

R&S® TopSec Mobile

TopSec Phone Windows PC

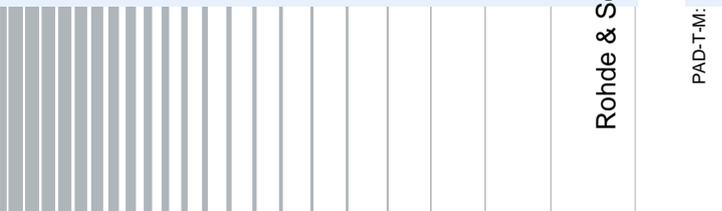
Usermanual



1234.5678.02 – 01

Rohde & Schwarz SIT GmbH
Usermanual

PAD-TM:



© 2013 Rohde & Schwarz GmbH & Co. KG

Muehldorfstr. 15, 81671 Munich, Germany

Phone: +49 89 41 29 - 0

Fax: +49 89 41 29 12 164

E-mail: info@rohde-schwarz.com

Internet: <http://www.rohde-schwarz.com>

Subject to change – Data without tolerance limits is not binding.

R&S[®] is a registered trademark of Rohde & Schwarz GmbH & Co. KG.

Trade names are trademarks of the owners.

The following abbreviations are used throughout this manual:

R&S[®]TopSec Mobile is abbreviated as R&S TopSec Mobile

Contents

1	Product-specific safety advices / additional notes	5
2	Documentation Overview	7
3	Conventions Used in the Documentation	9
4	Requirements	11
4.1	System requirements	11
4.2	Operational requirements	11
5	Icons and terms	13
6	Installation	14
6.1	Functional tests	14
7	Configuration and setup	16
7.1	VoIP server	16
7.2	Pairing with the TopSec Mobile.....	17
8	Usage	19
8.1	Starting the app.....	19
8.2	Overview	19
8.3	Contacts.....	20
8.3.1	Calling a contact	20
8.3.2	Managing contacts.....	22
8.4	Manual dialing via the keypad	23
8.5	Step-by-step: Adding a contact to the contact list.....	23
8.6	Step-by-step: Establishing an unencrypted connection	25
8.6.1	Connection establishment via the contact list.....	25
8.6.2	Connection establishment via the keypad	27
8.7	Step-by-step: Establishing an encrypted connection.....	28
8.7.1	Connection establishment via the contact list.....	28
8.7.2	Connection establishment via the keypad	31
8.8	Step-by-step: Answering a call	32
9	Appendix	35
A	Terms of use.....	35

10 Glossary 36

11 Index 37

1 Product-specific safety advices / additional notes

NOTICE

Emergency calls

The TopSec Phone app is not suitable for emergency calls. Please use your telephone for emergency calls.

NOTICE

Costs

The TopSec Phone app uses the data connection (packet data) of your computer. Hence, depending on the contract with your provider, additional costs can be incurred.

Very high roaming fees may occur in particular while abroad.

NOTICE

Tethering

The TopSec Phone app uses the data connection (packet data) of your computer for the VoIP communication. Depending on the contract with your provider, VoIP data and tethering respectively can be blocked for this connection. If so, the TopSec Phone app cannot be used. Please consult your provider about this.

For longer established contracts with Telekom, an adjustment of the existing contract may possibly be necessary.

NOTICE**SIP server utilization**

The use of a SIP server may have to be unlocked by your provider for VoIP telephony over SIP servers.

Please consult your provider about this.

NOTICE**Hardware requirements**

To use the TopSec Phone app, the computer must have speakers or headphones as well as a microphone installed and activated.

2 Documentation Overview

This documentation for the TopSec Phone for Windows PC app is available for download on the Rohde & Schwarz website (www.rohde-schwarz.com).

A PDF reader, e.g. Adobe Acrobat Reader (www.adobe.com) or FoxIt Reader (www.foxitsoftware.com), is required to view the documentation.

3 Conventions Used in the Documentation

The following conventions are used throughout the R&S TopSec Mobile Usermanual:

Typographical conventions

Convention	Description
"Graphical user interface elements"	All names of graphical user interface elements both on the screen and on the front and rear panels, such as dialog boxes, softkeys, menus, options, buttons etc., are enclosed by quotation marks.
"KEYS"	Key names are written in capital letters and enclosed by quotation marks.
<i>Input</i>	Input to be entered by the user is displayed in italics.
File names, commands, program code	File names, commands, coding samples and screen output are distinguished by their font.
"Links"	Links that you can click are displayed in blue font.
"References"	References to other parts of the documentation are enclosed by quotation marks.

4 Requirements

4.1 System requirements

The TopSec Phone application supports the Windows operating system in versions Windows 7 and Windows 8.

The operation of the app is possible over mobile data connections via GPRS, EDGE, UMTS, HSDPA as well as via LAN/WLAN. Over GPRS, problems with the plain call functionality can occur due to the low data rate.

For operation over mobile data connections, you have to ensure that you have an active data connection at your disposal. If your contract does not include a data connection, please consult your provider. Please consider the directions in your computer's user manual if necessary.

An active Bluetooth interface on the Windows PC is needed for the connection of the TopSec Mobile. TopSec Phone needs the Bluetooth SPP profile for its operation. Please find the information about which profiles of your Windows PC are supported by the Bluetooth interface in the manual of your Windows PC or directly contact the technical support of the manufacturer.

The application requires the Microsoft .NET software framework in version 4.5 and the Visual Studio 2012 Redistributable. The installation files for both are however provided alongside the one for TopSec Phone.

4.2 Operational requirements

For the VoIP communication, it is necessary to register to a VoIP server. The server assigns the connections between the individual users. Connections between different users can only be established if all users are registered at the same VoIP server, or if the servers are connected accordingly.

For the registration to the VoIP server, you need the registration details for your VoIP server. In the case of the VoIP server to be used being a company server, you will receive the information from the server administrator. In the case of a public server, you will receive your credentials in the course of the registration process from your provider.

The following data is needed:

- Server address (either IPv4 address or host name)
- Server port. For this field, default values are preset which you can find in the correspondent chapter. In case you should need settings differing from this, you have to request them from your administrator/provider.
- Registration details: User name, password
- For use of the IAX2 protocol: Only by using the Rohde & Schwarz VoIP proxy you can be called over IAX2 if you are using a mobile data connection.
- Caller ID/Own phone number: Your VoIP number

To use the app for encrypted communication, you have to pair your computer with your TopSec Mobile. The pairing has to be initiated on the TopSec Mobile. The procedure is described in section [Pairing with the TopSec Mobile](#)

5 Icons and terms

In this user manual the following icons and notations are used:

Icon	Icon/Label	Denotation
---	Warning	A warning which only exhibits an OK button merely signifies a hint. It does not provoke any change in the program execution. By clicking on OK, you can confirm the warning so it will not be shown any longer. \\
	Launcher-icon	Icon via which the app is called.
---	Settings	With this menu item the settings of the app are invoked. Here you can define server settings as well as ring tones.
---	Overview	With this menu item you can reach the call list and the favorite list.
---	Contacts	With this menu item the contact list is invoked.
---	Keypad	With this menu item the keypad for manual call placement is invoked.
	Button "Crypto call"	With this button you can start an encrypted call.
	Button "Plain call"	With this button you can start an unencrypted call.
	Button "Delete"	With this button you can correct erroneous input.
	Status Green	The status icons are displayed at the top right of the app. In case of status Green unencrypted as well as encrypted calls can be placed.
	Status Yellow	In status Yellow solely unencrypted calls are possible.
	Status Red	In status Red no telephony is possible at all.

6 Installation

The program is provided in the form of the installation file

`TopSec_Phone_Windows_[version number]_install.exe` It launches an assistant which guides you through the installation.

