: colored OLED display, 256 colors
Diagonal: 2"
Resolution: 128*160

Keyboard:
Keyboard type: mechanical
Number of keys: 20 (12 keys to input numbers and symbols, 8 function keys)

Operating system:
Low-level OS, a proprietary OS developed by MTT company

Power:
Battery type: Li-Ion
Capacity: 1500 mAh

Battery life:
•Voice encryption mode — 360 minutes
•Standby mode — 340 hours

Interfaces:
To connect to PC: USB (mini-USB)
To connect to mobile devices: Bluetooth 2.1 (KMBT007)

Processor:
Control processor: NXP LPC4337 Cortex-M4 200 MHz.
Crypto coprocessor: Texas instruments TMS320C5515 120 MHz
(Crypto coprocessor provides access to encryption keys, data encryption and decryption, processing of encrypted data in voice communication mode).

Memory:
•SD card for storing encryption keys (4 GB micro SD-card).
Only the crypto coprocessor can access the SD-card. It guarantees secure key storage.

•SD-card for data storage (32 GB micro SD-card).

Other features
•Hardware random number generator FDK RPG100
(It is connected to the crypto coprocessor to provide reliable random number generation, which is not subject to environmental influences and is necessary for the secure operation of encryption algorithms).

•Hardware real-time clock RTC Maxim DS1342U+

•Audio codec Texas instruments TLV320AIC3204
(Provides input and output of voice signals processed by crypto coprocessor)

•Hardware noise canceller BR262W30A103E1G
(improves the quality of a voice signal)

•Dimensions — 119 x 56 x 11 mm

•Weight — 129 g

EMCC ™
DR. RAŠEK

Notified Body Directive 99/5/EC
Notified Body EMC Directive 2004/108/EC
RFCAB under the Japan-EC MRA
FCB under the Canada-EC MRA
TCB under the USA-EC MRA

EC Identification No. 0678

Bundesnetzagentur

Recognized by the German Regulator
to act as a Notified Body in accordance with the
R&TTE Directive 1999/5/EC of 9. March 1999

BNetzA-bS-02/51-54

R&TTE STATEMENT OF OPINION

Registration No. G110371F

Certificate Holder
MOBILE TRUST TELECOMMUNICATIONS AG
Usteristrasse 11
8001 Zurich
Switzerland

Product Designation
Bluetooth encryption and decryption device, Model BM-700
Frequency Range: 2402 – 2480 MHz
Transmit Power: 3.38 dBm EIRP
Modulation Type: GFSK, π/4DQPSK, 8DPSK
Power Adapter: FJ-SW105

Product Description
Bluetooth device

Manufacturer
Victronics CO., LTD.
36, Samjak-ro, 144 beon-gil, Ojeong-gu
Bucheon-city, Kyunggi-Do
South Korea

Essential Requirement		Applied Specifications / Standards	Documentary Evidence	Result
Art. 3.1(a)	Health	Not assessed	-	-
Art. 3.1(a)	Safety	EN 60950-1+A11+A1+A12	Test Report F690501/RF-SAF007177 Test Report 17022866 002	conform
Art. 3.1(b)	EMC	EN 301 489-1/-17 EN 55022+AC, EN 55024	Test Report F690501/RF-EMG005388	conform
Art. 3.2	Radio	EN 300 328	Test Report F690501/RF-RTL008255	conform

The product shall be marked with the CE conformity marking
and our Notified Body number as shown on the right.

CE 0678

The scope of evaluation relates to the submitted documents only.

This Statement of Opinion is issued in accordance with Annex IV of the R&TTE Directive 1999/5/EC of 9th March, 1999 and is only valid in conjunction with the attached Annex.

Unterleinleiter,
2015-02-02

Christoph Schmidt
Notified Body

GERMAN NOTIFIED BODY · DEUTSCHE BENANNTE STELLE ·

Technical Construction File (TCF) Details

To demonstrate conformity with Article 3.1(a) Safety

Applied Standards	Version	Applied Standards	Version
EN 60950-1+A11+A1+A12	2011		

Report or Certificate No.	Issue Date	Issued by
F690501/RF-SAF007177	2015-01-19	SGS Korea Co., Ltd.
17022866 002	2013-01-28	TÜV Rheinland (Shenzhen) Co., Ltd.

To demonstrate conformity with Article 3.1(b) EMC

Applied Standards	Version	Applied Standards	Version
EN 301 489-1	V1.9.2	EN 55022+AC	2011
EN 301 489-17	V2.2.1	EN 55024	2010

Report or Certificate No.	Issue Date	Issued by
F690501/RF-EMG005388	2015-01-05	SGS Korea Co., Ltd.

To demonstrate conformity with Article 3.2 Spectrum Efficiency

Applied Standards	Version	Applied Standards	Version
EN 300 328	V1.8.1		

Report or Certificate No.	Issue Date	Issued by
F690501/RF-RTL008255	2014-12-11	SGS Korea Co., Ltd.

Declaration of Conformity

Signed by	Date
Anatoly Klepov	2014-01-15

Technical Documentation

Block diagram
Parts list
External / Internal photos
Schematic diagram
User Manual

EMCCert DR. RAŠEK GmbH • Stoernhofer Berg 15, 91364 Unterleinleiter, Germany
Tel.: +49 9194 72279-01 • Fax: +49 9194 72279-06 • E-mail: emc.cert@emcc.de • Web: www.emcc.de

OUR SECURITY IS YOUR SECURE FUTURE

Mobile Trust Telecommunications (MTT) present the super strong cryptographic Stealthphone information security system, which secures the information transferred through mobile phones, computers, satellite systems and VHF/UHF radio transmitters, based on the hardware encryptors developed in accordance with the TEMPEST standard.

Stealthphone information security system deploys Voice over IP technology which significantly decreases the cost of the information transfer.

- Stealthphone provides the super strong cryptographic security for the following kinds of information: voice, data, images, and video
- Using hardware encryption and providing the possibility for the users to store keys themselves, Stealthphone excels the popular programs Skype and Viber in the level of cryptographic data protection
- Stealthphone is designed for those who want to secure their information from the most high tech enemies in the world!

