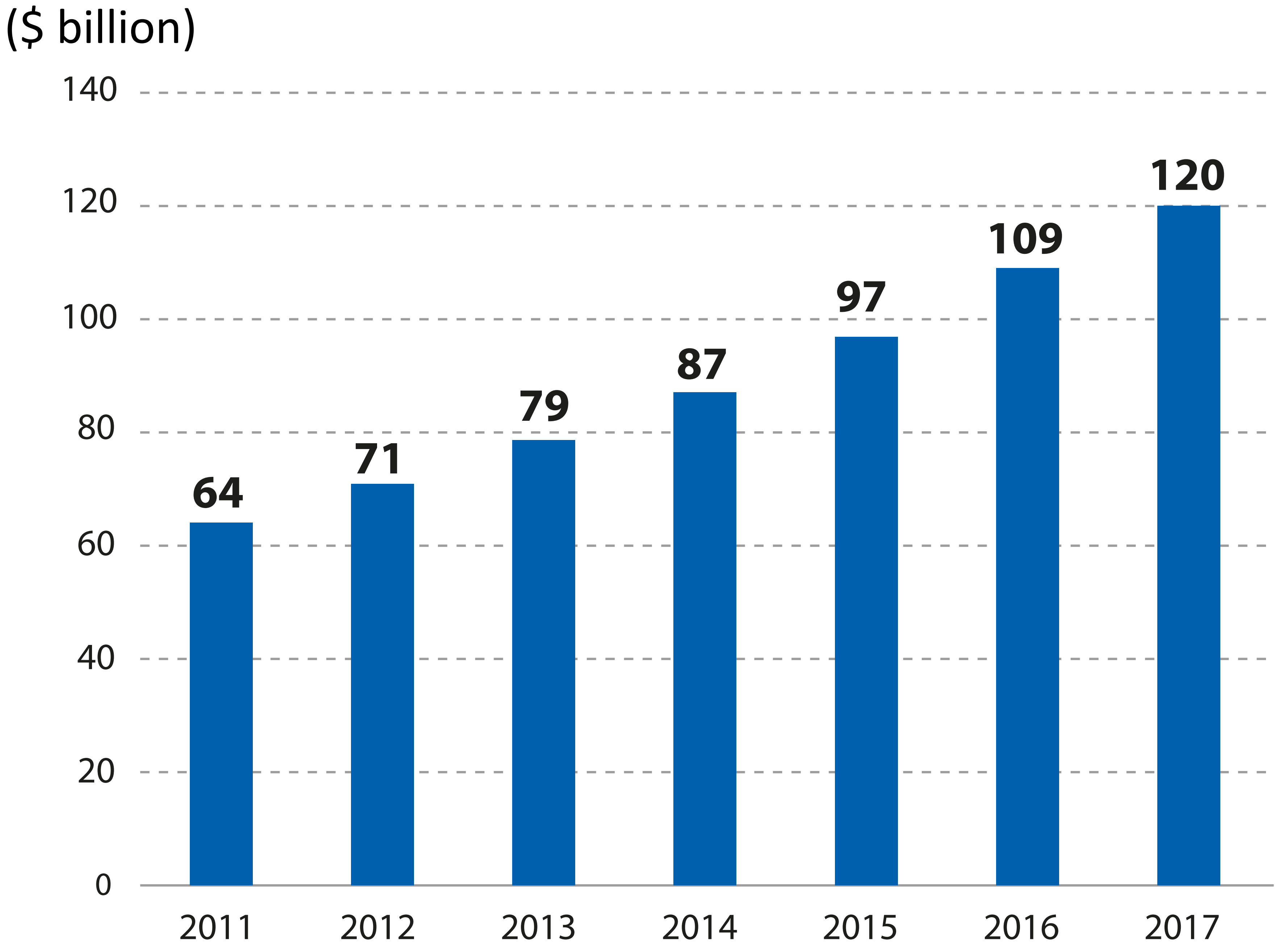
Hardware Encryption System for E-Commerce and Mobile Banking Security