There you can choose the destination directory whereupon all necessary files are copied and shortcuts in the Start menu under "All Programs" > "TopSec Phone" as well as on the desktop are created.

6.1 Functional tests

On every start of the application, the prerequisites are checked for the encrypted/unencrypted connection with the app and the TopSec Mobile device respectively. If one or more conditions are not fulfilled, a corresponding error message is displayed.

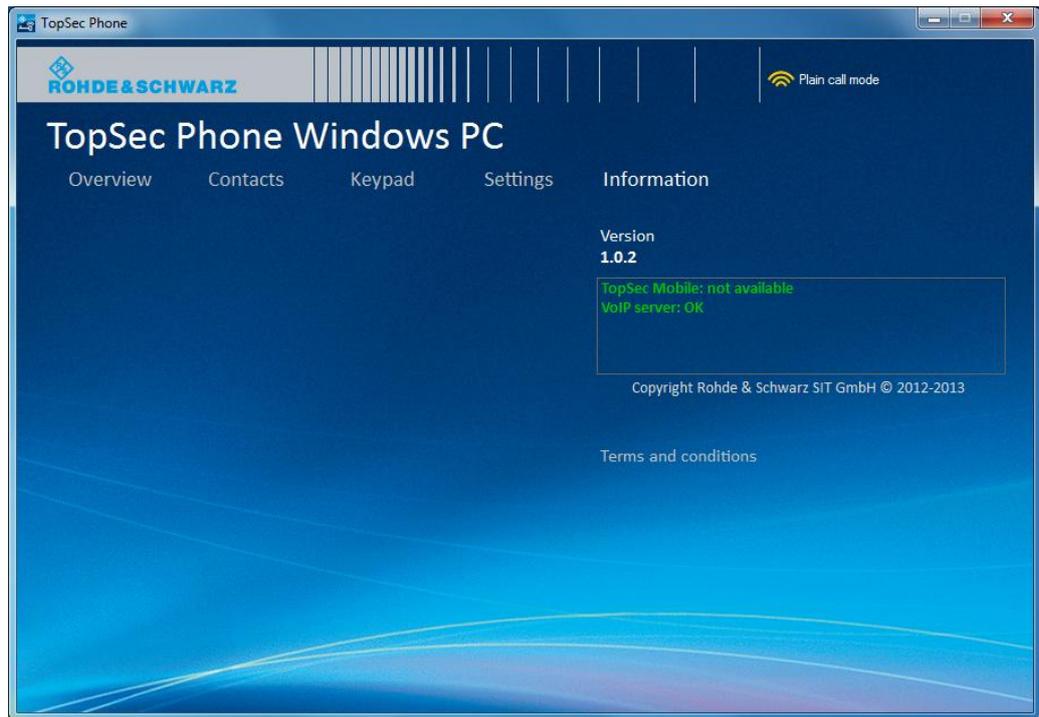
The following tests are conducted during the start process:

- Established internet connection
- Successful registration at the server
- Pairing between TopSec Mobile device and computer
- Bluetooth activated
- Established Bluetooth connection between TopSec Mobile device and computer

For the server registration, the user name and password are sent to the server. In case you are using a server which does not need a password you can leave this field empty.

Situation	Status	Possible actions
All checks successful and all conditions fulfilled	Green	Encrypted call are possible. Both call buttons are active.
Bluetooth® not activated	Yellow	Only unencrypted calls are possible. Only the button for unencrypted calls is active.
No pairing between TopSec Mobile and computer		
No connection between TopSec Mobile and computer		
Missing internet connection	Red	There is no connection to the server or the internet. There are no calls possible. Both call buttons are inactive.
No connection to the server, e.g. because of invalid registration		

The status of the app is displayed on the overview page in the configuration area.



NOTICE

Background mode for mobile devices

To be always available for encrypted calls, the app must run in the background constantly and stay connected with the server. For this purpose, the option "Registration via VoIP proxy" must be active.

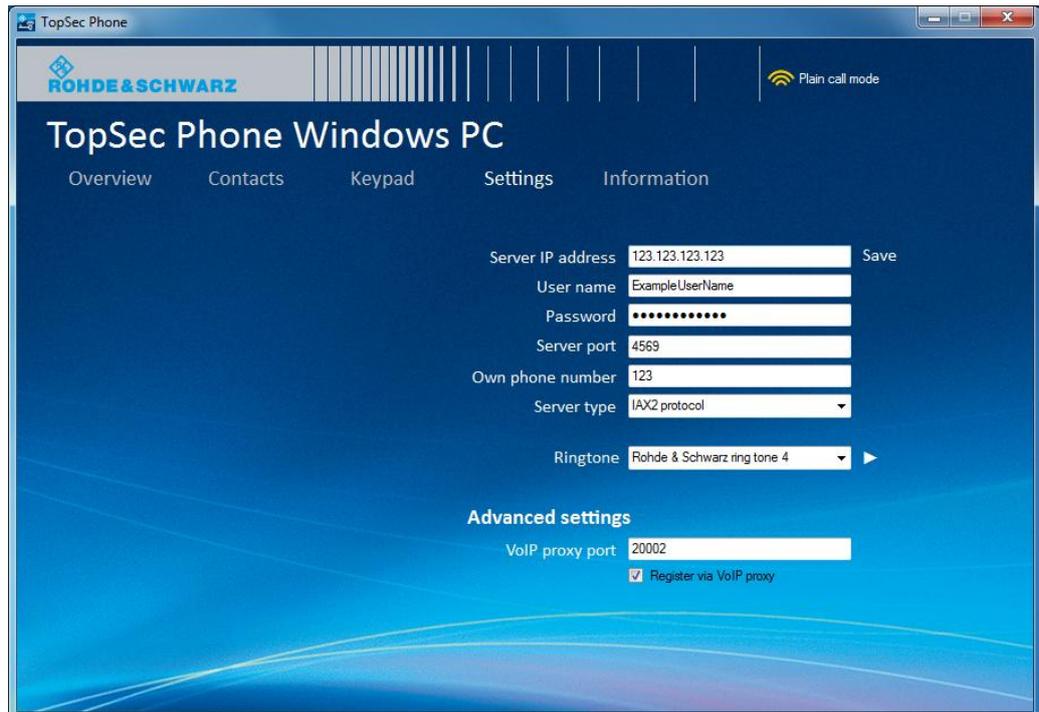
Furthermore, the use of the TCP VoIP proxy extends the standby time as larger registration intervals are employed.

7 Configuration and setup

The configuration is located under the menu item "Settings".

Here you can enter all server-related information, your own phone number as well as the desired server protocol.

Moreover, you can set your ring tone here. With a click on the play icon beside the field "Ring tone", you can listen to the ring tones which are available.



NOTICE

Language

The app uses the language of the operating system by default. If the language of your operating system is not supported by the app, English will be used.

7.1 VoIP server

In the field "Server IP address" you can either enter the IPv4 address or the host name.

To allow your VoIP number to be transmitted, enter it in the field "Own phone number".

Enter your user name and your password as well as the server port.

In the field "Server type" you can choose between an IAX2 and a SIP server. Here you define whether you are calling over the IAX or the SIP protocol.

The check box "Registration via VoIP proxy" under "Advanced settings" defines if a proxy will be used for the VoIP connection, see the above hint "Background mode for mobile devices".

Field	Default value	Range
"VoIP proxy port"	-	0 - 65535
"Registration via VoIP proxy"	OFF	ON/OFF

NOTICE

Public VoIP servers

Most of the public servers do not support the IAX protocol. Hence it is recommended to use the SIP protocol in the case of public VoIP servers.