Meet Stealthphone, the technology worthy of the 21th century!

THE REASONS TO TRUST US

- **Mobile Trust Telecommunications (MTT)** company manufactures crypto devices using the technologies of military and government level in the area of information security

- The crypto algorithms of **Mobile Trust Telecommunications (MTT)** company were certified by state organizations of neutral countries (South African Republic and Sweden). No other cryptographic company has achieved the same results

THE TECHNOLOGIES USED BY MOBILE TRUST TELECOMMUNICATIONS (MTT) COMPANY

Crypto security technologies

- Encryption and Decryption
- Symmetric-Key Encryption Algorithms
- Asymmetric Encryption Algorithms or Public Key Algorithms
- Authentication, Integrity and Non-Repudiation
- Weak Authentication of Parties (Passwords)
- Strong Authentication of Parties (Request –Response Schemes)
- Zero Knowledge Protocols
- Hash Function and Data Integrity
- Digital Signature
- Steganography
- Hardware-Software Key Generation

Intranet/Internet technologies

- Private virtual networks
- Information security in Internet/Intranet
- VoIP (Voice over IP)
- Firewall
- Crypto routers
- Higher level of identification procedures in communication networks

"CYBER THREAT IS ONE OF THE MOST SERIOUS ECONOMIC AND NATIONAL SECURITY CHALLENGES WE FACE AS A NATION. AMERICA'S ECONOMIC PROSPERITY IN THE XXI CENTURY WILL DEPEND ON CYBER SECURITY"

U.S. President Barack Obama, 29.05.2009

Products of Mobile Trust Telecommunications (MTT) company were created using information security technologies which were a step ahead of the potential threat

Data security

- Crypto secured email, the result of the cooperative work with Samsung company
- Hardware device for security from unauthorized access to PC
- Software for data encryption on PC
- Software for data encryption on CD, HD, USB and between PCs
- Crypto chips developed by Mobile Trust Telecommunications (MTT) company to encrypt information on PCs
- Security HD designed for Windows. Data stored on this secret disk are fully encrypted, including file names and directories
- Portable encryption devices for processing super secret information, developed according to TEMPEST standard

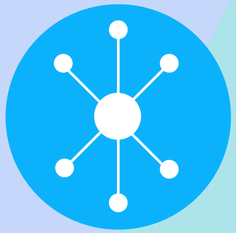
Voice and telephone communication security

PSTN encryptor

ISDN encryptor

Crypto secured GSM phone

Information security in Internet / Intranet



VPN –soft/hardware complex to provide data security for LAN and corporate networks.

PRODUCT

Security of radio networks

The device guarantees the high level of voice encryption for VHF/UHF radio transmitters on board aircraft (including supersonic jets), helicopters, armored cars, ships and for ground communication centers. The device uses the unique noise-suppression system

Certification authority

We created the system which can verify keys, using electronic digital signature certificates. The certification center of Mobile Trust Telecommunications (MTT) company uses the following algorithms: RSA Electronic signature algorithm with key length of 4096 bit and “Tiger” encryption algorithm, developed by Mobile Trust Telecommunications (MTT) company with key length of 256 bit

Stealthphone Token

Stealthphone encryption device can be used as a USB key for secure storage of personal information and reliable security from unauthorized access. It enables to encrypt data, voice, video and email messages transferred from computers and mobile phones as well as to sign documents with an electronic digital signature to prevent their modification

Hardware-software key generation and distribution of encryption keys

We developed the system where the users can generate and distribute encryption keys themselves using hardware or software key generator. The secret symmetric key matrix provides the maximum strength of the encryption system

"MOBILITY ISN'T SAFE. REPEAT AFTER ME: MOBILITY ISN'T SAFE. IT REALLY ISN'T."

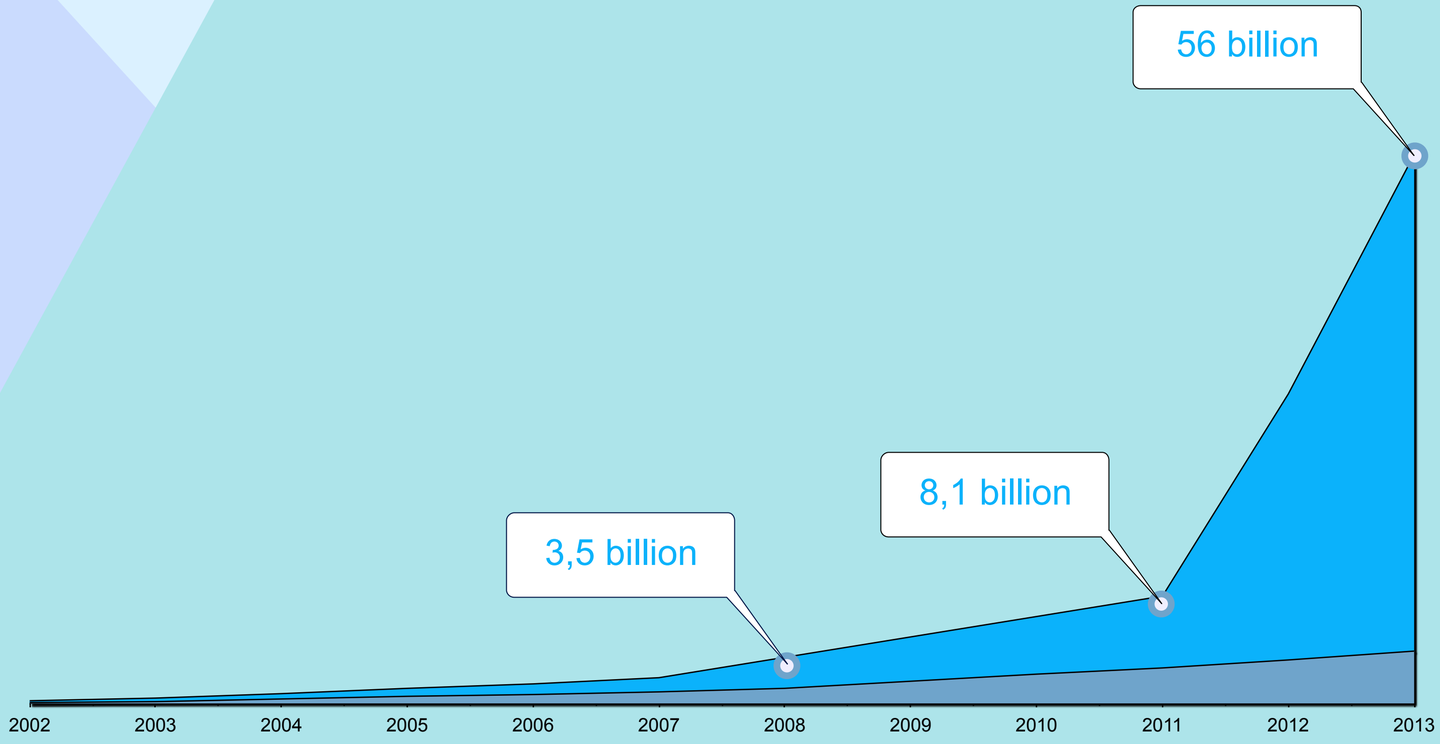
Gus Hunt, CIA Chief Technology Officer. Speech at the conference, 20.03.2013.