MOBILE TRUST

TELECOMMUNICATIONS

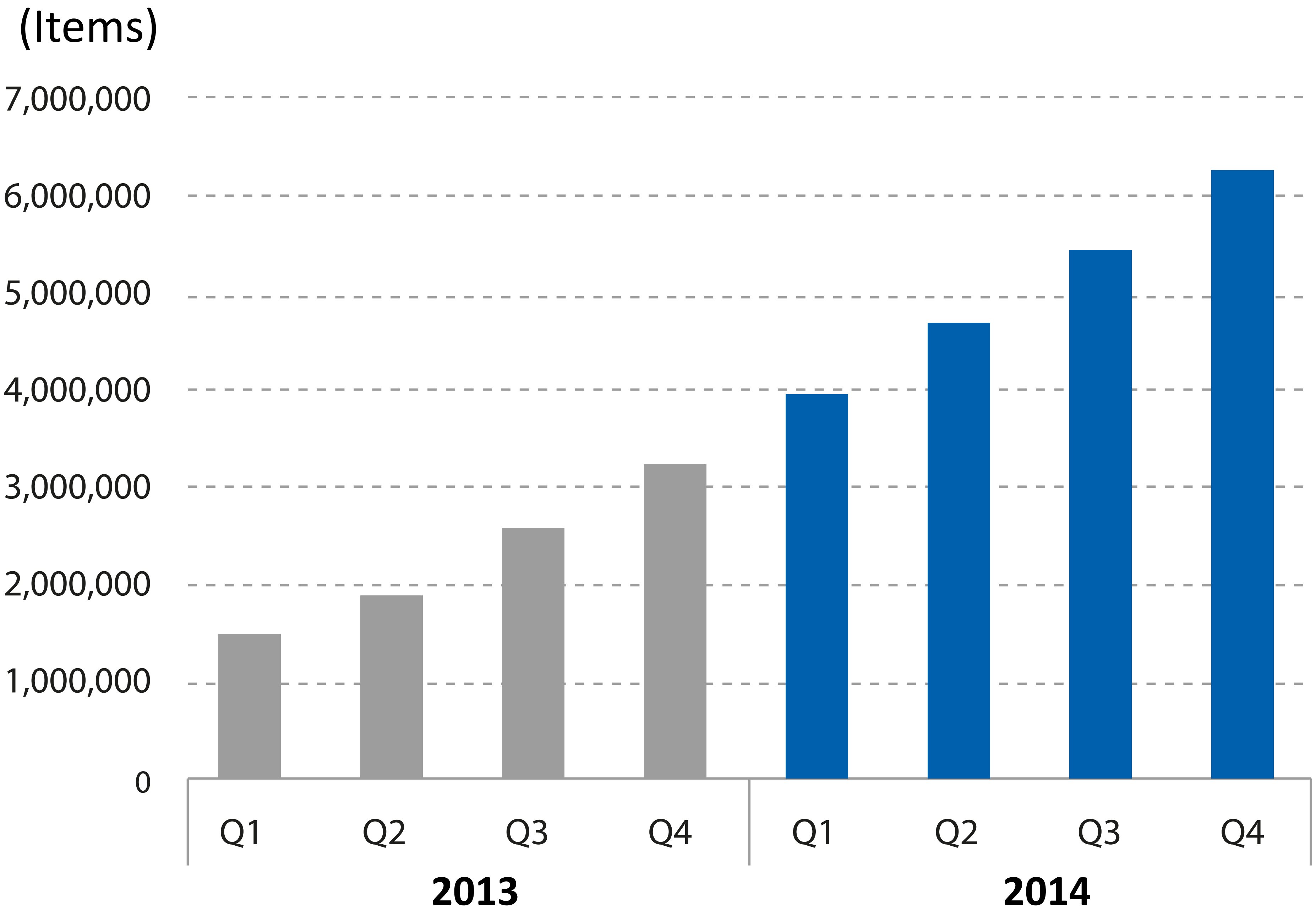
www.mttgroup.ch

INFORMATION SECURITY EXPENSES INCREASE



Source: MarketsandMarkets

INCREASE OF MALWARE APP COUNT TARGETING MOBILE PHONES



Source: AcAfee Kabs

CISCO stated in 2013 report the snowball-like growth of mobile traffic with a few years:
By 2017 the smartphone and tablet traffic will exceed that of desktop PCs three times as some 6 billion mobile phones have already been produced. The rapid growth and development of various mobile platforms and services stimulate mobile banking as well. The current and future trend assessment demonstrates the mobile banking users growth by 30-40%/year.

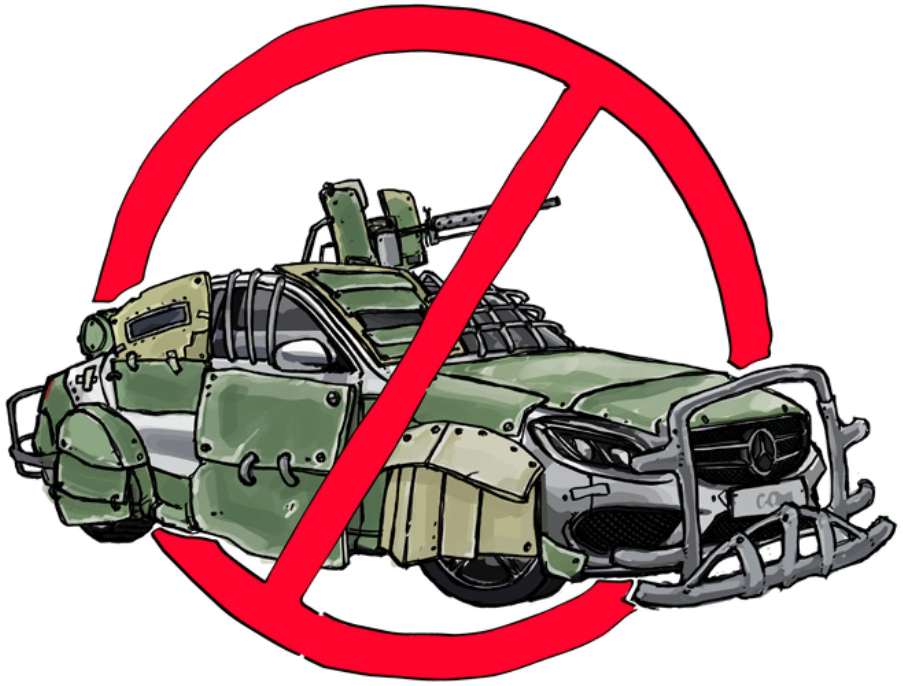
As the mobile banking gains its popularity it also increases the number of related threats.
In 2015 we have a track of over 2 billion hackers' attacks on mobile phones and computers. Hackers generate over $400 billion of profit exceeding the revenue of drug and illicit arms dealers altogether. UK Parliament has confirmed the fact.

The largest share of hackers' income comes from e-commerce and mobile banking thefts - the most dynamic field.

