TopSec Mobile

Secure voice encryption for smartphones and laptops

ROHDE&SCHWARZ

Secure Communications

Product Brochure | 02.00

TopSec Mobile
At a glance

The TopSec Mobile is a mobile encryption device for secure worldwide VoIP-based communications on smartphones and laptops.

The TopSec Mobile securely encrypts voice communications end-to-end on IP-based communications networks and on BGAN and Thuraya satellite links. Users access these communications networks with the TopSec Mobile connected to smartphones and laptops via Bluetooth®.

The TopSec Mobile is easy and intuitive to operate using apps that are available for the most widely used operating systems. Because the TopSec Mobile is a smartphone-independent encryption device, it cannot be manipulated by malware.

Key facts

- Encryption device offering maximum security
- For flexible connection to smartphones and laptops via Bluetooth®
- Intuitive operation thanks to easy-to-use apps
- Universal VoIP encryption via mobile radio, Internet and satellite connections

TopSec Mobile
Benefits and key features

Versatile
- Bluetooth® interface for connection to smartphones and laptops
- USB cable connection to laptops
- TopSec Phone app for smartphones and laptops
- Connection to IP networks via smartphones, laptops or satellite terminals
- Call setup over public or private VoIP servers

▷ page 4

TopSec encryption concept
- Method for maximum security
- Key agreement with elliptical curves, 384 bit
- Certificate-based authentication
- Voice encryption using the Advanced Encryption Standard (AES) 256-bit key

▷ page 6

Available models and software
- TopSec Mobile encryption device
- TopSec Phone app for iPhone
- TopSec Phone app for Android smartphones
- R&S®VoIP-SERVER S110

Telephone as usual: For a secure call, simply hold the TopSec Mobile to your ear.

Versatile

Bluetooth® interface for connection to smartphones and laptops

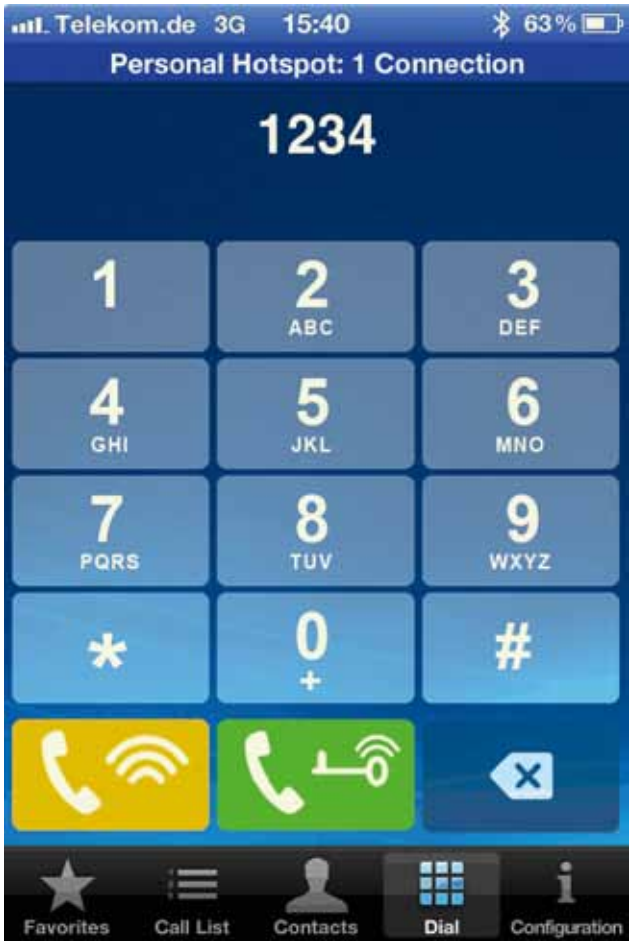
The TopSec Mobile is a highly versatile voice encryption device in terms of its ability to connect to communications terminal equipment and networks. With its Bluetooth® interface, it provides a dependable wireless connection to communications terminal equipment such as smartphones and laptops.

Users can make confidential calls either directly with the TopSec Mobile or with a headset (included); the calls are encrypted and decrypted in the TopSec Mobile. The voice data sent from and to the TopSec Mobile is already secured to the highest possible level while it is transmitted via the Bluetooth® interface.