The catastrophic situation in the field of mobile phone information security

According to «Symantec», hackers got a fantastic profit of $ 400 billion in 2012, which exceeded the income of criminal drug dealers and illegal arms dealers. It is due to the fact that technical means hackers are armed with today to intercept and tap cell phones, e-mail, social networks and Internet servers is as powerful as the equipment of the best state secret services.

Over the past 6 years mobile phones of 30 heads of state and hundreds of thousands of political activists, businessmen, bankers, judges, actors and journalists have been illegally intercepted. It caused major political and economic crises in those countries.

For example, hackers can check 56.000.000.000 passwords per second. Just a few years ago only processors in the research centers of the developed countries had the same efficiency. That's why it is assumed that 90% of passwords to emails and social network accounts will be cracked all over the world by 2014.

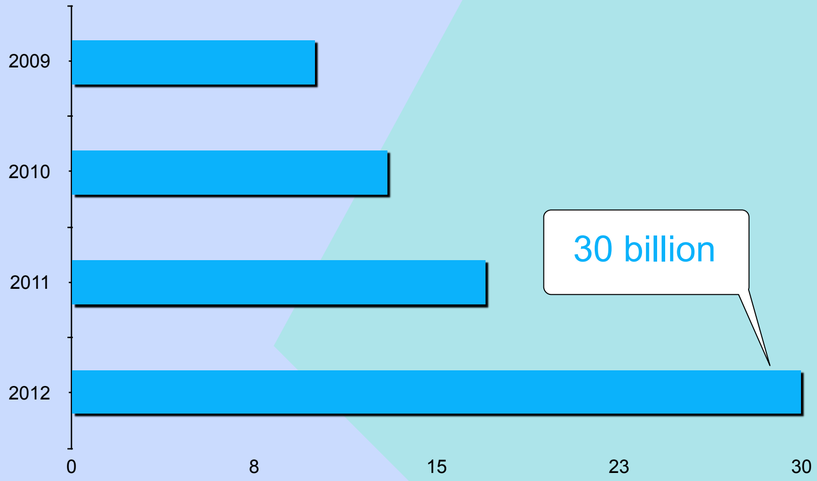


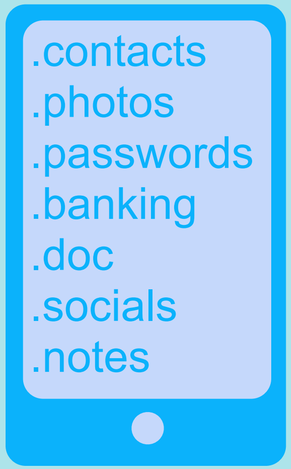
"MOBILITY ISN’T SAFE. REPEAT AFTER ME: MOBILITY ISN’T SAFE. IT REALLY ISN’T.”

Gus Hunt, CIA Chief Technology Officer. Speech at the conference, 20.03.2013.

According to the mobile security provider Lookout Inc., the total cost of mobile phones, stolen in the United States in 2012, is estimated at $30 000 000 000.

The average cost of data, stored in the stolen mobile phones, may be calculated on the basis the Counterworks research: it was worth $ 37,000. Thus, only in the United States the total cost of the stolen information, stored in the mobile phones, is 222 billion dollars. We can only assume that the cost of information stolen from mobile phones or lost all over the world every year is much more than one trillion dollars.





average cost:

37 000 $

"MOBILITY ISN’T SAFE. REPEAT AFTER ME: MOBILITY ISN’T SAFE. IT REALLY ISN’T.”