This leads to significant increase of e-commerce and mobile banking system security. Markets and Markets research indicates that mobile phone security expense share of total information security will be increasing every year. The company forecasts by 2018 companies will spend $94 billion/year on mobile phone information security.

MAIN CHALLENGES OF MOBILE BANKING

1. Hackers’ technical resources and capabilities rapidly improve
2. Data leak from companies monitoring mobile phones, PCs, and Internet services for government organizations
3. Phishing
4. Banks attempt to save on information security system



The following factors affect information security:

1. Hackers’ technical resources rapidly improve. Advanced graphic stations (featuring powerful CPU and GPU) enable hackers to bruteforce 56 billion password a second. Three years back only special service of some countries had such computer power at hand.

2. The most important factor is data leak from companies officially monitoring mobile phones, PCs, and Internet services for government organizations. Italian Hacking Team may be a good example. It looks like hackers get hold of the developments making their capabilities similar to those of special services.

3. In most bases the data leaks on bank activities are caused by hacking the bank employees’ corporate e-mails. And the most used e-mail hacking tool is phishing.
   According to the security experts at Trend Micro firm, spear phishing is the attack method used in some 91 percent of cyber-attacks. And the goal is to gain personal and other confidential data that may be used to further attack the bank and its customers.

4. Users do not realize the danger hackers pose and try to purchase the most inexpensive security systems. They fail to understand that this also means lower strength of security. This approach makes the banks implement cheap security systems, i.e. software solutions in most cases. However, the most significant threat to security technology is that the technology is applied to the smartphones that were not designed for that very purpose. The attempt to make a reliable information security system from an average device is absolutely similar to trying to turn your city car into a tank. Moreover, you decrease security level with every app you install on your smartphone.

LACK OF STRONG AND RELIABLE SECURITY FOR MOBILE BANKING RESULTS IN

1. Limiting financial transactions.
2. Complicating mobile payment procedures.
3. Increasing financial load on all e-commerce participants.

Therefore, we arrive at a distressing CONCLUSION: Software security apps for mobile phones cannot ensure efficient development of mobile commerce. Although, 99% of all mobile phone information security systems are software-only. There is no way you may create a strong and reliable information security solution just using a mobile phone.

Therefore, we arrive at a distressing CONCLUSION: Software security apps for mobile phones cannot ensure efficient development of mobile commerce.
Although, 99% of all mobile phone information security systems are software-only.
There is no way you may create a strong and reliable information security solution just using a mobile phone.

WORLD ONLY COMPANIES ABLE TO PRODUCE REALLY STRONG HARDWARE AND SOFTWARE ENCRYPTION SECURITY SYSTEMS FOR MOBILE BANKING, COMPLIANT WITH TEMPEST STANDARD

1. Boeing (USA)
2. Raytheon (USA)
3. Ancort (Russia)

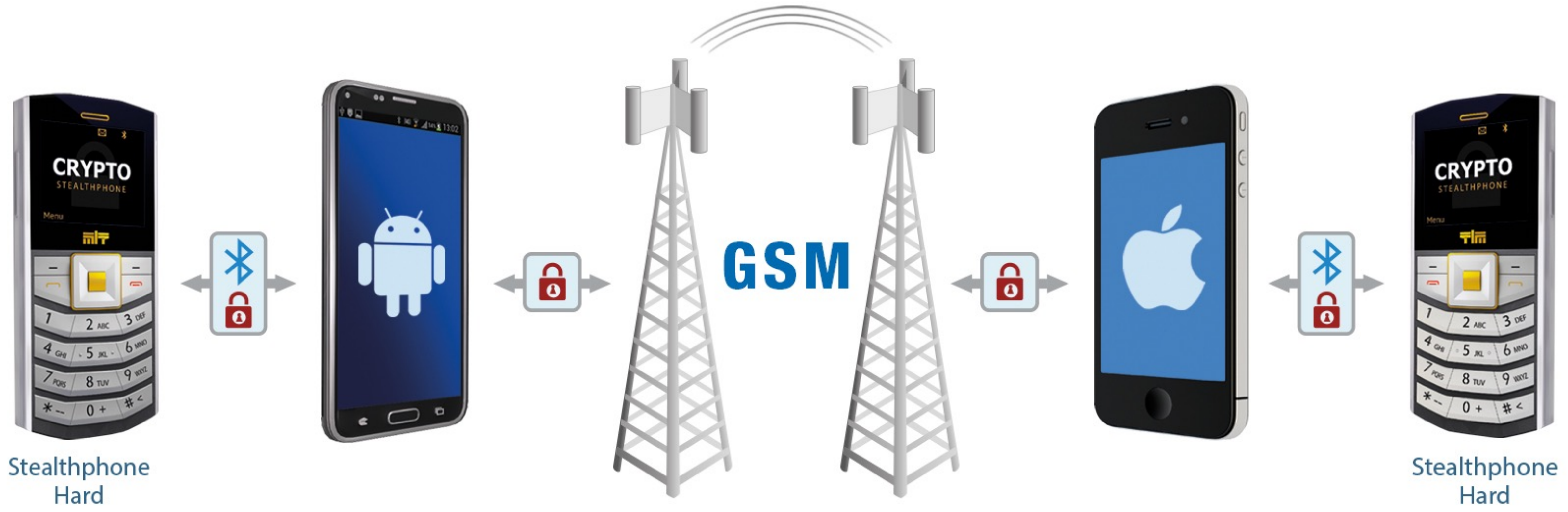
MAIN STEALTHPHONE HARD ADVANTAGES

- Super strong voice and data hardware encryption
- Secured against viruses
- TEMPEST-compliant
- Military grade encryption algorithms
- Developed based on engineering cryptography methods
- Proprietary low-level (C++) OS with engineering cryptographic security
- Works with mobile phones (over Bluetooth) and PCs (USB)