NOTICE

Please check if the connection to the VoIP server cannot be established

If the connection to the VoIP server cannot be established, try to establish an internet connection with the web browser. If it does not succeed either, this implies that there is generally no connection to the internet. If however a connection to the internet can be established, please verify the entered name and password.

7.2 Pairing with the TopSec Mobile

Before you can use the TopSec Phone application for encrypted calls, it has to be paired over Bluetooth with the TopSec Mobile device.

The prerequisite for this is the Bluetooth antenna of your Windows PC being activated and devices being allowed in the system's Bluetooth settings to find the computer. Please learn more detailed information about these procedures from the correspondent manuals of your PC and operating system.

As soon as these preparations have been made, start the application and turn on the TopSec Mobile. Choose "Settings" > "Bluetooth" > "BT Inquiry" from the menu of the device and wait until a list of found devices will be displayed. Browse through these

until the name of your Windows PC appears with "SPP" among the profiles and confirm.

You can adapt the then displayed PIN as it suits your needs and confirm again whereupon a notification about the pairing attempt should appear in Windows. Allow this by clicking on the notification and entering the PIN shown on the TopSec Mobile.

In case an error occurred during this procedure, e.g. because a confirmation happened too late, it is advisable to remove the respective other device on the Windows PC and the TopSec Mobile from the list of paired devices before a new attempt is made.

8 Usage

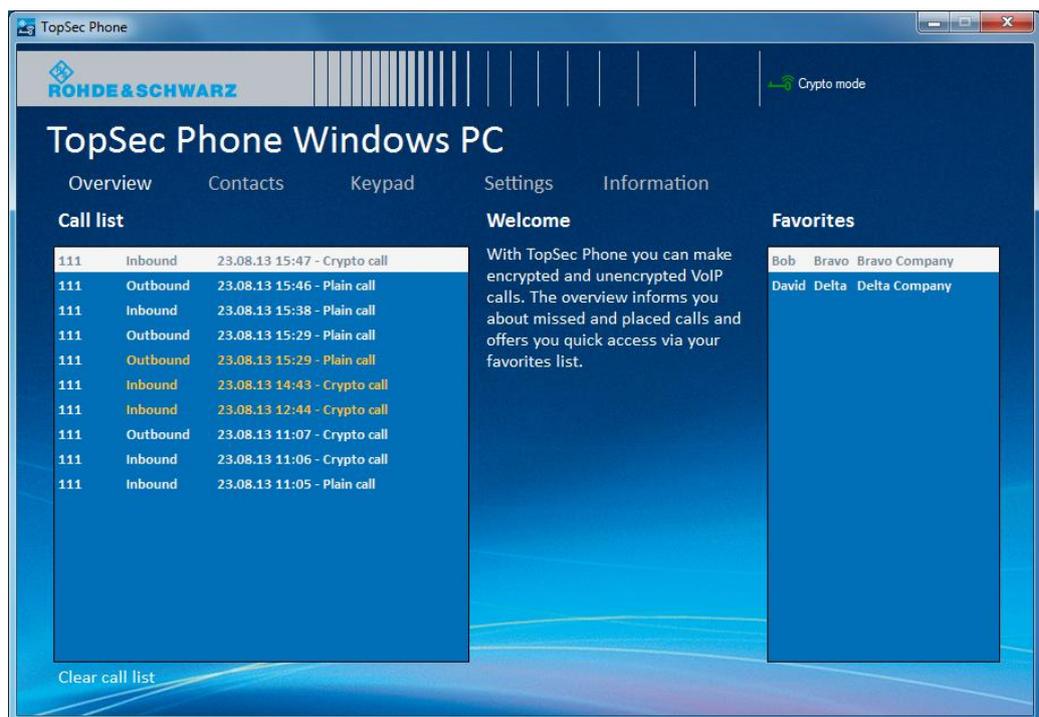
8.1 Starting the app

After the installation, the app can be started out of the Start menu via "All Programs" > "TopSec Phone" > "TopSec Phone" or via the desktop shortcut.

Alternatively, it is possible to directly execute the target file of the shortcut, TopSecPhone.exe, in the installation directory.

8.2 Overview

By selecting the menu item "Overview", you can access the call list as well as all contacts which you have set as favorites. Adding a contact to the favorite list or removing from it can be performed in the menu for contact edition.



You can place a call by double-clicking a contact both in the call list and the favorite list.

In the call list, missed calls are shown in orange font while answered calls appear in white font.

8.3 Contacts

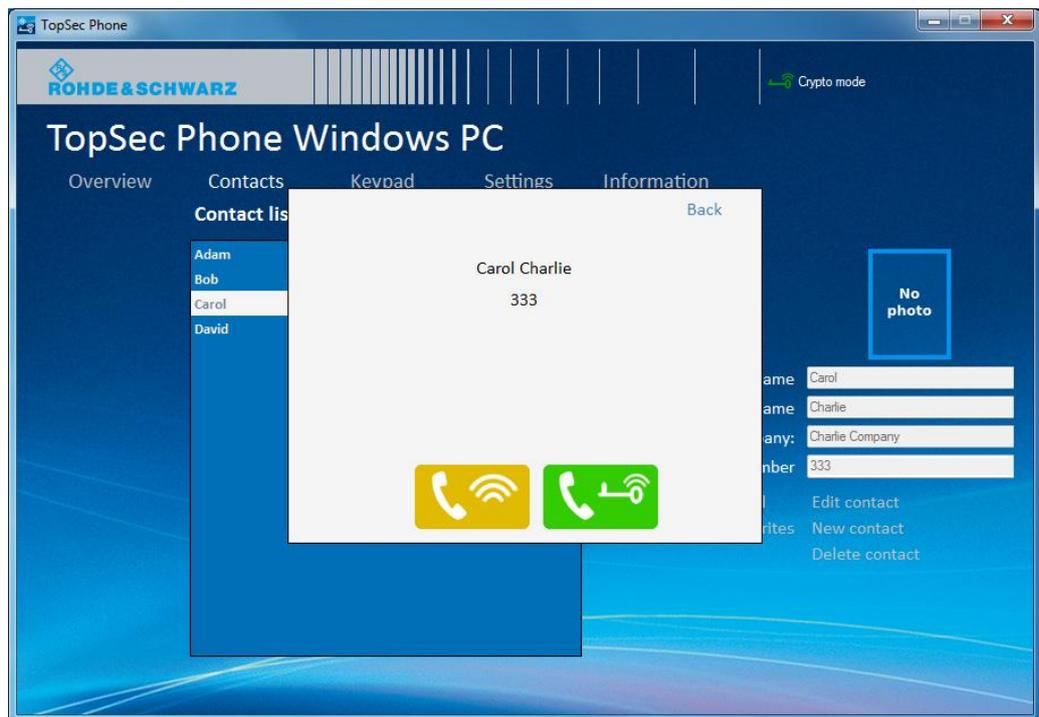
With the menu item "Contacts" you can reach the list of all contacts. Select the desired contact here.



8.3.1 Calling a contact

By single-clicking a name in the contact list, the contact details will be displayed on the right side. In this way, the contact can be edited or called.

By double-clicking the name or by clicking on the button "Call" you will attain to a screen where the call mode can be chosen.



On this screen, you will see the name and the number of the contact that you are about to call.

With a click on one of the two call buttons you determine whether an encrypted or unencrypted call will be placed.



Encrypted / Crypto call

Unencrypted / Plain call

The color of the buttons corresponds to the status of the app. In case of a yellow status, i.e. only unencrypted calls are possible, the green button for encrypted call is inactive (i.e. grayed out).

See the table in chapter [Functional tests](#).

Enter optional tip heading or delete this field



Whenever you call a contact, after having chosen a phone number, you will reach the screen for choosing the call mode where you determine whether an encrypted or unencrypted call will be placed.

