

# TopSec Product Family

## Voice encryption at the highest security level



**75** Years of  
Driving  
Innovation

  
**ROHDE & SCHWARZ**

# TopSec Product Family At a glance

The TopSec product family provides end-to-end voice encryption at the highest security level, across networks. The devices of the TopSec product family for encrypted transmission are the ideal solution when confidential and tap-proof information is to be transmitted.

The TopSec product family offers a suitable security solution for every application. It can be used to secure voice communications as well as video, data and fax transmissions.

Mobile phone users can choose between the TopSec Mobile, a voice encryption device equipped with a Bluetooth® interface, and the TopSec GSM, a mobile phone enhanced with a crypto module. Users with a digital Euro ISDN connection employ the TopSec 703+, those with an analog connection use the TopSec 711.

The TopSec Mobile, TopSec GSM, TopSec 703+ and TopSec 711 voice encryption devices are interoperable. Secure end-to-end voice encryption is possible within mobile radio networks, digital networks or analog networks, and can even be established across networks.

The TopSec product family is supplemented by the TopSec Administrator administration software. TopSec Administrator makes it possible to create cryptological user groups and generates certificates for the TopSec devices, which enable automatic authentication. TopSec Administrator allows secure administration and secure firmware updates.



# TopSec Product Family Benefits and key features

## **A suitable solution for every application**

- TopSec products:
  - TopSec Mobile voice encryption device
  - TopSec GSM encrypting mobile phone
  - TopSec 703+ encryption device for digital connections
  - TopSec 711 encryption device for analog connections
  - TopSec Administrator administration software
- Interoperability between the TopSec devices

▷ [page 4](#)

## **Reliable encryption concept**

- Hybrid approach for maximum security
  - Asymmetric method using 1024 bit encryption key length for key agreement
  - Symmetric encryption algorithm with a 128 bit encryption key:  $10^{38}$  possible keys

▷ [page 6](#)

## **Authentication for maximum security**

- Spoofed encrypted connections are prevented
- Man-in-the-middle attacks are prevented
- Ability to create closed user groups

▷ [page 7](#)

## **User-managed encryption**

- TopSec Administrator
- Open user groups
- Closed user groups

▷ [page 8](#)

## **TopSec Administrator — the convenient administration software**

- Trust center functionality
- Remote administration
  - Distribution of certificates
  - Black lists
  - White lists
- Settings for operational parameters

▷ [page 10](#)

# A suitable solution for every application

## TopSec Mobile voice encryption device

The TopSec Mobile is a highly versatile voice encryption device equipped with a Bluetooth® interface. The TopSec Mobile does not connect directly to communications network; instead, it connects to a communications terminal equipment such as a mobile phone. A TopSec Mobile allows encrypted communications with an interoperable partner encryption device using almost any mobile phone with a Bluetooth® interface. In order for this to work, it must be possible to activate the mobile phone's data service via Bluetooth®, which is possible with most mobile phones.

This solution offers two significant advantages: First, the TopSec Mobile is not confined to specific mobile radio frequencies. Second, users enjoy a great deal of freedom when choosing a mobile phone.

