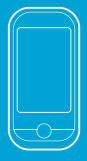
TopSec Mobile

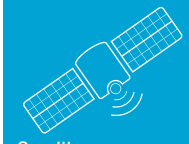
Tap-proof phone calls


iPhone


Android smartphone


PC


Fixed network


Satellite

ROHDE&SCHWARZ

Secure Communications

Product Brochure | 03.00

TopSec Mobile
At a glance

The TopSec Mobile is a mobile encryption device for tap-proof end-to-end voice calls using smartphones, PCs, fixed-network phones and satellite terminals.

Companies and government authorities use telephones and smartphones to share confidential information. However, voice calls, particularly on mobile devices, can be easily tapped and recorded. This is why official secrets and confidential company data must be protected by powerful encryption. At the same time, users want a simple and flexible security solution that enables them to make phone calls as usual without complicated communications processes.

The TopSec Mobile meets the highest security requirements and enjoys a high level of user acceptance. It is an external encryption device that connects to smartphones, PCs and satellite terminals via Bluetooth®. The TopSec Mobile is used whenever a conversation needs to be confidential. Voice input, encryption and output takes place exclusively on the trustworthy TopSec Mobile hardware, out of reach of viruses, Trojans and other spyware.

Key facts

- External encryption device for highest security requirements
- Smartphones maintain full functionality; existing communications devices and infrastructures can still be used
- Maximum flexibility thanks to Bluetooth® connection to commercial iPhones, Android smartphones and PCs
- Secure end-to-end voice calls in IP-based networks (secure VoIP)
- Worldwide contactability in wireless, wired and satellite IP networks
- Voice encryption using the Advanced Encryption Standard (AES) 256-bit key

TopSec Mobile
Benefits and key features

Highly versatile voice encryption
- Protection of smartphones, PCs and satellite terminals
- Support of public and private VoIP servers
- High security zones without mobile network coverage
- Worldwide crypto connections
- Device pools for tap-proof cooperation in project teams
- In the office or in the field – tap-proof voice calls for all employees

▷ page 4

Intuitive and user-friendly operation
- Encrypted voice calls via external crypto headset
- Easy operation using the TopSec phone app
- Intuitive security
- Brilliant voice quality and low latency
- Familiar communications devices

▷ page 6

Advanced encryption methods
- Hybrid approach for maximum security
- Elliptic curve Diffie-Hellman key agreement protocol
- Certificate-based authentication
- Voice encryption using the Advanced Encryption Standard (AES) 256-bit key for perfect forward secrecy

▷ page 8

Communicate as usual: For a secure phone call, the TopSec Mobile is used like a headset.

Highly versatile voice encryption

Protection of smartphones, PCs and satellite terminals

The TopSec Mobile can be connected to IP networks via almost all modern communications devices. Smartphones provide wireless access to UMTS networks and WLANs. Laptops, notebooks and PCs have an additional LAN port to enable a wired connection. The TopSec Mobile also enables users to encrypt communications via BGAN and Thuraya satellite terminals.

Support of public and private VoIP servers

VoIP connections between registered communications partners are set up via a server. The TopSec Mobile is compatible with two leading VoIP server protocols, SIP and IAX2. For companies and government authorities, Rohde&Schwarz offers the R&S®VoIP-SERVER, a preconfigured VoIP server product that permits operation in a secure server environment. Organizations can easily integrate the R&S®VoIP-SERVER into their own IT infrastructures.

High security zones without mobile network coverage

In tap-proof conference rooms, situation centers and development labs, mobile networks are often unavailable, or the use of mobile phones is not permitted for security reasons. In these special environments, the TopSec Mobile can be used to make encrypted calls by connecting via Bluetooth® or USB to an existing PC to access the network.

Worldwide crypto connections

Demanding tasks such as developing new sources of raw material in geographically remote areas also require encrypted communications. The TopSec Mobile can be paired with communications devices that are connected to BGAN or Thuraya satellite terminals.

External, hardware-based voice encryption for iPhones, Android smartphones, PCs, fixed-network phones and satellite terminals.