The only exception to this is the manual dialing of a number on the keypad because here the call mode is defined by selecting the correspondent button.

NOTICE**Changing the call mode after call initiation**

If you initiated an encrypted call, you cannot change it to an unencrypted call anymore. If you do not accept the call on your TopSec Mobile, the connection will be cancelled.

In case of an incoming call, you can answer in plain call mode a call which has been initiated as encrypted. In this case, answer the call on your computer.

8.3.2 Managing contacts

By clicking on the button "Edit contact", you will switch to the editing mode where you can edit the selected contact data including the photo. The label of the button will change to "Save" and next to it "Cancel" will appear. With both buttons the edit mode will be left. A click on a main menu item discards any changes just as "Cancel".

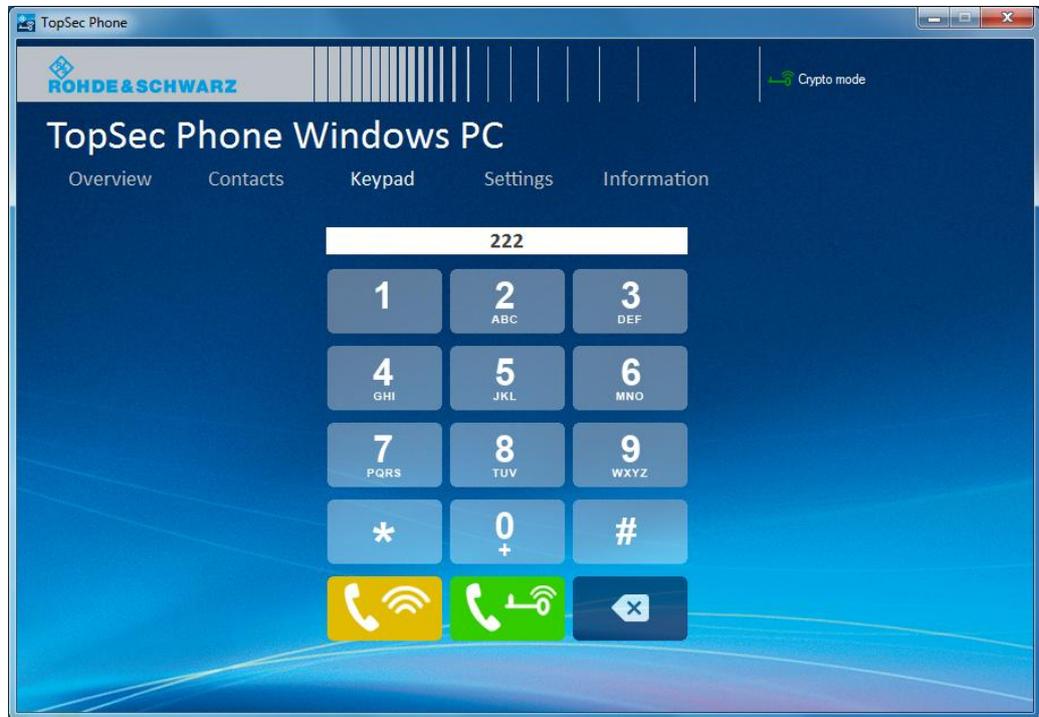
The button "New contact" behaves similarly, with the only difference that the input fields have to be filled and that "Save" does not change an existing contact but creates a new one.

At last, there is the possibility to remove the created contacts via "Delete contact". Please bear in mind that there is no confirmation prompt.



8.4 Manual dialing via the keypad

With the menu item "Keypad" you can manually enter a number and place an encrypted call as well as an unencrypted one.



Encrypted / Crypto call



Unencrypted / Plain call

The color of the buttons corresponds to the status of the app. In case of a yellow status, i.e. only unencrypted calls are possible, the green button for encrypted call is inactive (i.e. grayed out).

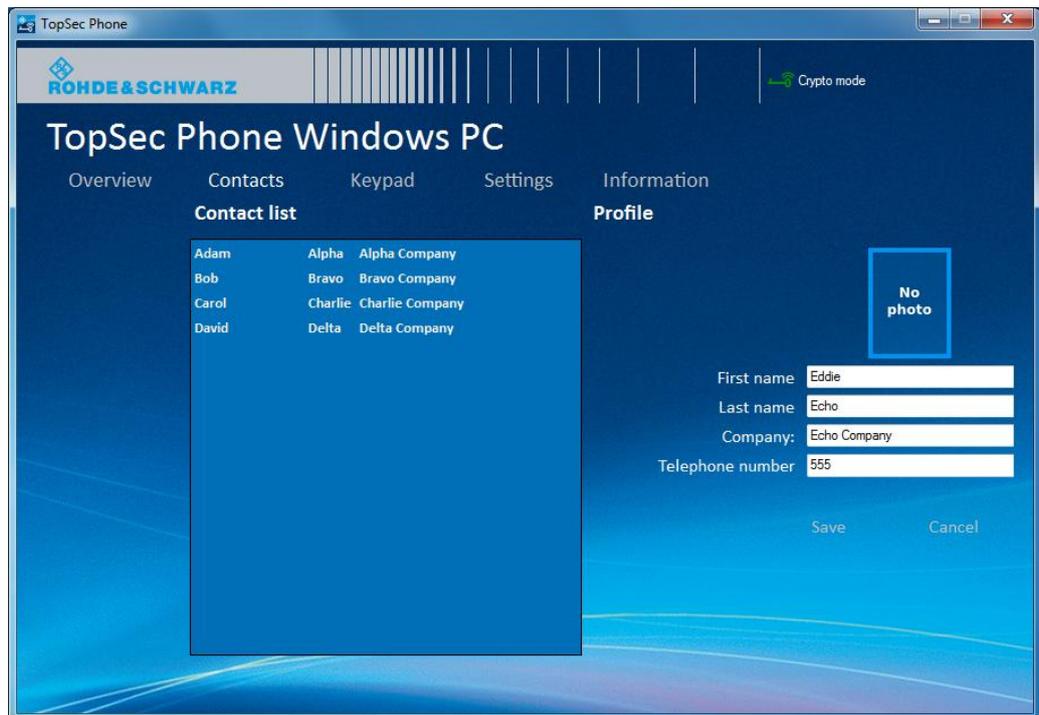
See the table in chapter [Functional tests](#).

8.5 Step-by-step: Adding a contact to the contact list

1. Select the menu item "Contacts", then the button "New contact".



2. Enter the data of the contact to be created into the input fields.



3. By clicking the picture place holder you can choose a photo.
4. Click on the button "Save" to finish the procedure.

Enter optional tip heading or delete this field



Your TopSec contacts are kept in a separate phone book inside the app. This means that changes which you make in the app will not be taken over to the standard phone book of the computer.

Additionally, there is no connection between a potentially existing phone book in your TopSec Mobile and the phone book of the app.