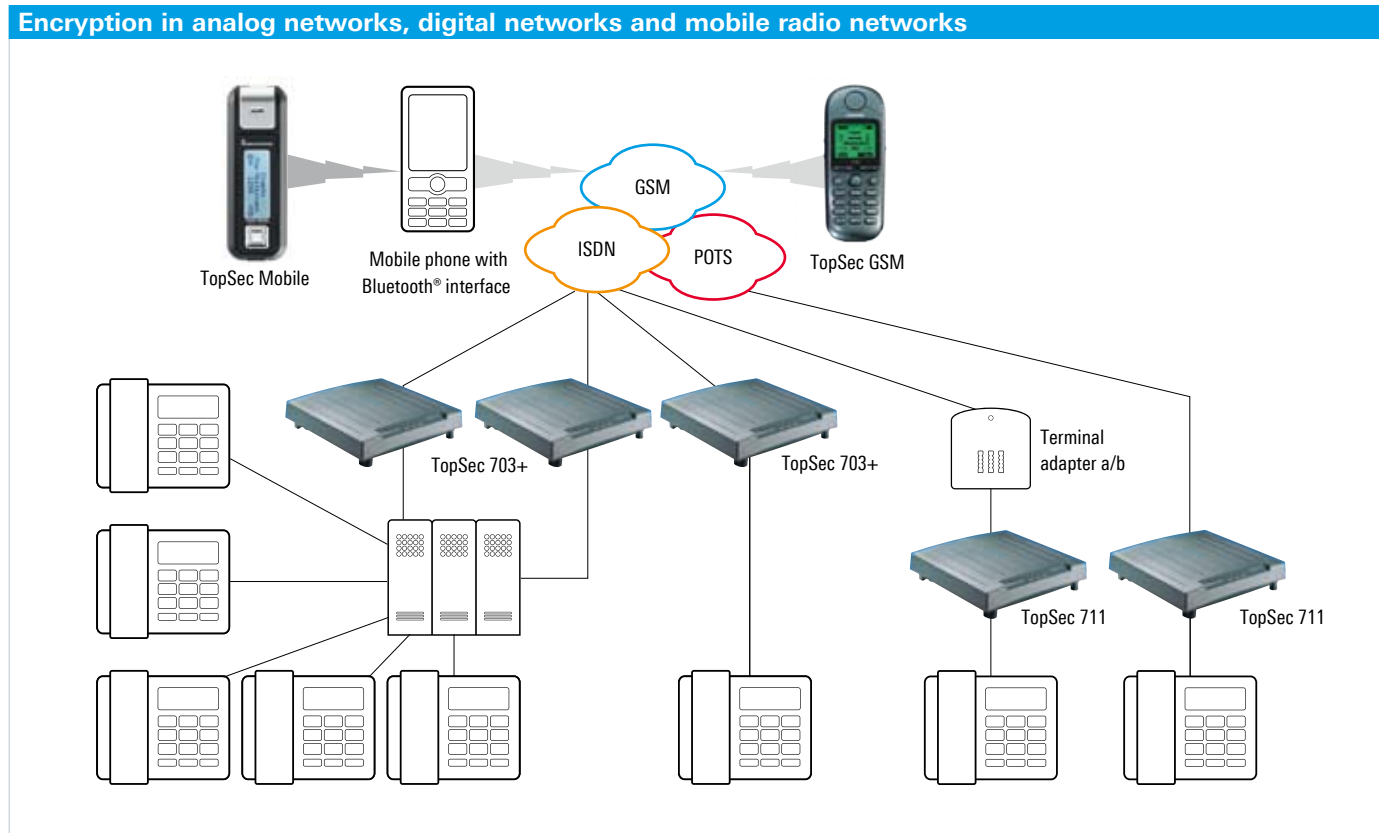
Besides the encryption components, the audio components (microphone and speaker) are also incorporated into the TopSec Mobile. This means that, in addition to the option of using a mobile phone, it is also possible to use an analog or ISDN modem with Bluetooth® for enabling the TopSec Mobile to gain network access.

For encrypted communications, the TopSec Mobile uses a data rate of 9.6 kbps. It can use either the ITU-T V.32 or V.110 communications protocol. Voice information is digitized and compressed with a vocoder prior to encryption.

## TopSec GSM encrypting mobile phone

The TopSec GSM is a dual-band encrypting mobile phone for the GSM network. This mobile phone is equipped with an integrated TopSec crypto module. To transmit encrypted voice information, the TopSec GSM uses a data channel with a data rate of 9.6 kbps. Depending on the specific partner encryption device, either the ITU-T V.32 or V.110 communications protocol is used. The voice information is digitized and compressed with a vocoder prior to encryption.

TopSec-secured communications between subscribers in an analog network, a digital network and a mobile radio network.



### TopSec 703+ encryption device for digital connections

The TopSec 703+ is an encryption device for digital Euro ISDN networks. It allows the encrypted transmission of all ISDN services. This means that voice, video, data and fax signals can be encrypted. Encryption is accomplished at the full data rate up to  $2 \times 64$  kbps.

The TopSec 703+ also enables secure voice communications with a TopSec Mobile or a TopSec GSM as a partner encryption device. In this scenario, the device supports ITU-T V.110 with a data rate of 9.6 kbps. The voice information is digitized and compressed with a vocoder prior to encryption.