STEALTHPHONE INFORMATION SECURITY SYSTEM

Crypto Voice Over GSM

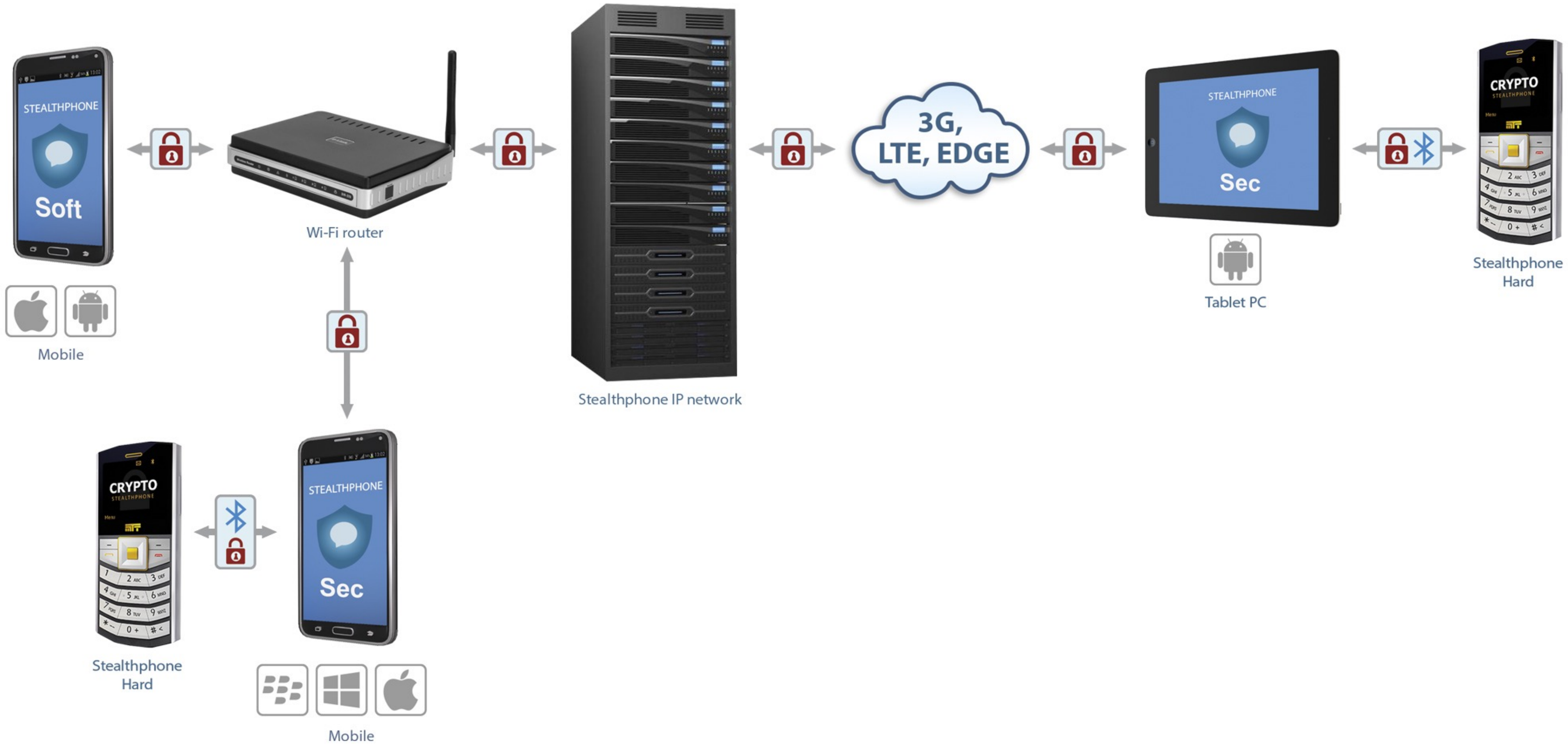
Stealthphone Hard connects to mobile phone to secure phone calls over GSM network.