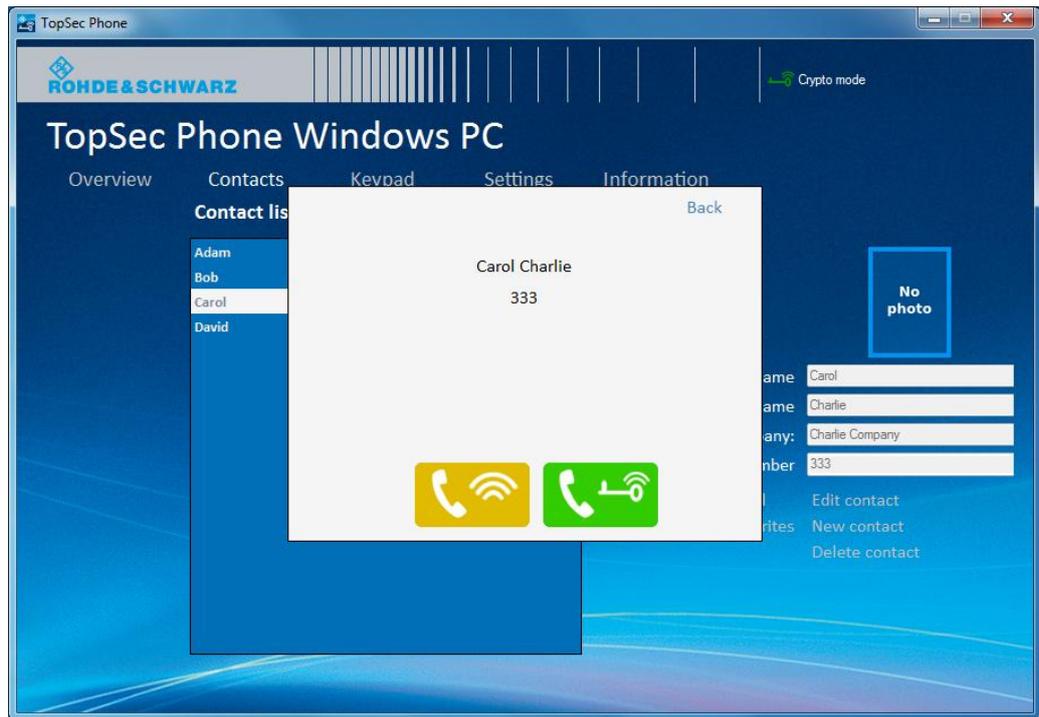
8.6 Step-by-step: Establishing an unencrypted connection

8.6.1 Connection establishment via the contact list

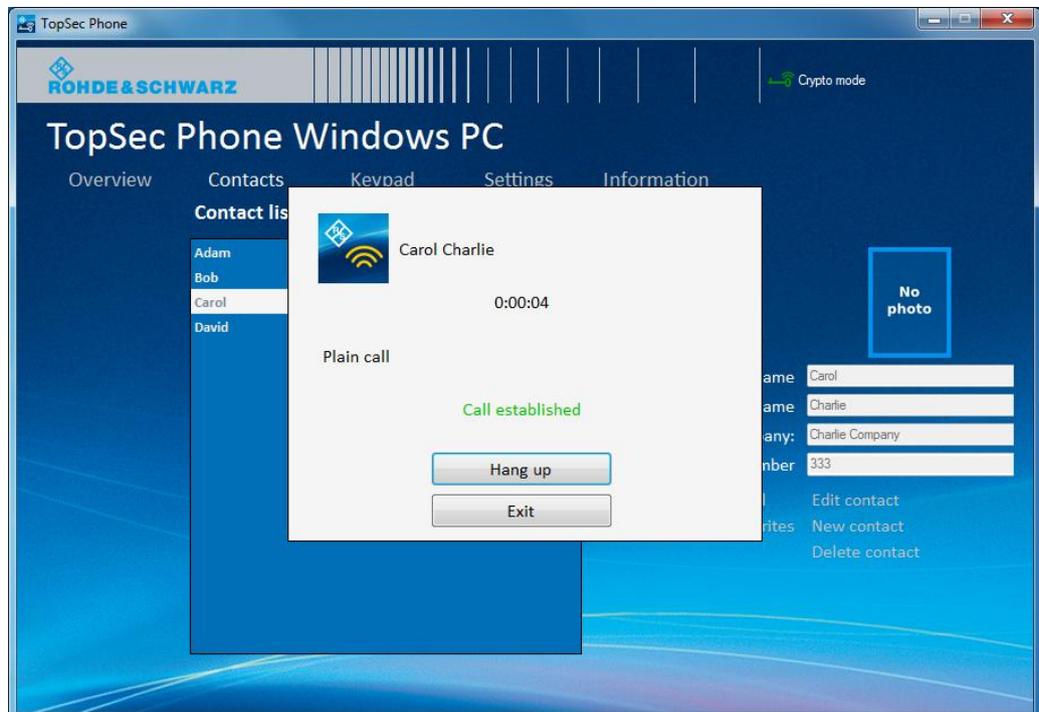
1. Select the menu item "Contacts". You will reach the contact list.



2. Select the desired contact by double-clicking its name. A dialog opens where you can choose the call mode.



3. Now select "Plain call" as call mode by clicking on the button "Plain call" .
4. The application now begins to establish a VoIP connection to the callee. In case the other party answers the call, the connection will be established.



5. The following screen displays the callee by means of his VoIP number or the associated name from the contact list. Furthermore, you can see the call mode and the duration of the call.
6. Terminate the call via the button "Hang up".