### TopSec 711 encryption device for analog connections

The TopSec 711 is an encryption device with analog interfaces. It can be used for voice or fax encryption. The TopSec 711 is connected between the analog communications network and a phone with an analog interface. As an alternative, the TopSec 711 can be connected to a terminal adapter for integration into a digital network.

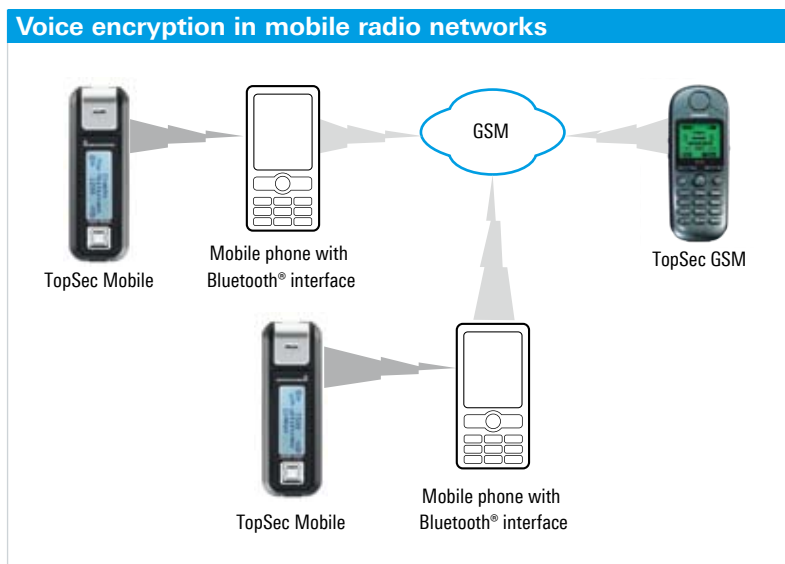
For encrypted communications, a data rate of 9.6 kbps is used. For communications with a partner encryption device, the ITU-T V.32 communications protocol is used. Prior to encryption, the voice information is digitized and compressed with a vocoder.

### TopSec Administrator administration software

The TopSec Administrator administration software offers a wide range of additional capabilities for securing a communications system. TopSec Administrator is available for installation on a Windows-based computer. TopSec Administrator serves as the central, trusted authority for a closed user group.

### Interoperability between the TopSec devices

The TopSec Mobile voice encryption device and the TopSec GSM encrypting mobile phone are interoperable with the TopSec 703+ and TopSec 711 fixed network encryption devices. For encrypted communications with the TopSec 703+, the ITU-T V.110 communications protocol is used; for encrypted communications with the TopSec 711, the ITU-T V.32 communications protocol is used.



### Interoperability matrix for voice encryption with TopSec devices

	TopSec Mobile	TopSec GSM	TopSec 703+	TopSec 711
TopSec Mobile	V.110, V.32	V.110, V.32	V.110	V.32
TopSec GSM	V.110, V.32	V.110, V.32	V.110	V.32
TopSec 703+	V.110	V.110	V.110	
TopSec 711	V.32	V.32		V.32

# Reliable encryption concept

## Hybrid approach for maximum security

The TopSec encryption processes have proven themselves in practical use. Encryption is based on a hybrid process in order to achieve the highest levels of security. This approach combines an asymmetric algorithm for key agreement with a symmetric algorithm for encrypting confidential information.

## Encryption concept

The encryption process used with the TopSec product family is designed to enable secure communications between two communicating parties. It is possible for the encryption devices to verify that both parties belong to the same closed user group.