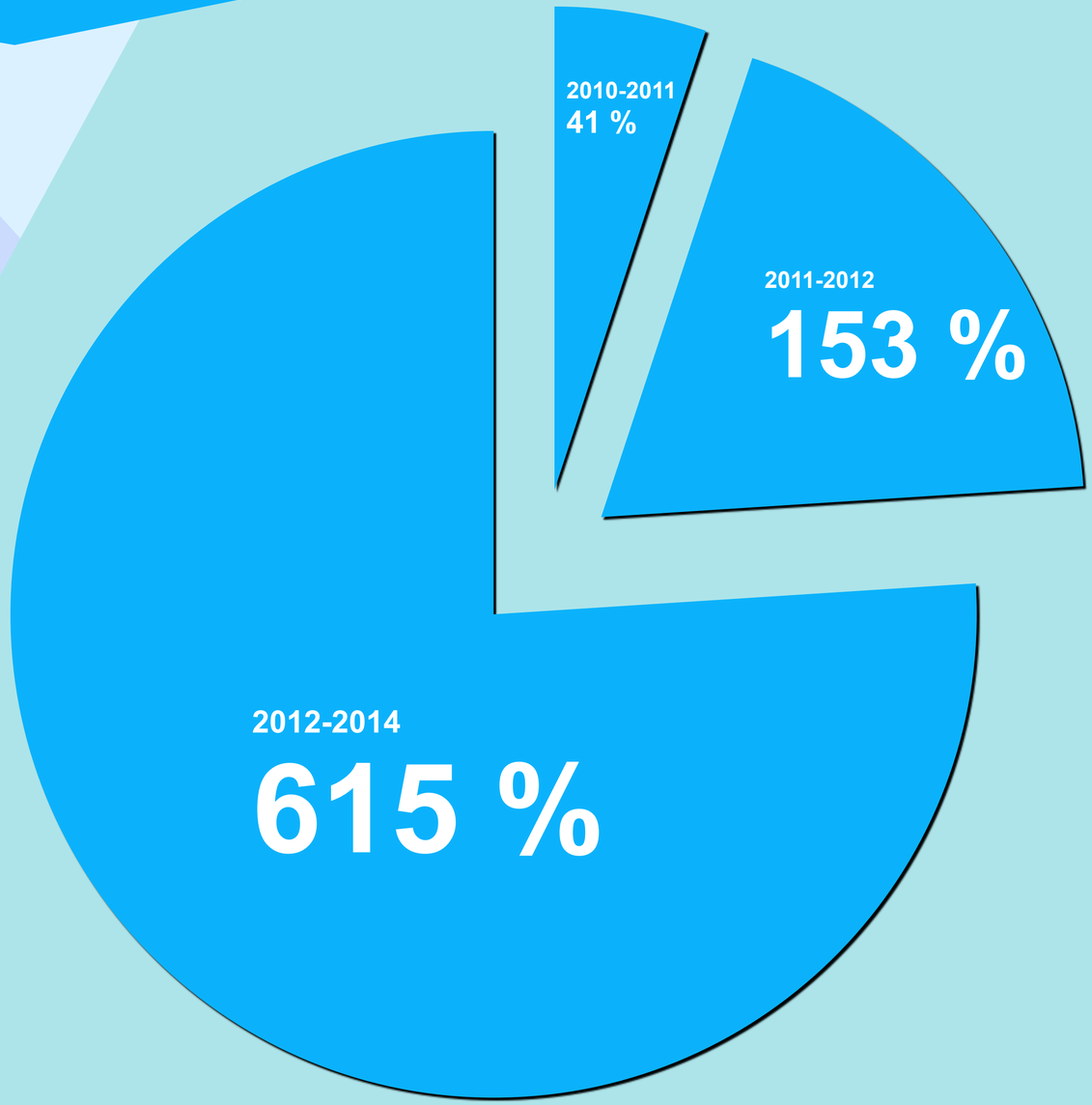
Gus Hunt, CIA Chief Technology Officer. Speech at the conference, 20.03.2013.

Smartphone sales are significantly growing. 210 million smartphones were sold worldwide in the first quarter of 2013 - 2.3 million more, than in the fourth quarter of 2012.

Smartphones are widely used, and mobile malware is getting more sophisticated. Most of the dangerous viruses are remotely intentionally entered into devices. It greatly improves theft efficiency. So just in the last two quarters of 2012 the number of specific mobile threats increased by 261%.

The risk of mobile phone virus attacks increases, because 80% of Internet connections will be performed using mobile phones or a tablet PCs by 2014.

The current situation in the field of information security of mobile phones becomes more complicated, because in pursuit of super-profits and low production costs many manufacturers of traditional information security systems offer mainly security software, which cannot reliably defend users’ information against hackers.



MAIN MOBILE SECURITY THREATS

- Interception and eavesdropping on subscribers’ conversations
- Falsification of subscribers’ speech in order to compromise them
- Delivery of SMS and MMS messages with viruses, which steal data
- Unauthorized access to a mobile phone
- Malware, which executes commands without subscriber’s authorization
- False authentication and authorization – unauthorized access to information by means of caller ID falsification
- False base stations – IMSI catcher reduces the standard encryption level and facilitates interception and eavesdropping of mobile phone information
- Remote switching of mobile phone camera and microphone enables unauthorized eavesdropping on conversations
- Loss of data stored in missing or stolen mobile phones
- Signal harmonics, derived from a mobile phone microphone, may be intercepted before the nearest GSM station has received the signal
- Near Field Communication and hacking in immediate proximity to mobile phones (breaking the security of NFC, built in mobile phones)
- Insecure Wi-Fi, network access and fraudulent access points enable hacking information, transferred by subscribers

SOLUTIONS FOR MOBILE PHONE INFORMATION SECURITY

There are three basic methods to secure information on mobile phones:

Software

Main disadvantages:
• weak defense against viruses and malware
• no protection against unauthorized activation of the mobile phone microphone
• no protection against dangerous radiation, induced on the mobile phone antenna from its microphone

Hardware-software method provides key storage on the SD card, installed in the mobile phone.

Main disadvantages:
• weak defense against viruses and malware
• no protection against unauthorized activation of the mobile phone microphone
• no protection against dangerous radiation, induced on the mobile phone antenna from its microphone

Hardware-software method provides crypto algorithm and key encryption on the SD card installed in the mobile phone.

Main disadvantages:
• weak defense against viruses and malware
• no protection against unauthorized activation of the mobile phone microphone
• protection against dangerous radiation, induced on the mobile phone antenna from its microphone

Hardware-software security method makes use of a hardware encoder, operating with a mobile phone via Bluetooth:

Main disadvantages:
• no protection against unauthorized activation of the mobile phone microphone

The companies, represented in the world market and working in the field of mobile phone cryptographic security, offer software or hardware encoders, which do not comply with TEMPEST standard. Thus there is the possibility to decrypt them.

STEALTHPHONE INFORMATION SECURITY SYSTEMS FOR MOBILE PHONES, TABLETS AND PCS

Mobile Trust Telecommunications (MTT) offers Stealthphone - a cryptographic encryption device, designed according to TEMPEST standard. It uses the unique technological solutions, tested by long-term practice, and military grade cryptographic algorithms, certified by state organizations of neutral countries - Sweden and the Republic of South Africa.