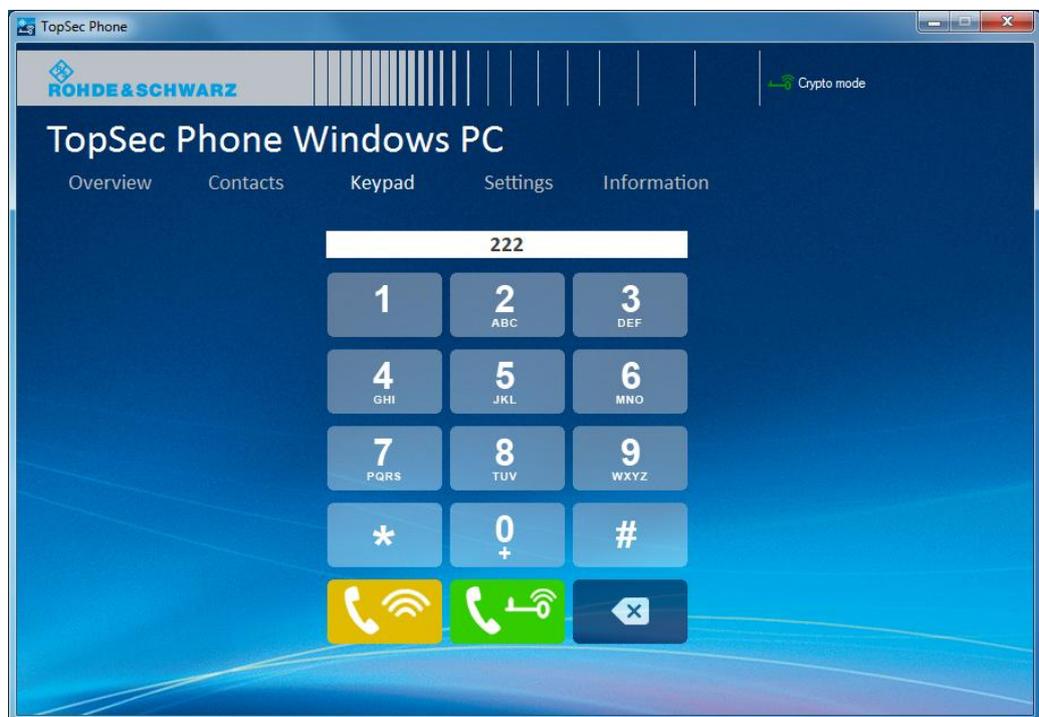


Enter optional tip heading or delete this field

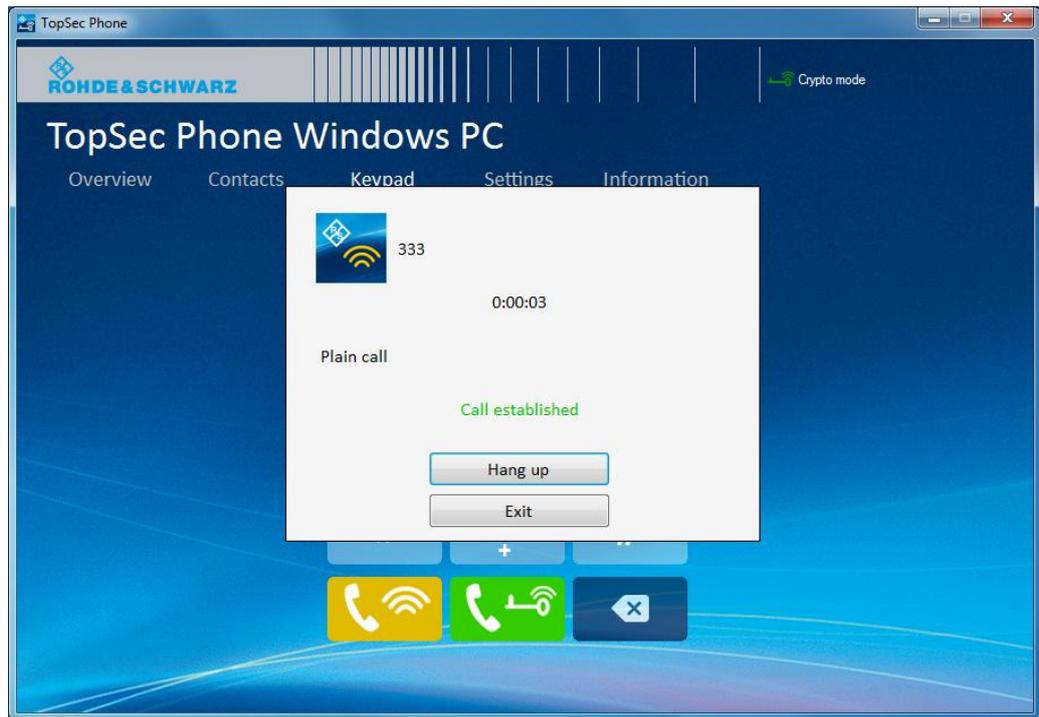
In the case of an unencrypted call, the TopSec Mobile is not needed.

8.6.2 Connection establishment via the keypad

1. Select the menu item "Keypad".



2. Enter the desired number with the help of the keyboard.
3. Now select "Plain call" as call mode by clicking on the button "Plain call" .
4. The application now begins to establish a VoIP connection to the callee. In case the other party answers the call, the connection will be established.
5. The following screen displays the callee by means of his VoIP number or the associated name from the contact list. Furthermore, you can see the call mode and the duration of the call.



6. Terminate the call via the button "Hang up".



Enter optional tip heading or delete this field

In the case of an unencrypted call, the TopSec Mobile is not needed.

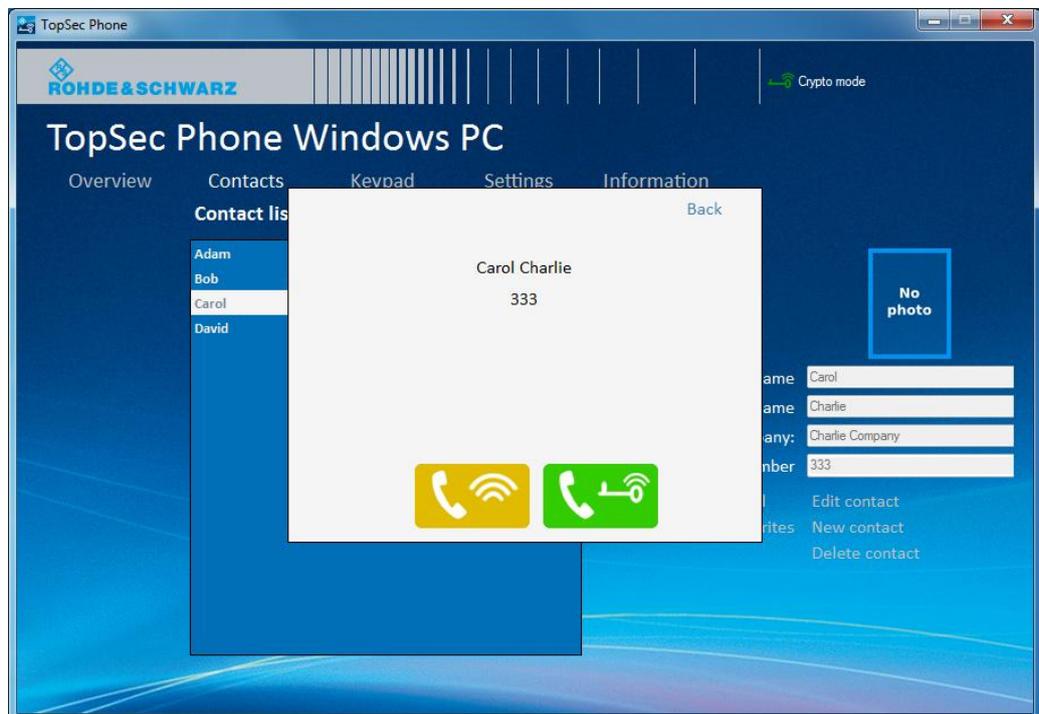
8.7 Step-by-step: Establishing an encrypted connection

8.7.1 Connection establishment via the contact list

1. Select the menu item "Contacts". You will reach the contact list.

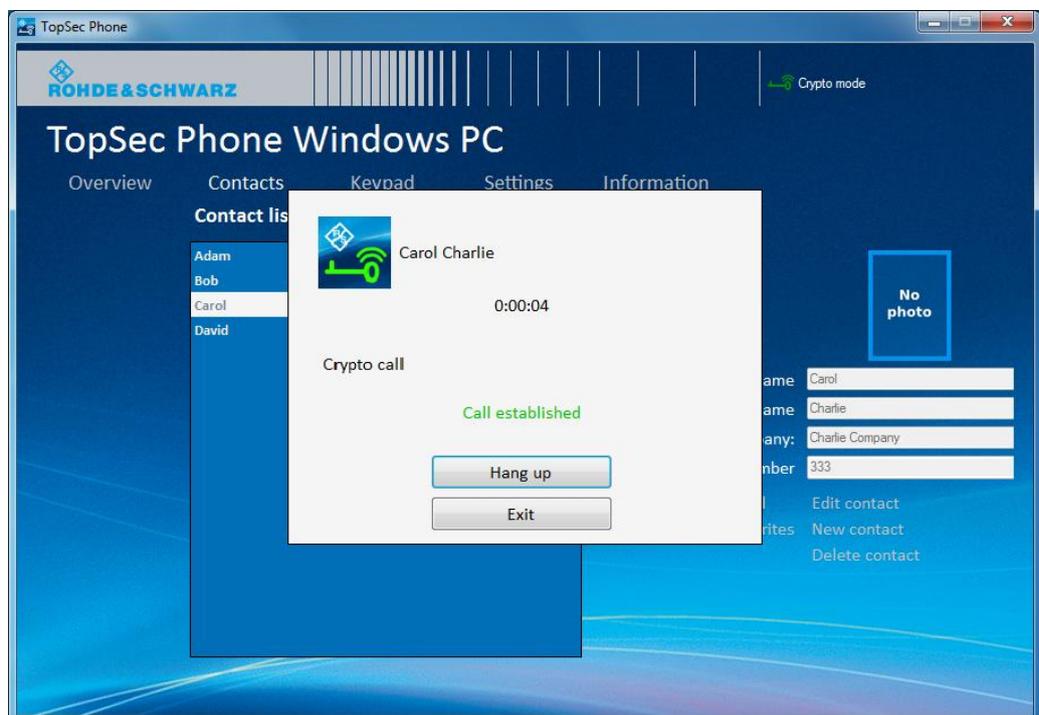


2. Select the desired contact by double-clicking its name. A dialog opens where you can choose the call mode.



3. Select the "Crypto call" button  to initiate an encrypted call.

4. Your computer now begins to establish a VoIP connection to the callee over the TopSec Mobile. In case the other party answers the call, the connection will be established.
5. If the callee answers the call in crypto mode (i.e. he answers the call on the TopSec Mobile), your TopSec Mobile will ring and you have to answer the call on it to establish an encrypted connection.
6. If the callee answers the call in plain mode (i.e. he answers the call on his smartphone or his computer), only your computer will ring and you can only make an unencrypted call.
7. If the call is established, the following screen appears. It displays the callee by means of his VoIP number or the associated name from the contact list. Furthermore, you can see the call mode and the duration of the call.