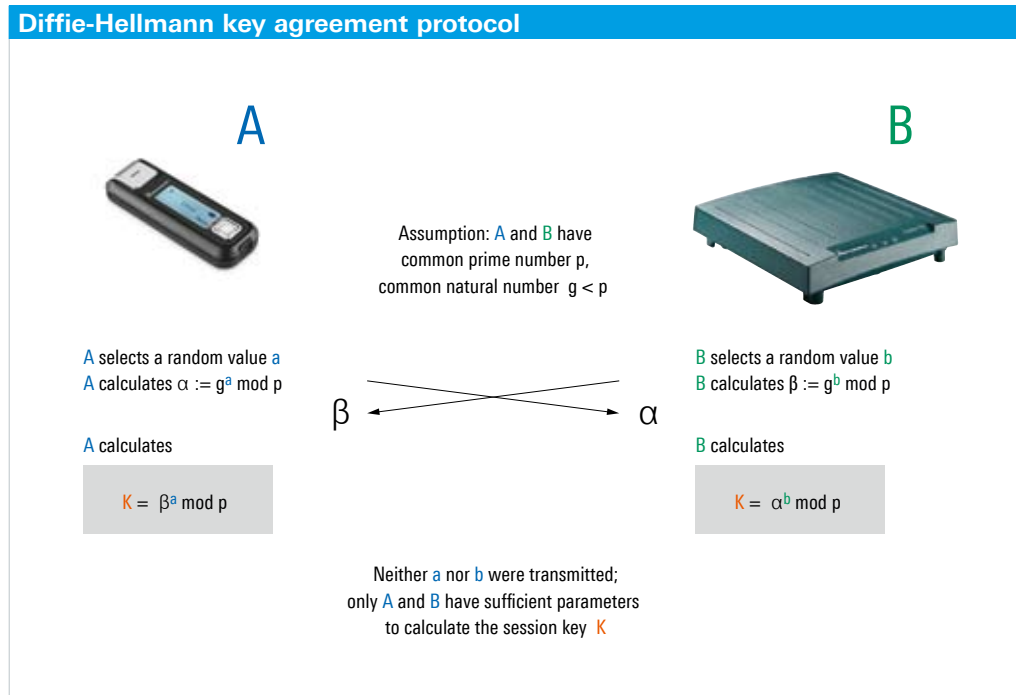
For an encrypted conversation, the partner encryption devices must have the same mathematical parameters at their disposal and use identical algorithms. The TopSec encryption devices utilize the Diffie-Hellman key agreement protocol to generate individual session keys for each call (see figure). The Diffie-Hellman key agreement protocol is a public key method.

This means that both public and secret parameters are used. Both parameters are pre-installed during the manufacturing process and delivered with the equipment.

The secret parameters of the Diffie-Hellman key agreement protocol are only generated temporarily for the relevant encrypted connection. Afterwards, the parameters are deleted. Using 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 crypto connection between any two TopSec encryption devices. 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.

## Encryption with a 128 bit encryption key: $10^{38}$ possible keys

In encryption mode, the devices of the TopSec product family and the partner encryption device automatically agree on a new 128 bit key during each call setup. A key is selected at random from a pool of  $10^{38}$  possible keys. The key is deleted immediately upon completion of the call.



# Authentication for maximum security

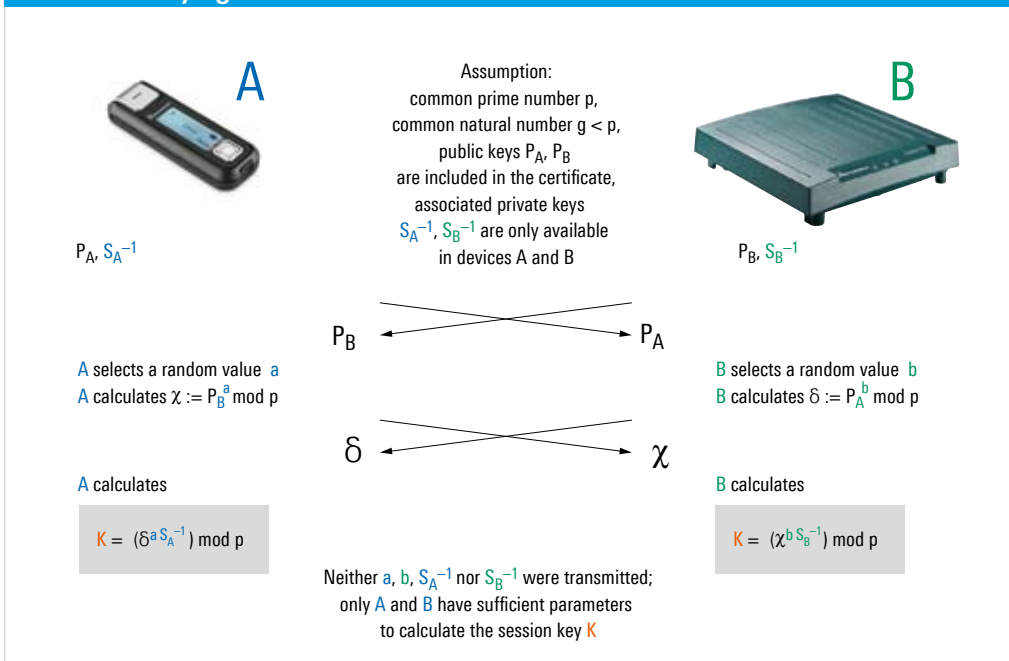
## Spoofer encrypted connections and man-in-the-middle attacks are prevented

TopSec encryption device users want to be certain that they have a secure, encrypted connection with their partner. All spoofed encrypted connections, and man-in-the-middle attacks in which unauthorized third parties masquerade as the legitimate communications partner, must be avoided.