Device pools for tap-proof cooperation in project teams

Thanks to external voice encryption, protection against tapping is not limited to a specific communications device. Purchased TopSec Mobiles can be used by different employees. This is very advantageous for companies where the members of project teams change, especially for international sales engineers and R&D teams, or when employees and freelancers are involved in special projects such as strategic acquisitions.

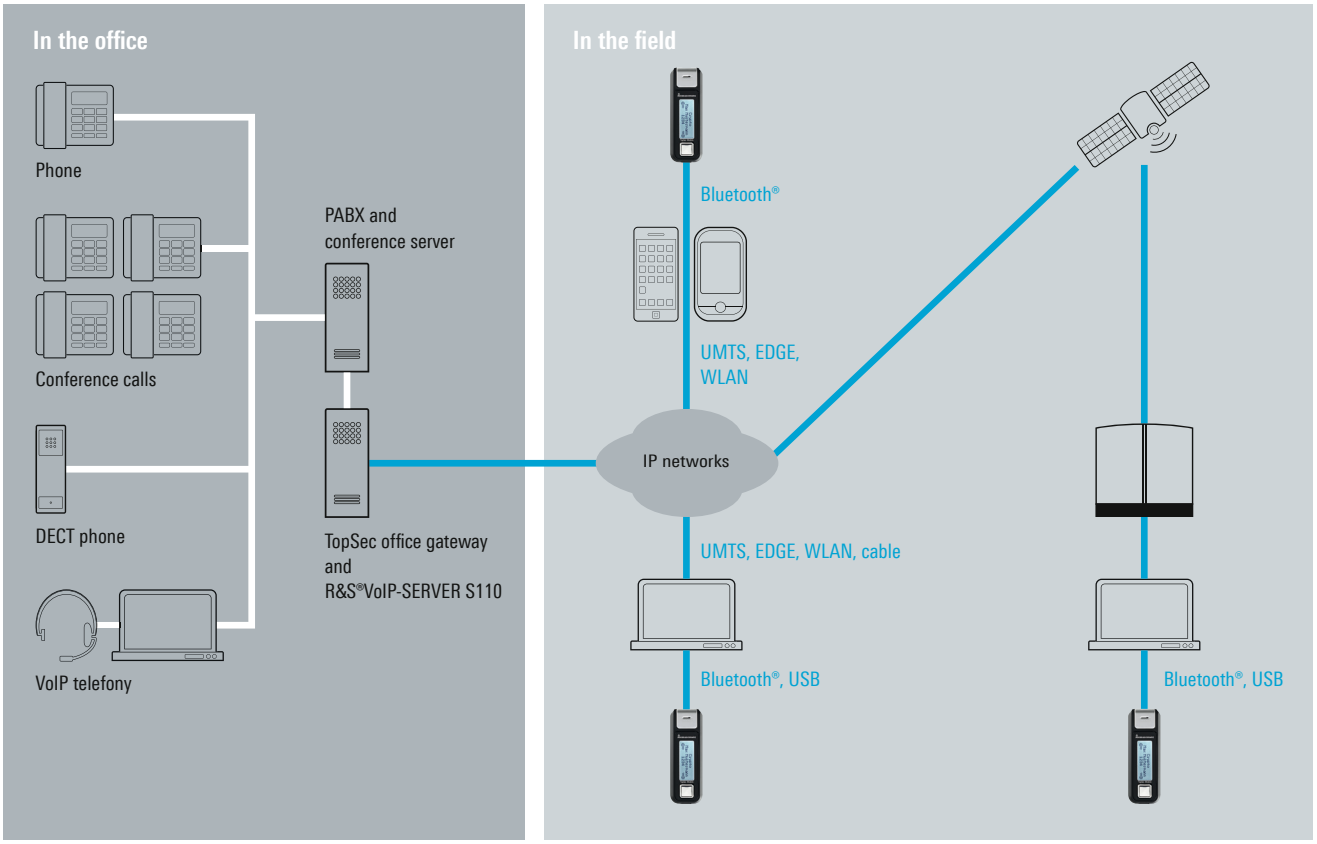
In the office or in the field – tap-proof phone calls for all employees

The TopSec office gateway allows employees who work in the field to make encrypted phone calls on their mobile phones to all fixed-network phones in their organization. Calls from a TopSec Mobile to the company's own telephone system are accepted by picking up the phone as usual. To make an encrypted call from a fixed-network phone to a TopSec Mobile, users simply need to enter a variable prefix.