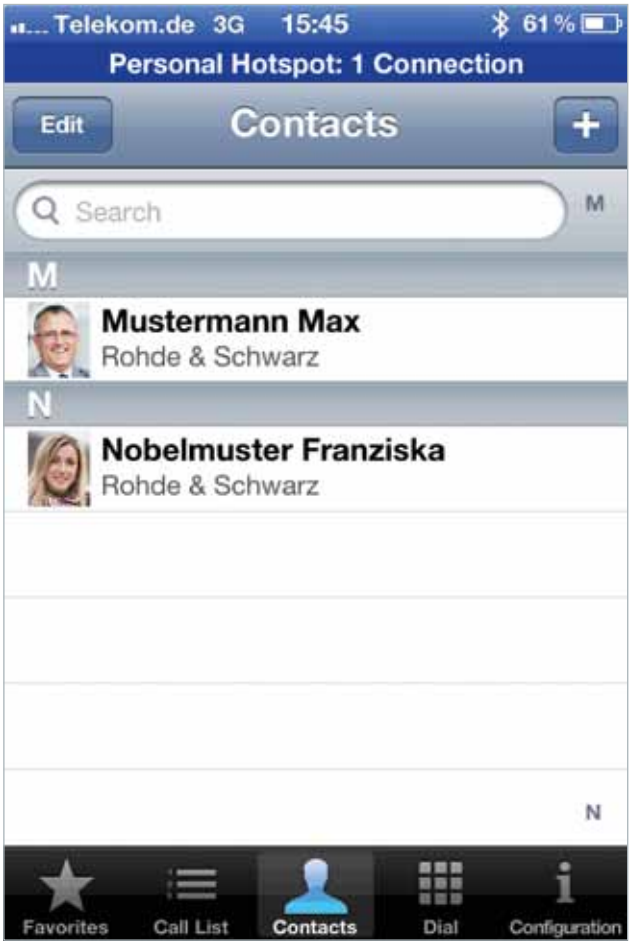
USB cable connection to laptops

As an alternative to the wireless Bluetooth® interface, the TopSec Mobile can be connected to a laptop via a USB cable. This enables users to set up an encrypted connection to an IP network in surroundings where a wireless connection is undesirable.

The dialer interface for Internet telephony: The green call button sets up an encrypted call with the TopSec Mobile; the yellow call button is for unencrypted VoIP calls.



The TopSec Phone contact list.



TopSec Phone app for smartphones and laptops

The TopSec Mobile can be used with advanced smartphones and laptops. Users choose the numbers of the persons they want to call from a contact list on their smartphone or laptop. They do this with the TopSec Phone app. TopSec Phone can be used to make unencrypted VoIP calls directly with the smartphone as well as encrypted VoIP calls over the TopSec Mobile.

Users accept encrypted VoIP calls directly on the TopSec Mobile. The encryption and decryption is carried out in the TopSec Mobile itself, without involving the smartphone or laptop. When making secure calls, users talk and listen through the TopSec Mobile's own microphone and speaker. This prevents possible manipulation by malware.

TopSec Phone also supports unencrypted VoIP. Users can access the full feature set available on their smartphone or laptop, and can simply choose secure calls when they wish.