In theory, the Diffie-Hellman key agreement protocol is susceptible to a man-in-the-middle attack. Although such attacks require tremendous effort, the TopSec encryption concept includes measures for detecting and preventing them.

For this purpose, a unique four-digit security code is generated for each encrypted connection. This code is displayed on and is only available in the TopSec encryption device and the partner encryption device. A secure call can be conducted only when the security codes are identical. With closed user groups, the system also performs certificate-based, automatic authentication between the TopSec partner encryption devices.

### Combined key agreement and authentication



# User-managed encryption

## Open user group

Upon delivery the encryption devices of the TopSec product family are able to begin cryptographic operation with other devices of the same product family; they use the open user group. Within a key agreement protocol (see figure on page 6 for the Diffie-Hellman key agreement protocol), the session keys are always generated for each connection and are immediately deleted upon completion of the call. To prevent the possibility of a man-in-the-middle attack, the two communicating parties check that the four-digit security code is the same on both devices. This provides extremely effective encryption management without any additional effort.

## TopSec certification

Creating a digital signature using TopSec Administrator

Certificate

Device ID

Name of trust center  
Parameter 1  
Parameter 2  
Parameter n  
Parameter k  
Parameter xyz  
 $P_U$

Creation of hash value

Hash value

Digital signature

RSA signature with  $S_U$

Generation of  $P_U$

Prime number  $p$ , generator  $g$

Device  $U$  generates  $S_U$ ;  $1 < S_U < p-1$ ;  $\text{GCD}(S_U, p-1) = 1$

$S_U^{-1}$  is the inverse of  $S_U$ ;  $S_U S_U^{-1} = 1 \pmod{p-1}$

$P_U = g^{S_U} \pmod{p}$

Device  $U$  saves  $P_U, S_U^{-1}, P_{TC}$

$P_U$  is part of the certificate

Checking the digital signature using the TopSec Mobile

Certificate

Device ID

Name of trust center  
Parameter 1  
Parameter 2  
Parameter n  
Parameter k  
Parameter xyz  
 $P_U$

Creation of hash value

Hash value

Digital signature

RSA verification with  $P_{TC}$

?  
=

Hash value

All TopSec devices within a closed system receive a certificate from TopSec Administrator. This certificate confirms their membership in a specific user group.

## Closed user groups

Another way to prevent man-in-the-middle attacks and limit the number of potential partners for secure communications connections is to create closed user groups.

This requires an entity referred to in some systems as a trust center. In the TopSec system, this trust center is called TopSec Administrator. TopSec Administrator combines the functions of a trust center with the centralized administration of operational parameters. The trust center function is required when creating closed user groups.

All TopSec devices within a closed system receive an individual certificate from TopSec Administrator. This certificate confirms membership in the group. The certificate contains information defined in the ITU-T X.509 standard. The most important pieces of information contained in the certificate are the device ID for the TopSec device and a corresponding public authentication key. The certificate contains a digital signature. Within TopSec Administrator, a public key pair is generated for this digital signature. This pair consists of a public and a private key. The certificate's hash value is signed using the private key  $S_{TC}$  (digital signature). The private key  $S_{TC}$  remains in TopSec Administrator because it is the most confidential part of a closed system. The public key  $P_{TC}$  is used to verify the digital signature, and thus validate the certificate.

TopSec devices that belong to a closed system generate an additional public key pair during initialization. This pair is used for authentication. The private authentication key  $S_U^{-1}$  remains stored in the TopSec device; the public authentication key  $P_U$  is included in the certificate. Together with the certificate, the TopSec devices receive the public key  $P_{TC}$  for validating certificates.