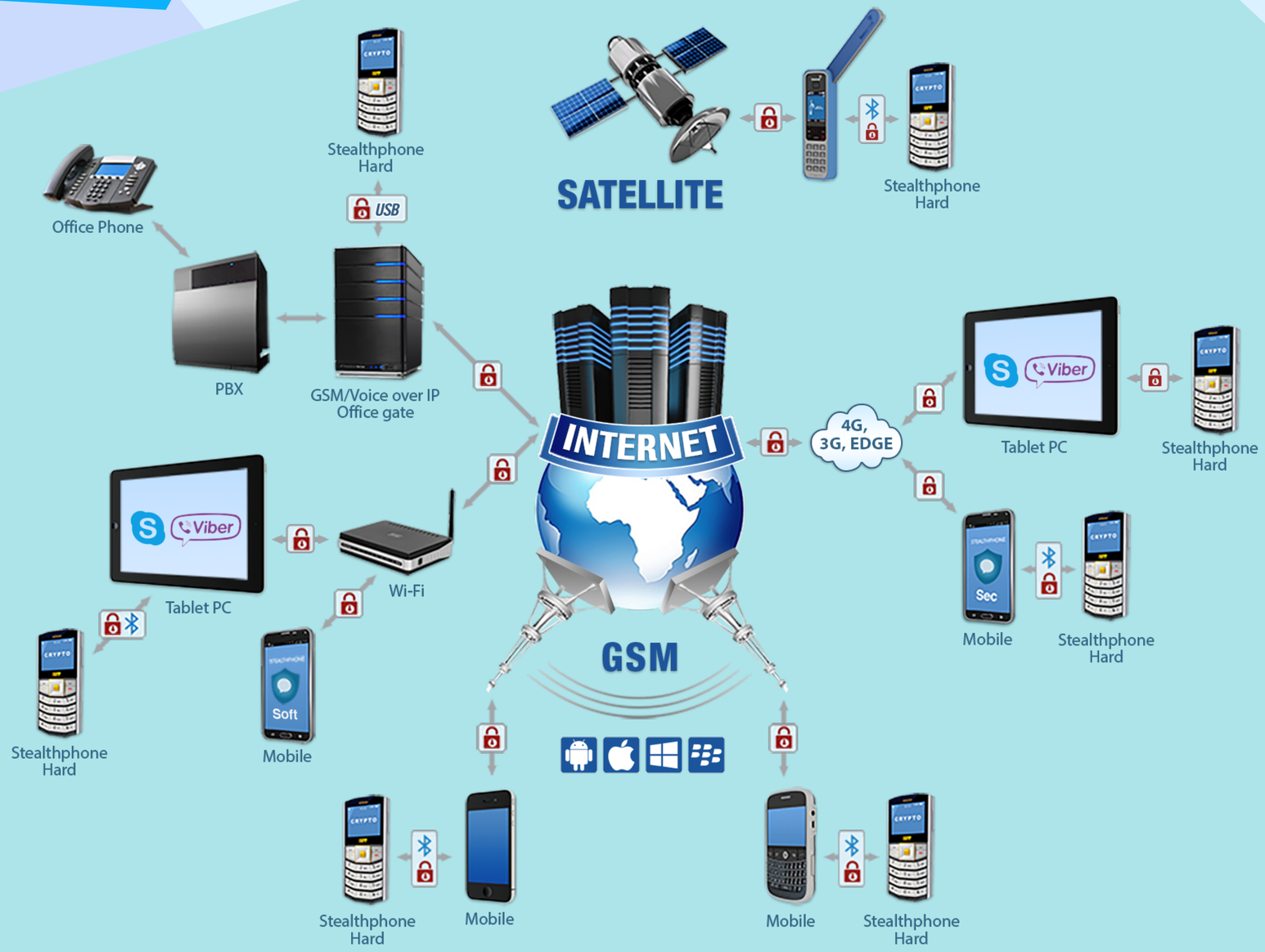
Compared with the competitive solutions Stealthphone Information security system is more improved, because:

- Voice, SMS, MMS, Email encryption does not require a variety of devices; all encryption is performed by Stealthphone encoder
- Stealthphone provides the possibility to organize secure crypto chat and crypto conference between two or more parties
- Subscribers' data are encrypted by Stealthphone encryption device. Data are transmitted in encrypted form throughout the transmission from one party to another
- Users can independently produce and distribute encryption keys using a hardware encryption key generator
- Each data type (voice, SMS, MMS, crypto chat, crypto conference and E-Mail) is encrypted using a separate encryption matrix
- Email messages can be encrypted if Stealthphone is connected to a PC via USB
- "Speechlike interference" function, implemented in the mobile phone, enables the suppression of cell phone signals and prevents voice interception
- All encoders are compatible with each other. Information can be encrypted with the hardware encryption device and decrypted by the cryptographic software

Stealthphone hardware encryption device is compatible with most modern mobile phones equipped with Bluetooth and running Android, BlackBerry, iOS, Symbian or Windows Phone operating systems.

STEALTHPHONE INFORMATION SECURITY SYSTEMS FOR MOBILE PHONES, TABLETS AND PCS

Cryptonetwork subscribers can use three communication channels to exchange encrypted data



SIP-SERVER NETWORK

SIP server by MTT company

Server network

**WE SECURE YOUR INFORMATION FROM THEFT,
AND YOUR THOUGHTS – FROM DESTRUCTION!**

Why is our product revolutionary?