STEALTHPHONE INFORMATION SECURITY SYSTEM

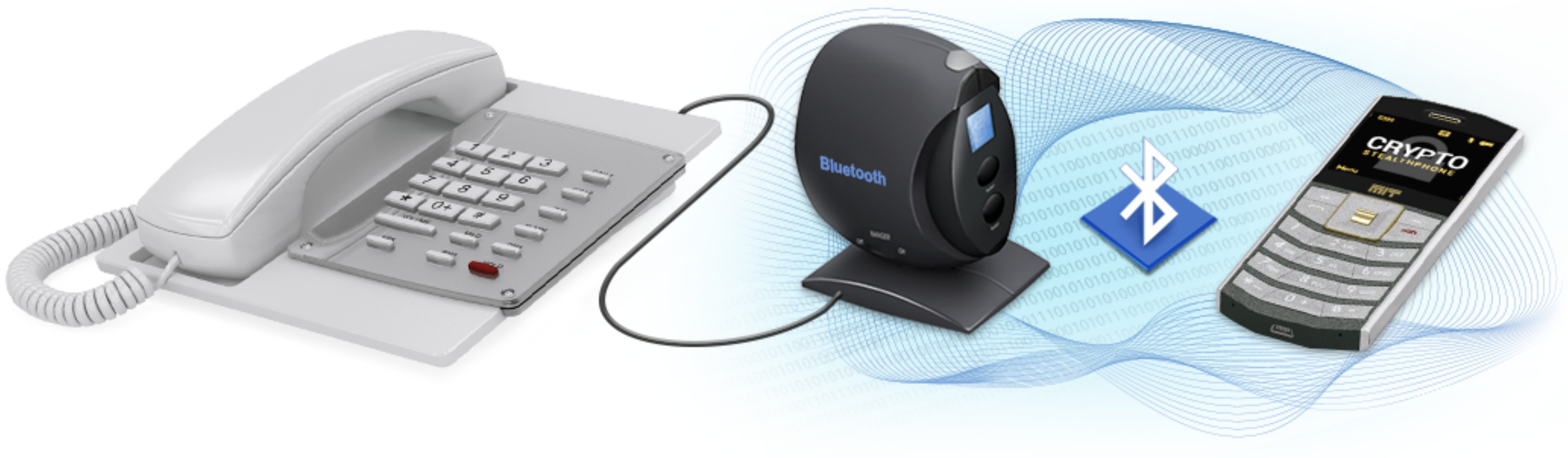
Crypto Voice Over IP

Voice encryption over IP channels, including popular messengers (Skype, Viber).



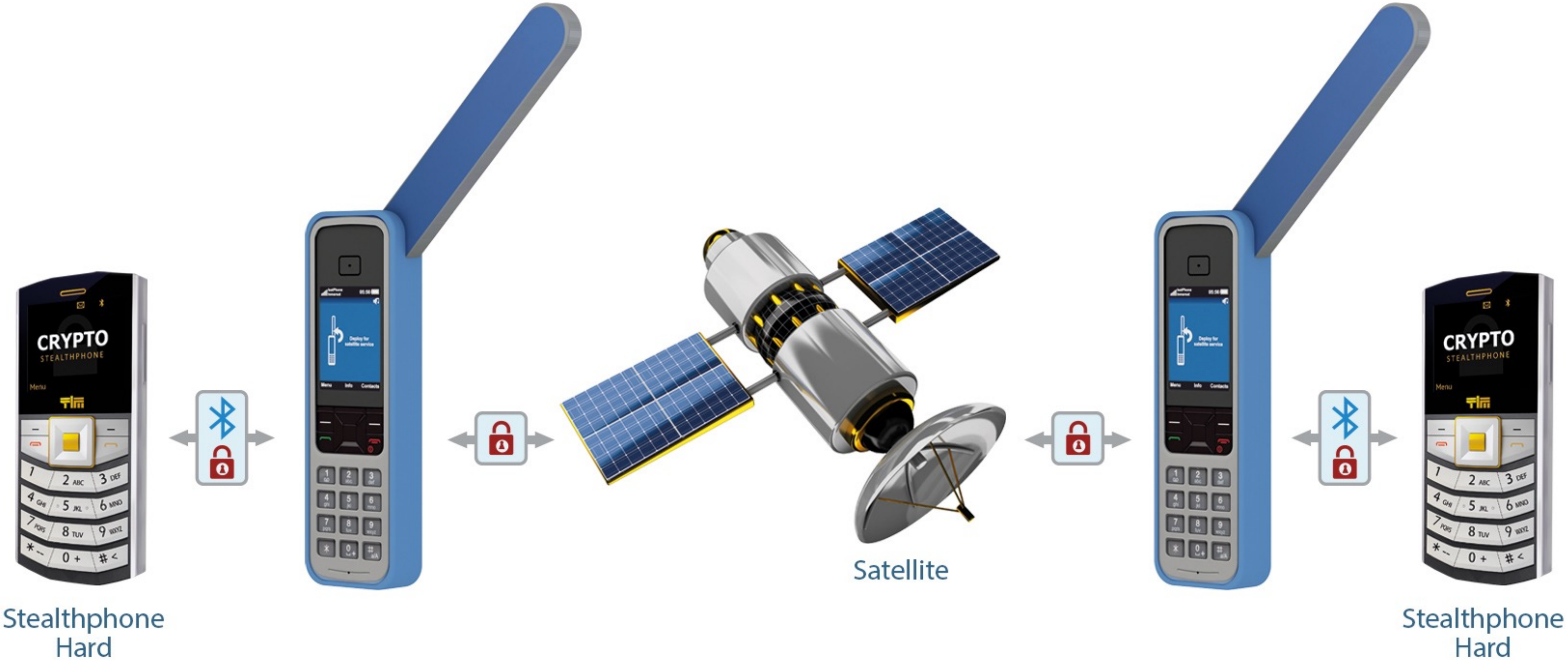
STEALTHPHONE INFORMATION SECURITY SYSTEM