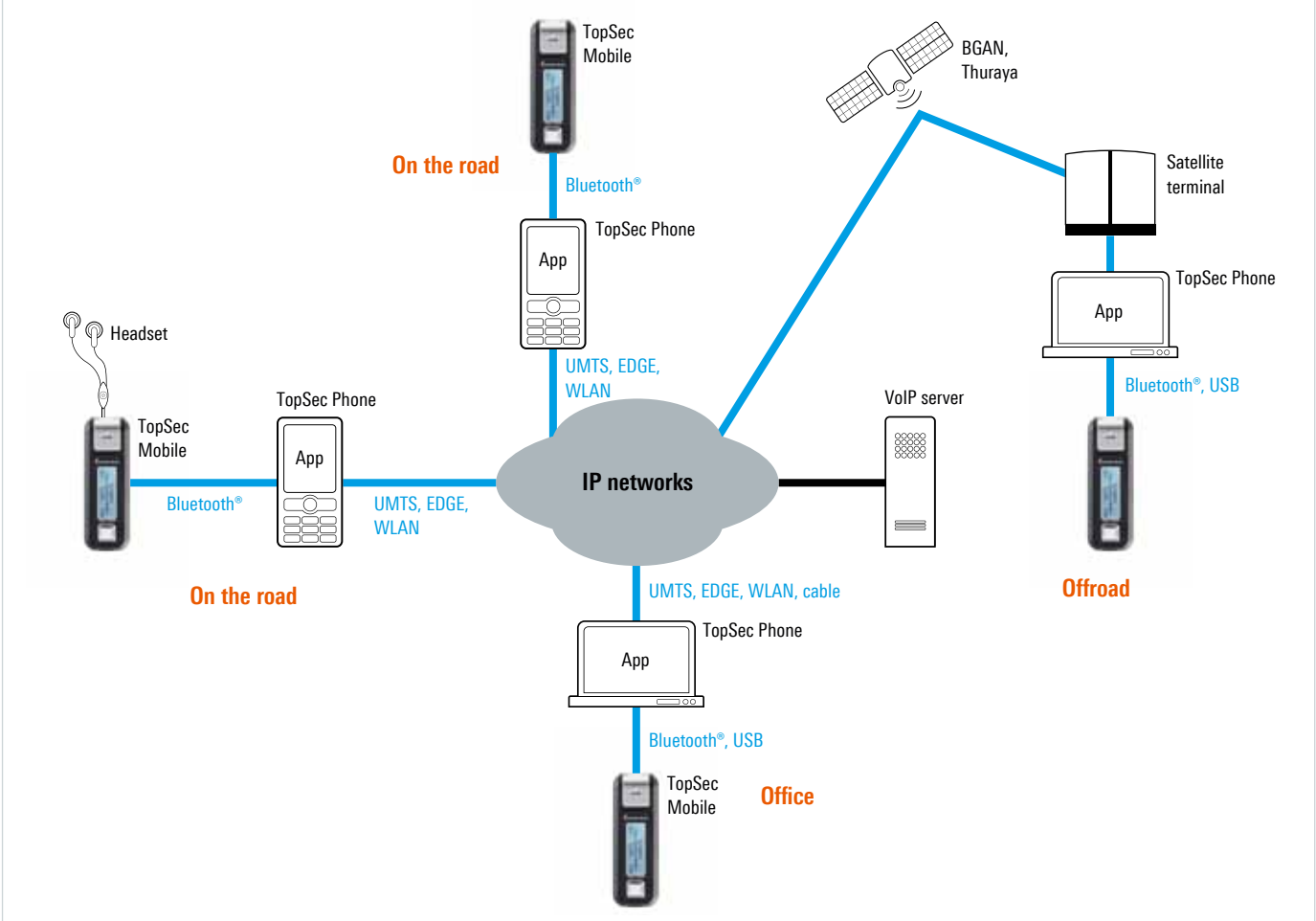
Connection to IP networks via smartphones, laptops or satellite terminals

Users connect to IP networks via the communications terminal equipment. Smartphones provide wireless access to UMTS networks and WLANs. Laptops generally have a LAN port in addition to enable a wireline connection to IP networks. With the TopSec Mobile, users are also able to encrypt communications via BGAN and Thuraya IP satellite terminals.

Call setup over public or private VoIP servers

To place and receive VoIP calls, users must be registered on VoIP servers. The TopSec Mobile can set up encrypted connections using two common signaling protocols, SIP and IAX2. It works both with public SIP servers and with the R&S®VoIP-SERVER S110. The R&S®VoIP-SERVER S110 is especially suited to user groups with special security requirements who prefer to operate their own VoIP server.

Voice encryption with the TopSec Mobile



TopSec encryption concept

Method for maximum security

Encryption in the TopSec Mobile is based on a hybrid process to achieve the highest level of security. This method requires that the partner encryption devices have the same mathematical parameters and that they use identical algorithms.

Key agreement with elliptic curves, 384 bit

The Diffie-Hellman key agreement protocol enables encrypted communications between two partner encryption devices without the need for central administrative services. This is referred to as an open system, because it is possible to establish a secure crypto connection with other TopSec Mobile encryption devices without the need for certificate-based authentication. The session key "K" calculated by the two partner encryption devices is used by the symmetric algorithms to encrypt or decrypt the digitized and compressed voice information.

This open system uses a four-digit security code to prevent man-in-the-middle attacks. A new code is calculated on both TopSec Mobile encryption devices for each encrypted call and is displayed on the TopSec Mobile's built-in screen. When the security codes are identical, a secure call is established.