- The hand-held device provides super cryptographic information security and defends data in mobile phones and PCs
- The device transmits data in Voice over GSM mode, ensuring the security of communication
- No other companies in the world have designed similar solutions

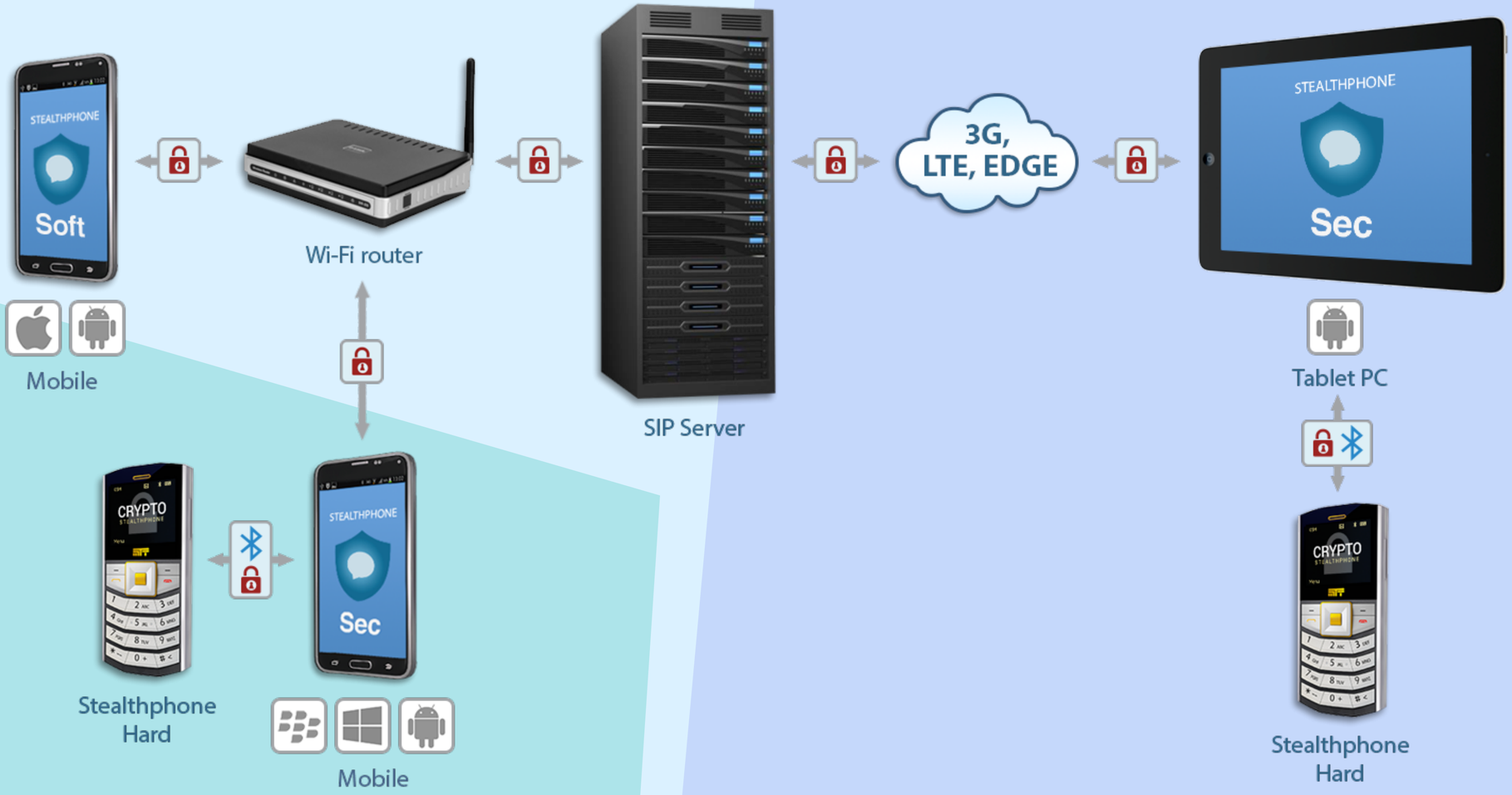
- Stealthphone is a miniature encoder, which combines the latest information security technologies:
- Provides super strong cryptographic protection of mobile phone information
- Ensures data security in accordance with TEMPEST standard
- Protects human brain from harmful mobile phone radiation
- BYOD (Bring Your Own Device) – utilizes the hardware method to distinguish users' personal and business information

VOICE ENCRYPTION
CRYPTO VOICE GSM

Stealthphone
Hard

Stealthphone
Hard

VOICE ENCRYPTION
CRYPTO VOICE IP



STORAGE OF ENCRYPTED INFORMATION ON STEALTHPHONE BUILT-IN SD-CARD

The encryption key distribution scheme in the Stealthphone information security system

- Generation of encryption keys of any specified length
- Key generation speed is up to 250 Kbit/s, which provides the possibility to generate a full key matrix with key length of 256 bits for 1,000 users in 8 minutes
- Generated keys may be stored in TouchMemory external memory without the use of a PC

