MOBILE TRUST
TELECOMMUNICATIONS

Feature comparison between Stealthphone Hard of Mobile Trust Telecommunications AG and TopSec Mobile of Rohde & Schwarz

TopSec Mobile	Stealthphone
Standard Bluetooth - version 2.0; supports operation with one mobile phone: it does not support the connection to a computer.	Standard Bluetooth - version 2.1 EDR; supports up to 5 connected mobile phones; supports the connection to a computer via USB.
Standby time is up to 100 hours	Standby time is up to 150 hours
Operation in voice encryption mode is up to 4 hours	Operation in voice encryption mode is 8 hours
The minimum data transfer speed required for operation is 9.6 Kbit / s	The minimum data transfer speed required for operation is 9.6 Kbit / s
Transfer protocol - V.32, V.110, TCP/IP	Transfer protocol – TCP/IP
None	A phone format keypad; the possibility to assign 10 speed dial numbers.
Liquid Crystal Display	Liquid Crystal Display
The device is charged using a USB cable; a charger supplied with the device.	The device is charged using a USB cable; a charger supplied with the device.
Supported data transfer channels: 3G, EDGE, Wi-Fi	Supported data transfer channels: LTE, 3G, HSDPA,EDGE, Wi-Fi, WiMax.
Geolocation of servers: unknown	Geolocation of servers: Russia, USA, Germany, Singapore

None	Voice over GSM support
None	Passwords, and card PIN-codes can be stored in the device
None	Storage of a phonebook and a call log
Supported OS: iOS, Android	Supported OS: iOS, Android, BlackBerry, Windows Phone
Dimensions - 99 mm x 34 mm x 22 mm	Dimensions - 118 mm x 51 mm x 12,5 mm
Weight - 58 grams	Weight – 80 grams
Cryptographic characteristics	
User authentication: false encrypted communication is impossible; effectively prevents hacker attacks; creates closed user groups	User authentication: false encrypted communication is impossible; effectively prevents hacker attacks; creates closed user groups
Symmetric encryption algorithm with a 256 bit encryption key	Symmetric encryption algorithm (developed by MTT) with a 256 bit encryption key
Voice encryption	Encryption of voice, SMS, MMS, E-Mail, “crypto chat” and “crypto conference” modes (secure chat for two or more users)
No SD-card	A 32GB SD-card is used for storage of encrypted information. The recording speed in the encryption mode is at least 200 MByte/sec; it can be used in an encryption mode with a password and in the normal mode without a password and access to previously encrypted data.
None	A mobile phone microphone is secured against unauthorized activation
None	Own mail server
None	Access codes can be dialed from an encryption device keypad

None	Unauthorized access is prevented by means of a password system used to start the device itself, Bluetooth and a crypto SD-card.
User authentication in the phone call encryption mode.	User authentication in the phone call encryption mode.
Voice encryption prevents Man-in-the-middle (MITM) attacks	Voice encryption prevents Man-in-the-middle (MITM) attacks
None	Secure IPSec protocol is used in a tunnel mode to provide the connection with a specialized SIP-server.
None	Key destruction and locking cryptographic services in case the device is lost or stolen.
None	The «Stealthphone Software» emulator for mobile phones provides the security of subscribers' confidential information.
None	The device is connected to a computer via a USB port. Encryption of E-mail sent between computers, between computers and mobile phones.
None	Prevents unauthorized switching of mobile phone microphones.
Key system	
Asymmetric encryption algorithm, based on elliptic curves, with a 384 bit key length.	Asymmetric encryption algorithm, based on elliptic curves, with a 256 bit key length.
Symmetric voice encryption algorithm with a 256 bit key length.	Symmetric voice encryption algorithm with a 256 bit key length
Session key computation is used to encrypt voice using the combination of the Diffie-Hellman method	Session key computation is used to encrypt voice using the combination of the Diffie-Hellman method and a secret long-term pairing key.
One-time session keys. (They are generated at the beginning of the session and are guaranteed to be deleted at the end of the session.)	One-time session keys. (They are generated at the beginning of the session and are guaranteed to be deleted at the end of the session.)

None	A one-time random session key is generated to encrypt data: SMS, MMS, E-Mail, using a full key matrix of up to 10000 users. A key matrix is generated by a software package using a physical random number generator and software audit of the statistic values.
None	10 security levels. Each level has its own key. The highest level can call the lower levels.