8. In the case of a crypto call, you can terminate it on your computer or your TopSec Mobile. In the case of a plain call, you can terminate it on your computer by clicking the button "Hang up."

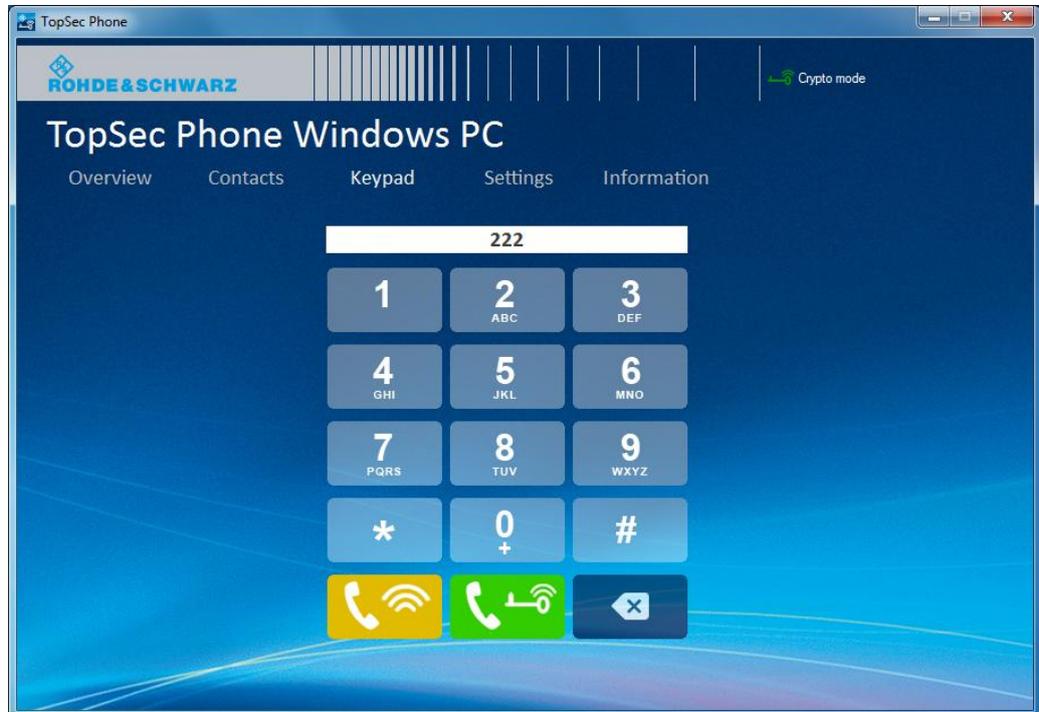
NOTICE

Changing the call mode after call initiation

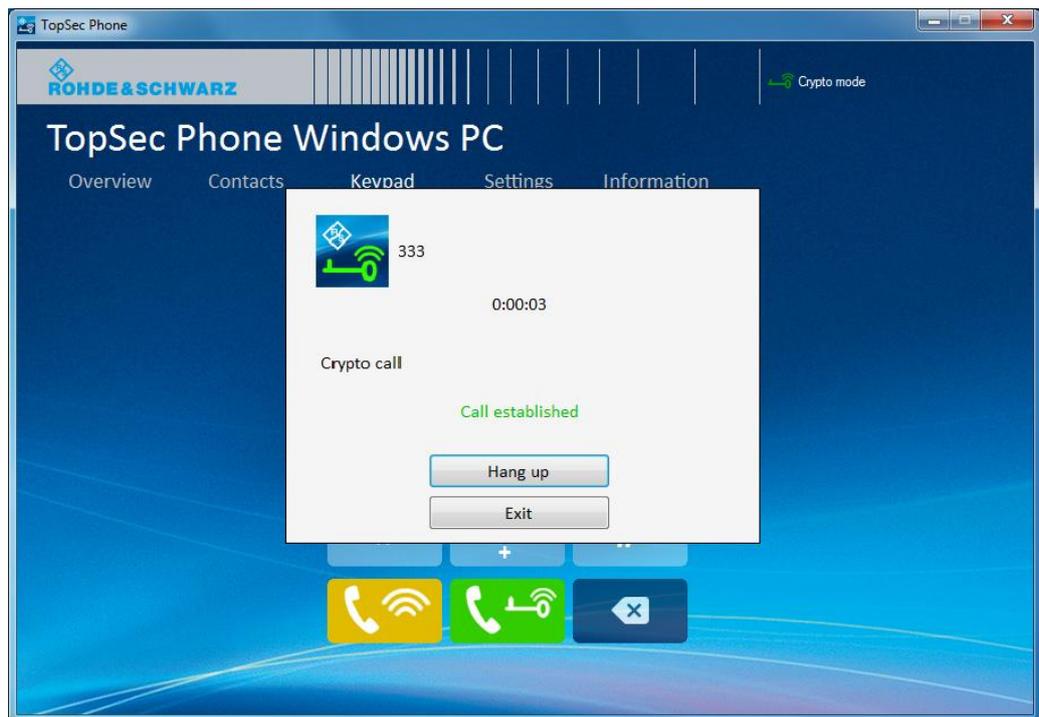
If you initiated an encrypted call, you cannot change it to an unencrypted call anymore. If you do not accept the call on your TopSec Mobile, the connection will be cancelled.

8.7.2 Connection establishment via the keypad

1. Select the menu item "Keypad".



2. Enter the desired number with the help of the keyboard.
3. Select the "Crypto call" button  to initiate an encrypted call.
4. Your computer now begins to establish a VoIP connection to the callee over the TopSec Mobile. In case the other party answers the call, the connection will be established.
5. If the callee answers the call in crypto mode (i.e. he answers the call on the TopSec Mobile), your TopSec Mobile will ring and you have to answer the call on it to establish an encrypted connection.
6. If the callee answers the call in plain mode (i.e. he answers the call on his smartphone or his computer), only your computer will ring and you can only make an unencrypted call.
7. If the call is established, the following screen appears. It displays the callee by means of his VoIP number or the associated name from the contact list. Furthermore, you can see the call mode and the duration of the call.



8. In the case of a crypto call, you can terminate it on your computer or your TopSec Mobile. In the case of a plain call, you can terminate it on your computer by clicking the button "Hang up".

NOTICE

Changing the call mode after call initiation

If you initiated an encrypted call, you cannot change it to an unencrypted call anymore. If you do not accept the call on your TopSec Mobile, the connection will be cancelled.

8.8 Step-by-step: Answering a call

1. During an incoming call your computer (plain call) or your TopSec Mobile (crypto call) rings, depending on the call mode. In addition, your computer displays the call as well as the call mode.
2. In the case of a crypto call, you have to answer it on the TopSec Mobile to make an encrypted call. If you answer the call on your computer instead, an unencrypted connection will be established.
3. In the case of a plain call, you can answer it only on the computer.
4. If you do not want to answer the call, reject it with the button "Hang up".

5. If the call is established, the following screen appears. It displays the callee by means of his VoIP number or the associated name from the contact list. Furthermore, you can see the call mode and the duration of the call.