TopSec devices that are already members of a closed system can later be supplied with new certificates and the associated public key via public communications networks. This is accomplished using a secure process that is protected against manipulation and includes authentication by TopSec Administrator. Devices that have certificates and belong to the same closed system are able to authenticate each other automatically. To accomplish this, each encryption device first examines the certificate that identifies its partner encryption device. This is followed by a combined process for key agreement and authentication (see figure on page 7 for the Combined key agreement and authentication). An encrypted connection is only established if this process succeeds. In addition, the communicating parties can verify the authentication by checking the four-digit security code. Consequently, calls made using the TopSec encryption devices meet the highest security requirements.

# TopSec Administrator — the convenient administration software

## Trust center functionality

The TopSec Administrator administration software offers additional options for securing the system. A connection between a TopSec encryption device and TopSec Administrator via a telecommunications network is always encrypted. Using this encrypted connection, the TopSec encryption devices and TopSec Administrator authenticate each other's identity before any device configuration takes place. TopSec Administrator is a trust center that is run under the responsibility of the system operator.

## Remote administration

Administered TopSec encryption devices that are members of a closed user group can be configured by TopSec Administrator via the public network (remote administration). Using this remote administration process, it is possible to issue new certificates and distribute black lists and white lists.

## Black lists

Black lists contain device IDs that are not allowed to participate in a specific user group's cryptographic operation. (These device IDs are also included in the certificates.)

## White lists

Within a closed user group, white lists allow additional segmentation of the potential communicating parties. Only those TopSec encryption devices that are entered in a white list in the same subgroup can establish an encrypted connection.

## Settings for operational parameters

For TopSec encryption devices that are managed by TopSec Administrator, this software can set operational parameters — depending on the specific device model. For example, with the TopSec 711, it is possible to determine whether pulse dialing or tone dialing is to be used for call setup. The software for the TopSec 711 and TopSec 703+ can be updated securely by TopSec Administrator via a telecommunications network.

# Specifications

TopSec voice encryption devices	
<b>Data rate with voice encryption</b>	
TopSec Mobile, TopSec GSM, TopSec 703+, TopSec 711	9.6 kbps
<b>Maximum data rate</b>	
TopSec 703+	up to 2 × 64 kbps
TopSec 711 (fax mode)	up to 14400 bps
<b>Communications protocol used with the partner encryption device</b>	
TopSec Mobile, TopSec GSM, TopSec 703+	V.110
TopSec Mobile, TopSec GSM, TopSec 711	V.32
<b>Communications interface</b>	
TopSec GSM	GSM900/1800
TopSec Mobile	Bluetooth®, version 2.0
TopSec 703+	four-wire, basic rate interface (S <sub>0</sub> ), Euro ISDN
TopSec 711	two-wire, analog interface

# Ordering information

Designation	Type	Order No.
Voice Encryption Device	TopSec Mobile	5411.0002
Encrypting Mobile Phone	TopSec GSM	3531.6527
Encryption Device for digital connections	TopSec 703+	3531.6504
Encryption Device for analog connections	TopSec 711	5400.2450
Administration Software	TopSec Administrator	3531.6610

## 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 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
- | ISO 14001-certified environmental management system

Certified Quality System  
**ISO 9001**

## Rohde & Schwarz SIT GmbH

Am Studio 3 | D-12489 Berlin  
+49 30 65884-223 | Fax +49 30 65884184  
E-Mail: [info.sit@rohde-schwarz.com](mailto:info.sit@rohde-schwarz.com)  
[www.sit.rohde-schwarz.com](http://www.sit.rohde-schwarz.com)

[www.rohde-schwarz.com](http://www.rohde-schwarz.com)

## Regional contact

- | Europe, Africa, Middle East  
+49 89 4129 137 74  
[customersupport@rohde-schwarz.com](mailto:customersupport@rohde-schwarz.com)
- | North America  
1 888 TEST RSA (1 888 837 87 72)  
[customer.support@rsa.rohde-schwarz.com](mailto:customer.support@rsa.rohde-schwarz.com)
- | Latin America  
+1 410 910 79 88  
[customersupport.la@rohde-schwarz.com](mailto:customersupport.la@rohde-schwarz.com)
- | Asia/Pacific  
+65 65 13 04 88  
[customersupport.asia@rohde-schwarz.com](mailto:customersupport.asia@rohde-schwarz.com)