Landlines



STEALTHPHONE INFORMATION SECURITY SYSTEM

Satellite



STEALTHPHONE INFORMATION SECURITY SYSTEM

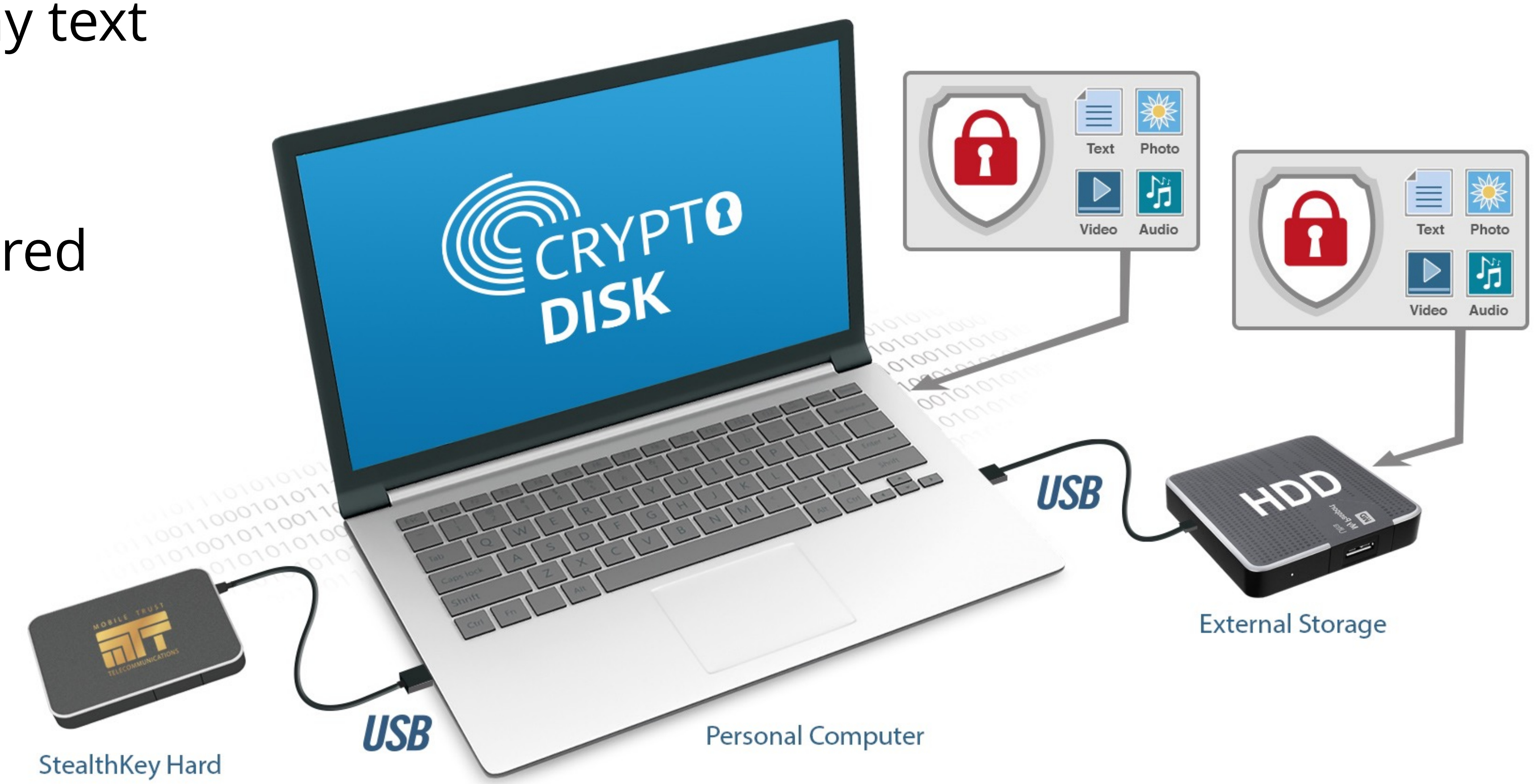
Transferred data encryption:

- SMS
- Instant messages
- Files
- Emails

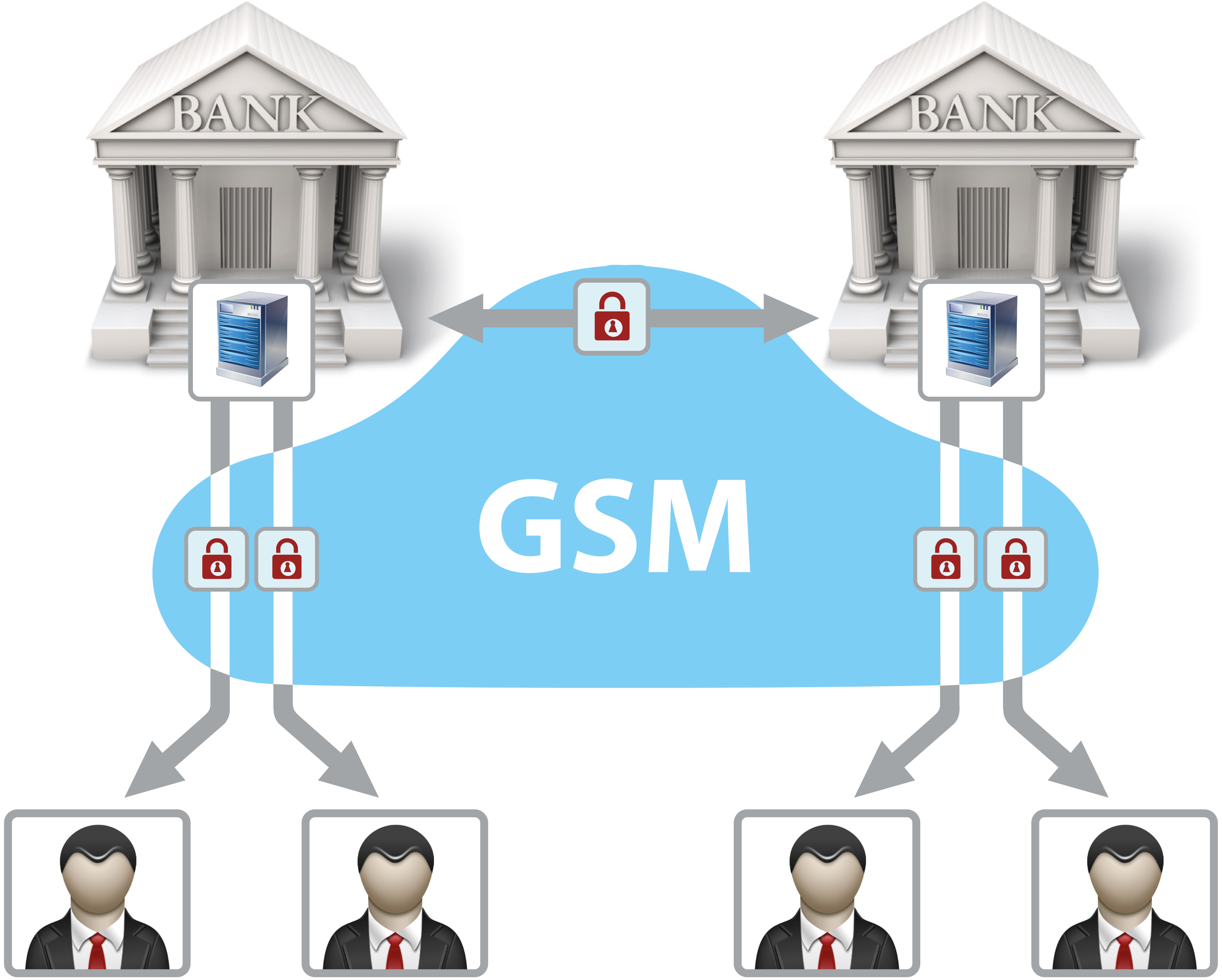
STEALTHPHONE INFORMATION SECURITY SYSTEM