ENCRYPTION IN PC

The scheme of work of the Cryptodisk hardware-software complex

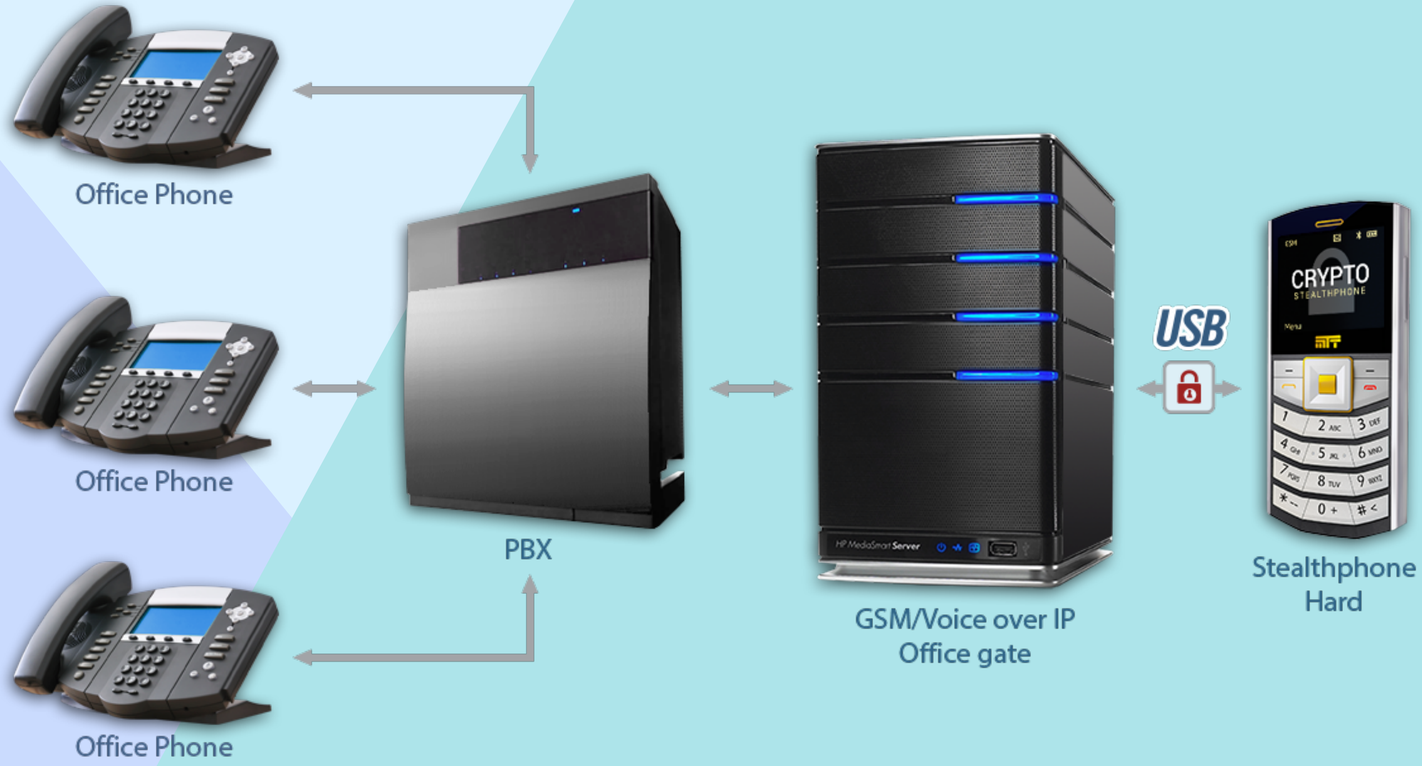
- Stealthphone Hard, plugged to a computer with a USB-cable, undertakes encryption of data.
- Possibility to create encrypted disks
- Possibility to transfer encrypted information to other users
- Quick disconnection and removal of encrypted drives in emergency situations
- Guaranteed removal of encrypted disks without a possibility to locate and restore removed data

Stealthphone CryptoFile

- The software (which is a part of software-hardware encryption complex Stealthphone Hard) allows you to send encrypted text and files via any common communication software - Skype, Facebook, Google Talk, ICQ or via e-mail

- To encrypt text and files you need to connect hardware encryption device Stealthphone Hard to your PC via USB. You also need to install Crypto File on your PC

STEALTHPHONE CRYPTO OFFICE GATE



The following operations are available with the OfficeGate system:

- Reception of encrypted incoming calls from Stealthphone network subscribers, decryption of calls and transmission to the corporate network in the unencrypted form
- Outgoing encrypted calls from any office phone in the corporate network to mobile phones of Stealthphone network subscribers
- Encrypted calls between two company offices (several OfficeGate systems are required)

BYOD FUNCTION

- Mobile telephones are used for business and personal purposes in most government and commercial organizations. According to the study, conducted by Ponemon Institute in 2012, 60% of smartphones, lost or stolen in the United States each year, contain important sensitive information

- A vast amount of confidential information, that may be easily lost or stolen, is accumulated in the memory mobile phones and tablets. That’s why BYOD (Bring Your Own Device) solution is the most urgent problem for the security of mobile phones information

- The possibility to distinguish personal and corporate information (BYOD) (Bring Your Own Device) is implemented in the Stealthphone information security system using a hardware method. It significantly reduces the risk of covert interception and disclosure of sensitive corporate information: financial, technological, official, intellectual, personal information about company managers and shareholders

The scheme of work of Stealthphone Key hardware-software complex

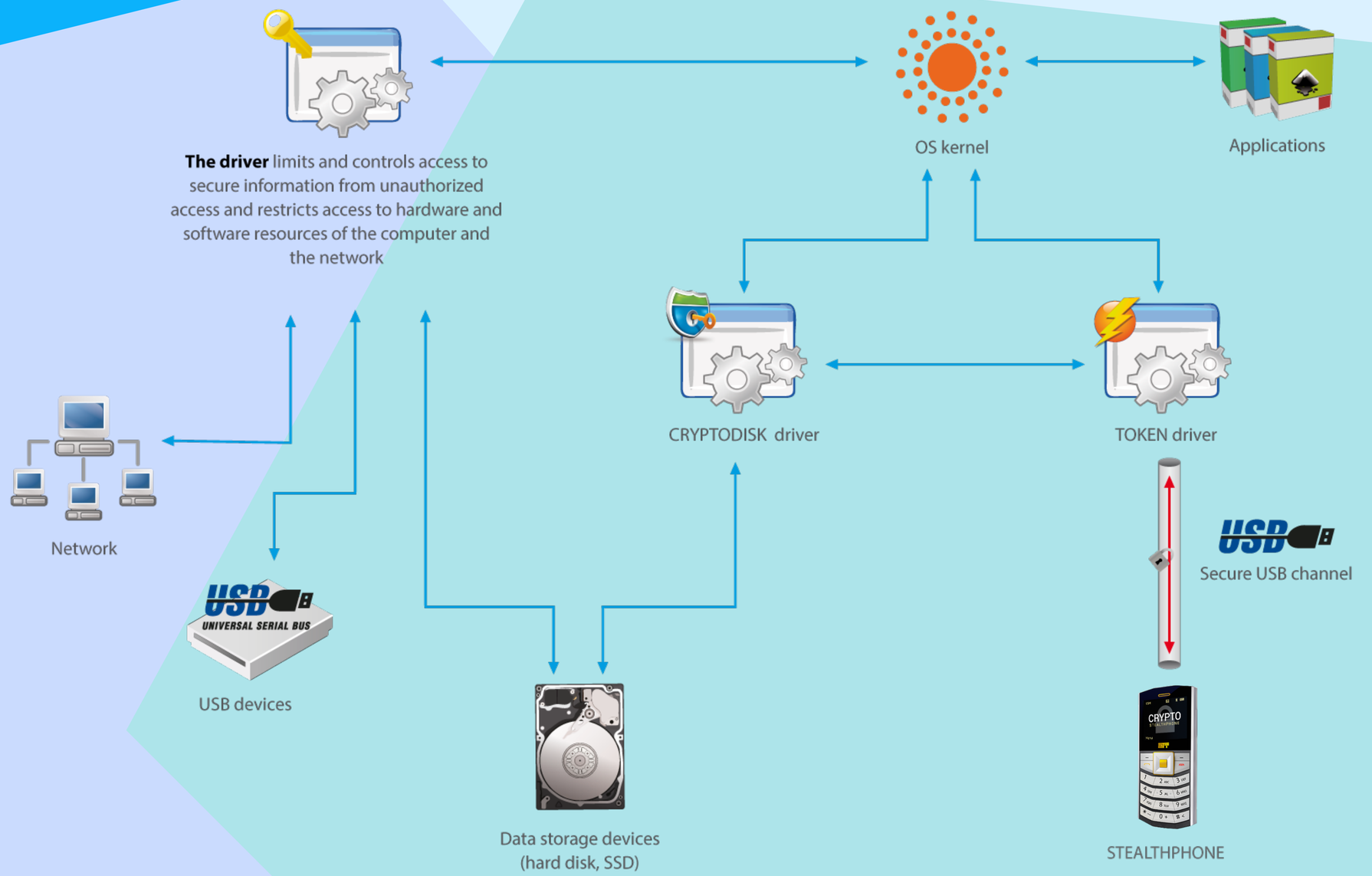
- Cryptographic algorithm is required to encrypt and decrypt messages. A cryptoalgorithm is like a safe, and ecnryption key is used to open it