Encryption and decryption are carried out in the server room, unnoticed by the user. In the server room, the TopSec office gateway is connected to the company's VoIP telephone system via standard protocols using SIP trunking.

Since the TopSec office gateway runs on server hardware with different performance classes, the number of possible simultaneous encrypted calls can be matched to meet user requirements.

Encrypted calls between the office and employees in the field



Intuitive and user-friendly operation

The compact, handy TopSec Mobile measures less than 10 cm in length and weighs only 58 g.

Encrypted voice calls via external crypto headset

Users can make confidential calls either directly with the TopSec Mobile or with the included headset. The calls are encrypted and decrypted in the TopSec Mobile. The voice data sent from and to the TopSec Mobile is secured at the highest possible level when transmitted via the Bluetooth® interface. The communications device is merely used to transmit the encrypted VoIP data. Call interception is futile. The encrypted information cannot be decrypted by a third party. The smartphone's microphone and speaker are disabled.

Easy operation using the TopSec phone app

Users choose a contact on their smartphones as usual, using the intuitive TopSec phone app, which includes a contact list and call list. The call recipient's TopSec Mobile rings instead of the recipient's usual mobile device.

The recipient accepts the call by pressing a button on the TopSec Mobile, causing the caller's TopSec Mobile to ring or vibrate. The caller presses a button to accept the call. Keys are then exchanged and a secure link is set up. To eliminate the possibility of a man-in-the-middle attack, a four-digit security code appears on both TopSec Mobile devices. This security code can be verbally compared at the start of the conversation, which offers additional security.

Intuitive security

In contrast to integrated one-box solutions where users need to pay close attention to device messages, the security concept of the TopSec Mobile provides a clear overview and a high degree of transparency. When the external crypto headset is used, the call is always encrypted. When the smartphone is used, the call is always unencrypted. Supposedly secure unencrypted calls are avoided.

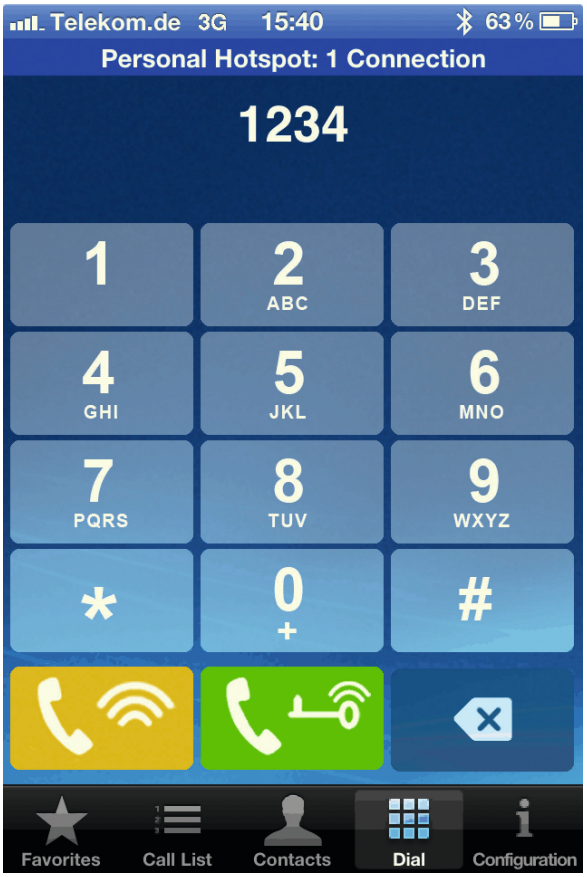
Brilliant voice quality and low latency

In addition to the intuitive operation and high flexibility, users especially appreciate the brilliant sound quality when making encrypted calls with the TopSec Mobile and TopSec office gateway. The latency due to encryption is extremely low and there are no perceptible delays in the conversation.