Transfered data encryption on digital media:

- Encryption of any text and data files
- Creation of secured virtual disks



OfficeGate

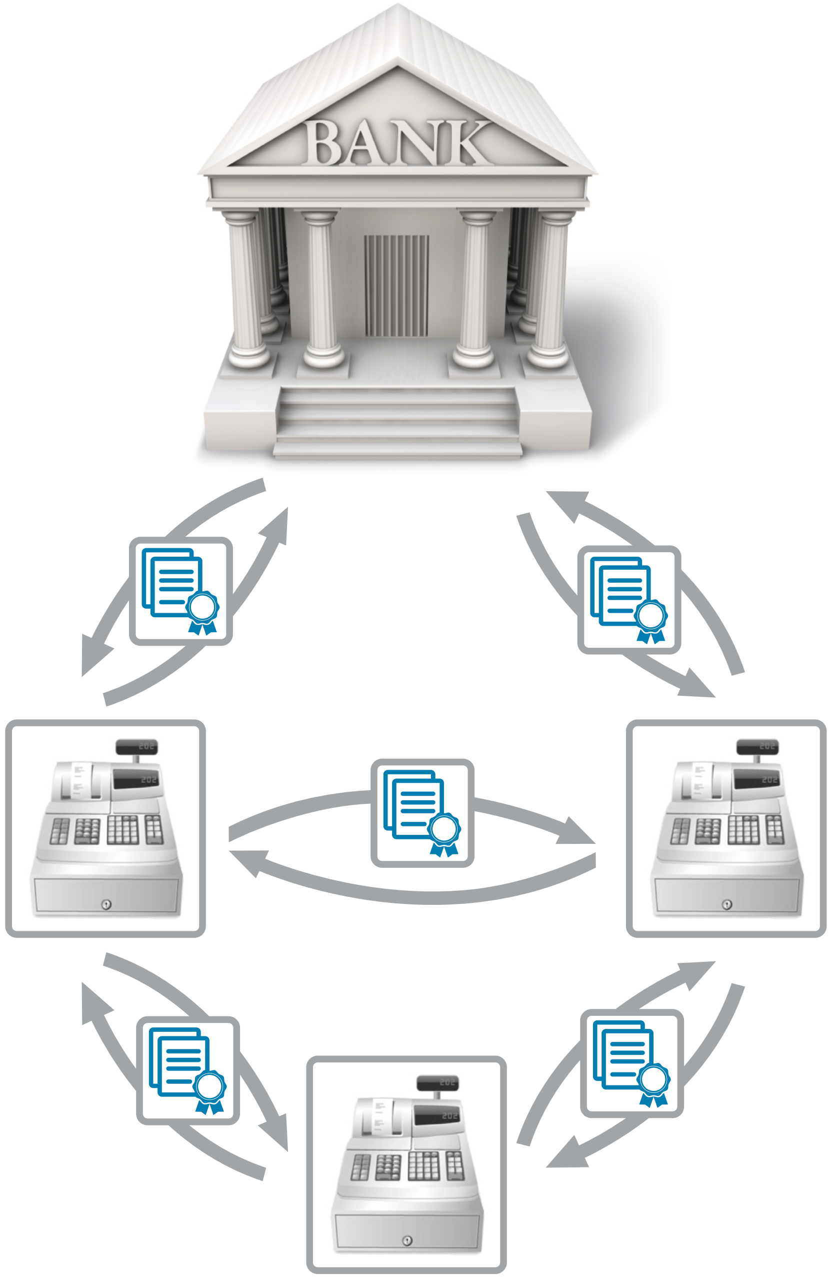


OfficeGate hardware and software set is one of the voice encryption systems that connects to the office phone switchboard. Voice encryption, including Voice Over GSM via OfficeGate may be used to secure customers’ calls to bank office, i.e. as a powerful tool of additional authentication factor (combined with key work or one-time password). Moreover, the system secures against wiretapping.