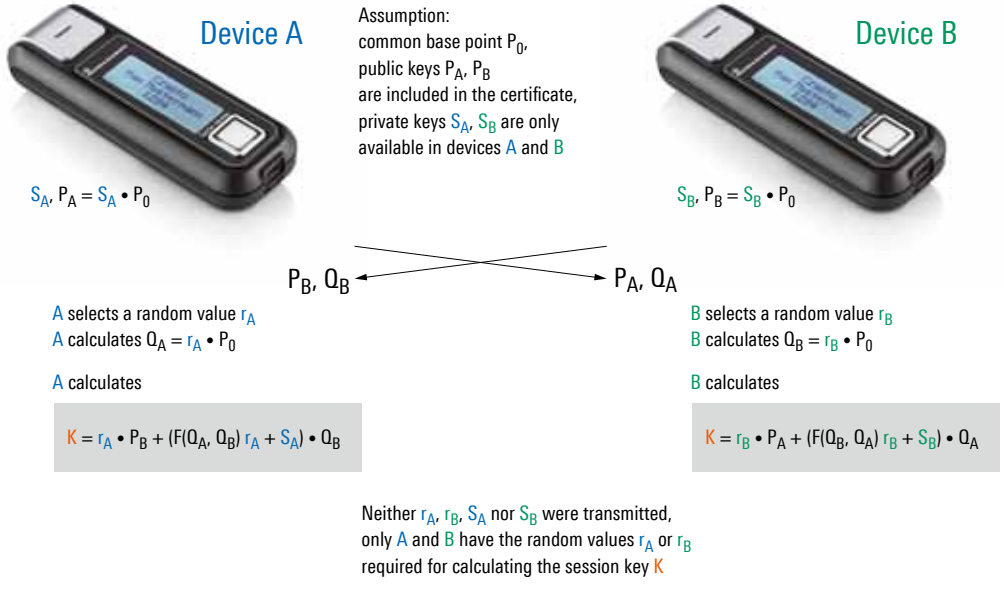
Certificate-based authentication

Another measure to prevent man-in-the-middle attacks is to create closed user groups. This requires the TopSec Administrator, which combines the functions of a trust center with the centralized administration of operational parameters. During an initialization process, the TopSec devices receive a certificate and generate a public key pair that is used for authentication. In closed systems, authentication between the TopSec encryption devices takes place automatically. An encrypted connection is only established if authentication is successful. Consequently, calls made using the TopSec encryption devices meet the highest security requirements.

Voice encryption using the Advanced Encryption Standard (AES) 256-bit key

The TopSec Mobile and the partner encryption device automatically agree on a new 256-bit key during each call setup. A key is randomly selected from a pool of 10^{76} possible keys and then deleted immediately upon completion of the call.

Combined key agreement and authentication



Specifications

Specifications	
TopSec Mobile	
Bluetooth® standard	version 2.0
Standby time	up to 100 h
Talk time	up to 4 h
Dimensions	99 mm × 34 mm × 22 mm (3.9 in × 1.3 in × 0.9 in)
Weight	58 g (0.13 lb)
TopSec Phone	
TopSec Phone app for Android	Android operating system version 2.3/4.0
TopSec Phone app for iPhone	iPhone operating system version 5/5.1
VoIP protocols	
SIP	RFC3261
IAX2	RFC5456

Product overview

Designation	Type
Voice Encryption Device	TopSec Mobile
App for Android	TopSec Phone for Android
App for iPhone	TopSec Phone for iPhone
VoIP Server	R&S®VoIP-SERVER S110
Administrator Software	TopSec Admin

Service you can rely on

- Worldwide
- Local and personalized
- Customized and flexible
- Uncompromising quality
- Long-term dependability

About Rohde&Schwarz

Rohde&Schwarz is an independent group of companies specializing in electronics. It is a leading supplier of solutions in the fields of test and measurement, broadcasting, radiomonitoring and radiolocation, as well as secure communications. Established more than 75 years ago, Rohde&Schwarz has a global presence and a dedicated service network in over 70 countries. Company headquarters are in Munich, Germany.

Environmental commitment

- Energy-efficient products
- Continuous improvement in environmental sustainability

Certified Quality System
ISO 9001

Rohde&Schwarz SIT GmbH
Am Studio 3 | D-12489 Berlin
Phone +49 30 65884-223 | Fax +49 30 65884-184
E-mail: info.sit@rohde-schwarz.com
www.sit.rohde-schwarz.com

Rohde&Schwarz GmbH&Co. KG
www.rohde-schwarz.com

Regional contact

- Europe, Africa, Middle East | +49 89 4129 12345
  customersupport@rohde-schwarz.com
- North America | 1 888 TEST RSA (1 888 837 87 72)
  customer.support@rsa.rohde-schwarz.com
- Latin America | +1 410 910 79 88
  customersupport.la@rohde-schwarz.com
- Asia/Pacific | +65 65 13 04 88
  customersupport.asia@rohde-schwarz.com
- China | +86 800 810 8228/+86 400 650 5896
  customersupport.china@rohde-schwarz.com

PD 3606.6492.12 | Version 02.00 | May 2012 | TopSec Mobile

3606649212