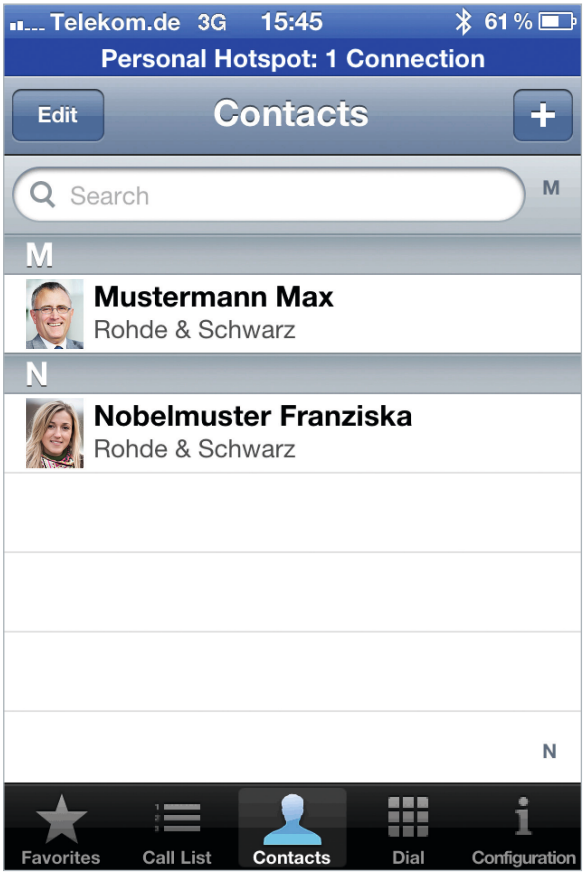
Familiar communications devices

The TopSec Mobile ensures maximum protection against attacks from the network or smartphone malware, while allowing users to continue using their familiar smartphones without requiring special ruggedization. Users do not need to get used to an unfamiliar new encryption device with limited functions. The TopSec office gateway acts as an interface to the company network and employees can be reached on their normal phones while in the office. This increases its acceptance in government authorities and companies.

The keypad 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 app contact list.



Advanced encryption methods

Hybrid approach for maximum security

Encryption in the TopSec Mobile is based on a hybrid approach 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.

Elliptic curve Diffie-Hellman key agreement protocol

The Diffie-Hellman key agreement protocol with 384-bit elliptical curves enables encrypted communications between two TopSec encryption devices without the need for central administrative services. The session key "K" calculated by the two encryption devices is used by the symmetric algorithms to encrypt or decrypt the digitized and compressed voice information. A four-digit security code is used 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 built-in screen. In a connection without a man in the middle, the security codes are identical.

Certificate-based authentication

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

The TopSec Mobile displays the word "Crypto" and a four-digit security code to confirm that an encrypted connection has been established.

Voice encryption using the Advanced Encryption Standard (AES) 256-bit key for perfect forward secrecy

The TopSec Mobile and the partner encryption device automatically agree on a new random 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, ensuring perfect forward secrecy.

Combined key agreement and authentication

Assumption:
common base point P_0,
public keys P_A, P_B
are included in the certificate,
private keys S_A, S_B are only
available in devices A and B

S

P_B, Q_B → P_A, Q_A

A selects a random value r_A
A calculates $Q_A = r_A \bullet P_0$

A calculates

$$K = r_A \bullet P_B + (F(Q_A, Q_B)\, r_A + S_A) \bullet Q_B$$

B selects a random value r_B
B calculates $Q_B = r_B \bullet P_0$

B calculates

$$K = r_B \bullet P_A + (F(Q_B, Q_A)\, r_B + S_B) \bullet Q_A$$

Neither r_A, r_B, S_A nor S_B were transmitted, only A and B have the random values r_A or r_B required for calculating the session key K