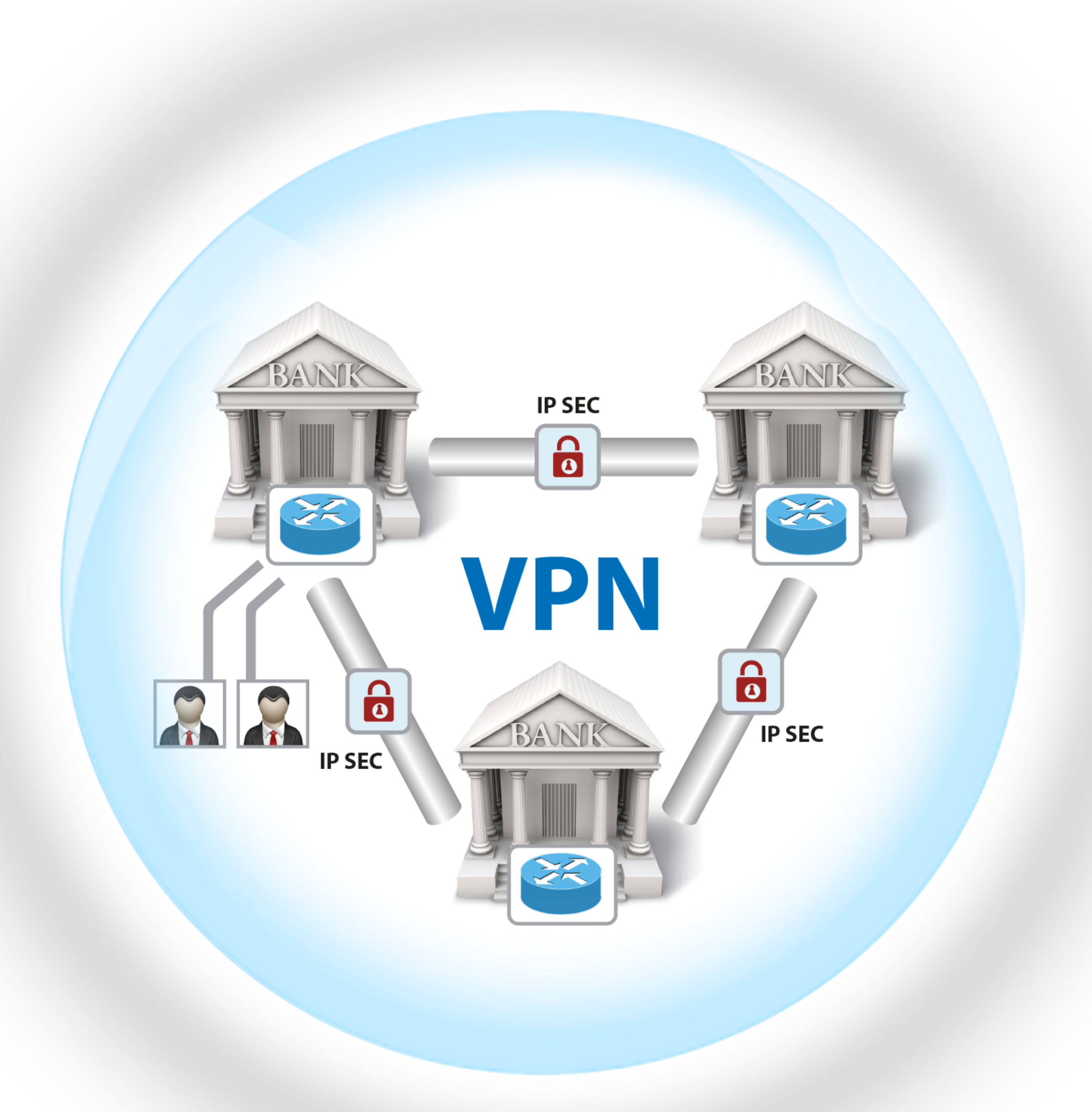
Stelathphone Hard can be used in mobile banking to generate digital signature (DS).

In 1992 it took Ancort Company three months to resolve the fake aviso problem by developing mini-DS system for financial documents.

- Equipped some 2,000 cash processing centers of Central Bank with hardware encryption devices
- Developed and deployed key management system
- Generated and distributed encryption keys between cash management centers
- Trained some 6,000 operators
- Took part in development of vast volume of procedure documents for Central Bank that specified the system activity and interaction with other Central Bank systems



CRYPTOROUTER-BASED VPN



Nowadays Ancort Company offers a range of unique multi-feature MTT-GW encryption routers that enable to connect all bank branches, including ATMs, into one virtual private network (VPN). All bank services and procedures (client-server systems, mail, conference, data exchange, phone calls) will run secured.

Every employee may joint the office virtual office even on the go using VPN client in Stealthphone Hard hardware encryption device.

Stealthphone informations security system - Stealthphone Hard hardware encryptor and range of hardware crypto routers - can be seamlessly integrated into internal bank systems therefore drastically increasing level of security.
IP component of Stealthphone system may be used within or outside the VPN. VPN enables to create external security circuit.

Using Stealthphone system to secure BOTH internal bank communications and communications with customers significantly increases reliability, manageability, and efficiency of the system.

Stealthphone system key advantage is support of non-IP voice channels (GSM, Satellite, Landlines) and SMS service. All the features are implemented in hardware. The abovementioned features enable to increase the overall security of the system and may be used to ensure the integrity and continuity of bank business processes.

MOBILE TRUST

TELECOMMUNICATIONS

Mobile Trust
Telecommunications AG

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