- To achieve the highest degree of encryption strength, you need to use the hardware random number generator stealthphone key hard together with stealthphone key software

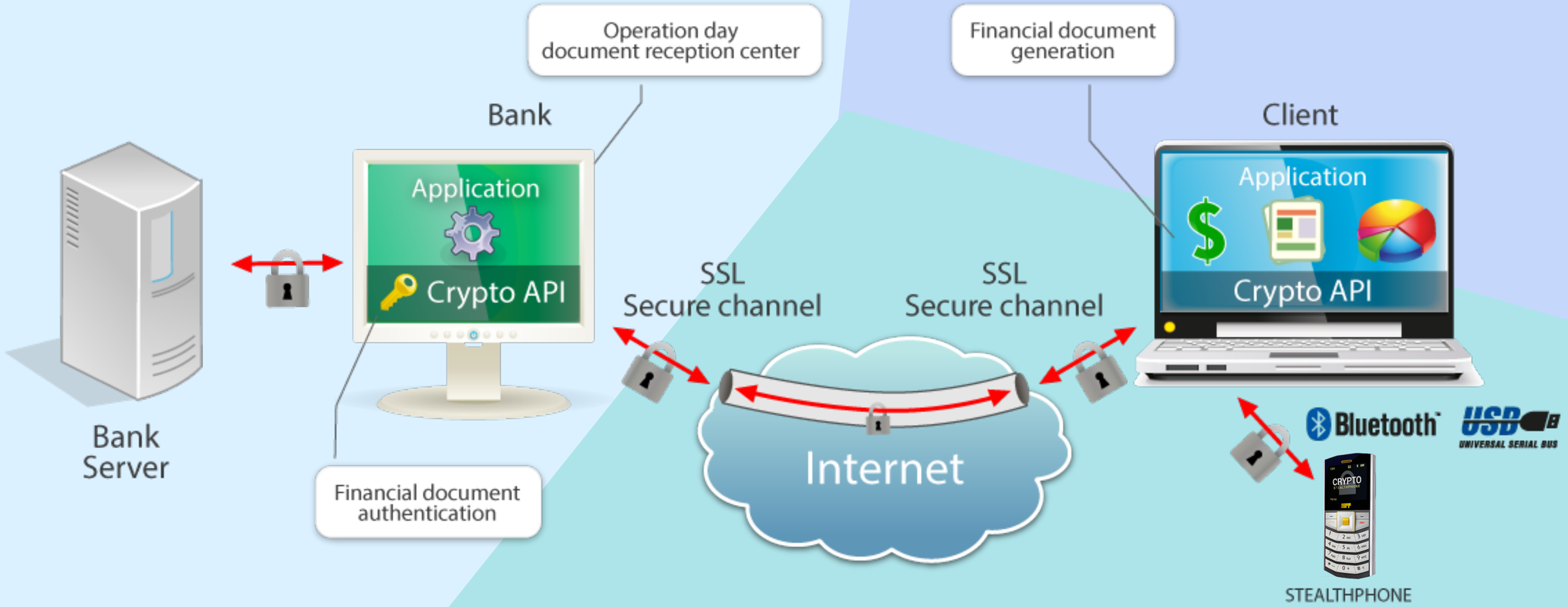
- Users require encryption keys in order to exchange data or to make calls. Eeach pair of users has the unique set of these keys. The stealthphone crypto network consists of the subscriber pairs

STEALTHPHONE TOKEN – ETOKEN FUNCTION

Stealthphone encryption device can be used as a USB key for secure storage of personal information and reliable security from unauthorized access. It enables to encrypt data, voice, video and e-mail messages transferred from computers and mobile phones as well as to sign documents with an electronic digital signature to prevent their modification.



INTERNET BANKING WITH STEALTHPHONE



THE USE WITH PORTABLE RADIO TRANSMITTERS

THE USE WITH SATELLITE PHONES

STEALTHPHONE
INFORMATION SECURITY SYSTEM

MOBILE TRUST
TELECOMMUNICATIONS

Our address:

Mobile Trust Telecommunications AG

Usterristrasse 11
8001 Zurich
Switzerland
Tel: + 41 44 21 03 743

E-mail: info@mttgroup.ch
URL: http://www.mttgroup.ch