Specifications

Specifications	
TopSec Mobile	
Bluetooth® standard	version 2.0
Operating 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
TopSec phone app for iPhone	iPhone operating system, version 5 or later
TopSec phone app for Windows PCs	Windows 7, Windows 8
VoIP protocols	
SIP	RFC 3261
IAX2	RFC 5456

Ordering information

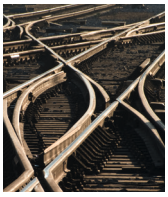
Designation	Type
Voice Encryption Device	TopSec Mobile
App for Android	TopSec Phone for Android
App for iPhone	TopSec Phone for iPhone
App for Windows	TopSec Phone for Windows 7 and Windows 8
VoIP Server	R&S®VoIP-SERVER S110
Administrator Software	TopSec Admin
Gateway for Telephone System	TopSec Office Gateway

You act. We protect.
Rohde&Schwarz SIT

Encryption and IT security

Industry

An organization's product ideas, manufacturing processes, patents and financial data make up around 70 percent of its intangible assets. These trade and business secrets are fundamental to the organization's ability to create added value and require special protection. The IT security solutions from Rohde&Schwarz SIT protect companies worldwide against espionage and manipulation of data. The products combine maximum protection with a minimum of administrative effort and offer users an optimum price/performance ratio. The Rohde&Schwarz SIT product portfolio comprises encryption solutions for protecting data transmission in public and private networks, next-generation firewalls for ensuring the secure use of clouds and the Internet, and flexible solutions for tap-proof voice calls.



Critical infrastructures

Critical infrastructures keep our society and economy functioning smoothly. Attempts to manipulate the infrastructures on which energy suppliers, transport operators, emergency services and the financial sector rely could pose a serious threat to public safety. Rohde&Schwarz SIT offers operators of critical infrastructures smart IT security products to secure the control and communications networks between power plants, switch towers, tollbooths, radio masts and network nodes. In addition to encryption solutions for networks and end-to-end communications, hardware security modules (HSM) in public key infrastructures protect corporate campuses and installations from unauthorized access.

Government

A country's internal political dealings encompass a wide range of sensitive topics, including economic and fiscal affairs and energy policy. Internal communications among policymakers, government authorities as well as public safety and security (PSS) agencies need to remain confidential. For more than 20 years, Rohde&Schwarz SIT has been supplying highly secure solutions that ensure absolute confidentiality at all security classification levels. To safeguard their sovereignty, countries can use their own national cryptographic algorithms. The Rohde&Schwarz SIT product portfolio includes encryption products for all classification levels to protect networks and end-to-end communications. The products for government use are approved by Germany's Federal Office for Information Security (BSI) and by the EU and NATO (up to top secret and cosmic top secret security classification levels).

Armed forces

Operations launched to protect societies involve serious risk. Precise, timely information is necessary for strategic command of operations such as peacekeeping, humanitarian aid and disaster relief. Maintaining information superiority has the utmost priority. Rohde&Schwarz SIT, an IT security partner to the Federal Republic of Germany since 2004, is involved in various NATO equipment programs. The company provides solutions for effectively protecting voice, data, images and video transmitted over fixed-networks, radio relay and satellite links. Rohde&Schwarz SIT stands for long-term product availability and the interoperability of solutions with existing equipment. The products for military use are approved by Germany's Federal Office for Information Security (BSI) and by NATO and the EU (up to top secret and cosmic top secret security classification levels).

Service that adds value

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

About Rohde&Schwarz

The Rohde&Schwarz electronics group is a leading supplier of solutions in the fields of test and measurement, broadcasting, secure communications, and radiomonitoring and radiolocation. Founded more than 80 years ago, this independent global company has an extensive sales network and is present in more than 70 countries.
The company is headquartered in Munich, Germany.

Sustainable product design

- Environmental compatibility and eco-footprint
- Energy efficiency and low emissions
- Longevity and optimized total cost of ownership

Certified Quality Management
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

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 03.00 | February 2014 (ch)
TopSec Mobile
Data without tolerance limits is not binding | Subject to change

3606649212

3606.6492.12 03.00 PDP 1 en