6. In the case of a crypto call, you can terminate it on your computer or your TopSec Mobile. In the case of a plain call, you can terminate it on your computer by clicking the button "Hang up".

NOTICE

Reminder

Only your computer can answer a call in plain mode; plain calls cannot be made on the TopSec Mobile.

Encrypted calls are only possible on the TopSec Mobile.

9 Appendix

A Terms of use



Terms and Conditions for royalty-free Products

Issued June 8, 2010 (PF 0095.9046.00 V01.01)

LEGAL NOTICE: PLEASE READ THESE TERMS AND CONDITIONS BEFORE DOWNLOADING, INSTALLING OR OTHERWISE USING THE ROYALTY-FREE SOFTWARE PROGRAMMS, BETA RELEASE PROGRAMMS, INFORMATION, METHOD DESCRIPTIONS, PICTURES, GRAPHS, INTERFACES, DATABASES AND OTHER CONTENTS PROVIDED BY ROHDE & SCHWARZ GMBH & CO. KG (HEREINAFTER REFERRED TO AS "PRODUCT" OR "PRODUCTS"). ALL USE OF THE PRODUCT IS SUBJECT TO THE TERMS AND CONDITIONS SET FORTH BELOW (HEREINAFTER REFERRED TO AS "TERMS AND CONDITIONS").

TO INSTALL THE PRODUCT, THE USER MUST FIRST AGREE TO THE TERMS AND CONDITIONS. NOTWITHSTANDING ANYTHING TO THE CONTRARY IN THESE TERMS AND CONDITIONS, INSTALLING OR OTHERWISE USING ANY OF THE PRODUCT INDICATES THE USER'S ACCEPTANCE OF THESE TERMS AND CONDITIONS.

Scope of these TERMS AND CONDITIONS

The User shall be entitled to view and download the PRODUCT including enhancements and documentations if any. The use of the PRODUCT shall be free of charge. The right to use the PRODUCT requires the prior acceptance of these TERMS AND CONDITIONS.

If and to the extent the PRODUCT is provided to the User by ROHDE & SCHWARZ GmbH & Co. KG (hereinafter referred to as "R&S") in order to fulfil R&S' warranty or non gratuitous maintenance obligations under any other already existing agreement with the User, the use of the PRODUCT shall be governed by such other agreement.

Grant of License

R&S grants to the User a non-exclusive, non-transferable, royalty free, perpetual right to use the PRODUCT for the sole purpose for which it is intended and provided by R&S.

The license granted hereunder is limited to R&S and R&S licensors' intellectual property rights in the PRODUCT. R&S reserves all rights not expressly granted hereunder to the User.

Restrictions

The User shall not (i) copy the PRODUCT except for archival purposes or unless it is essentially required for its authorized use, (ii) modify, adapt or create derivative works of the PRODUCT or disable any of its features, (iii) remove, alter or obscure any product identification, copyright or other intellectual property notices embedded within or on the PRODUCT, or (iv) publish, disclose, sell, rent, lease, lend, distribute, make available online, sublicense or provide the PRODUCT to any third party without R&S' prior written consent. The User shall not decompile, disassemble or reverse engineer the PRODUCT unless stipulated otherwise by mandatory law.

Third Party Product / Open Source Software

To the extent that the PRODUCT is provided to the User for which R&S has only derived rights to use (Third Party Product), the above Sections "Grant of License" and "Restrictions" shall – also concerning the relationship between R&S and the User – be amended and superseded by the conditions of use agreed between R&S and its licensor. To the extent that the User is provided with Open Source Software, the provisions of the above Sections "Grant of License" and "Restrictions" shall be amended and superseded by the conditions of use of the according Open Source Software. Upon request, R&S shall provide the User with the source code if the provision of the source code has been agreed in the conditions of use of the Open Source Software licence. R&S shall point out in the contract documents or in any other appropriate document if Third Party Products (including, but not limited to Open Source Software) and pertaining conditions of use exist and shall make the conditions of use available if so requested by the User. Any breach of the conditions of use on the part of the User shall entitle not only R&S, but also its licensor, to assert claims and rights arising there from in their own name.

Copyright

R&S is and will remain the sole owner of all right, title and interest, including all intellectual property rights, in and to the PRODUCT, and all modifications, enhancements, updates, upgrades and derivative works thereof made by R&S. The User shall not copy the written materials accompanying the PRODUCT. The User must reproduce all copyright notices in the original PRODUCT on all permitted copies.

Limitation of Warranty

The PRODUCT shall be made available to the User free of charge. R&S shall in particular make no warranty or representation that any PRODUCT will meet the User's expectations, requirements or works in combination with any hardware or applications software provided by third parties, that the operation of the PRODUCT will be uninterrupted or error-free, or that any defects in any PRODUCT will be corrected. Furthermore, R&S shall make no warranty that the PRODUCT is free from any third-party rights. The afore-mentioned exclusion of warranty shall not apply if and to the extent R&S fraudulently conceals a defect of title or material defect of the PRODUCT, in which case R&S shall be obliged to indemnify the User for damages resulting there from.

Product Support

R&S offers a limited support for the PRODUCT at its sole discretion on voluntary basis and reserves the right to update the contents of the PRODUCT and its associated programs, files, documentation and/or other elements.

Liability

R&S shall only be liable in case of intent and gross negligence. This limitation shall not apply in case of injuries of life, body or health. Mandatory liability pursuant to product liability law shall remain unaffected.

Consequential Damages

In no event shall R&S be liable for (i) any indirect, consequential or economic damages, and (ii) loss of profit, risk/replacement purchase, interruption of business, loss of production, contractual claims of third parties, loss of data due to a software error and loss of interest.

Revocation

R&S may revoke the License upon notice for failure of the User to comply with any of these TERMS AND CONDITIONS. Upon revocation, the User shall immediately stop the use and immediately return or destroy the PRODUCT, together with all copies, adaptations and merged portions in any form. In case of destruction the User shall prove such destruction if requested by R&S.

Applicable Law / Place of Jurisdiction

These TERMS AND CONDITIONS and the contractual relationship between the User and R&S shall be governed by German law, excluding the provisions on conflict of laws. The application of the UN Convention on Contracts for the International Sale of Goods (CISG) shall be excluded.

The courts of Munich shall have exclusive jurisdiction in case of any disputes arising directly or indirectly from the contractual relationship, provided that the User is a businessman, a body corporate, a legal entity under public law, or a special fund under public law. R&S shall also have the right to take legal actions at the User's domicile.

Miscellaneous

If any provision of these TERMS AND CONDITIONS are held invalid, the offending clause will be modified so as to be enforceable and, as modified, shall be fully enforced, and the remainder of these TERMS AND CONDITIONS will continue in full force and effect.

ROHDE & SCHWARZ GmbH & Co. KG, Muehldorferstr. 15, 81671 Munich, Germany

10 Glossary

T D

DNS: Domain Name System

I

IAX: InterAsterisk Exchange

IAX2: InterAsterisk Exchange protocol in version 2

IPv4-Adresse: IPv4 is the Internet Protocol version 4. The addressing over IPv4 is used in packet-oriented networks. IPv4 addresses are written in decimal in four blocks, e.g. 207.142.131.235.

P

PAN: [PAN] Personal area network. A profile for transmission of network connections via Bluetooth®.

S

SIP: Session Initiation Protocol; protocol for localization of users and for establishment and termination of connections

T

TCP: Transmission Control Protocol

Tethering: Connection of a smartphone with a PC, PDA or another end device to enable an internet connection over GSM/UMTS for it. The mobile phone thereby assumes the role of a modem.

V

VoIP: Voice over IP

11 Index

Configuration	16	Keypad	20
Contacts	18	Language	16
Conventions.....	6, 9	Pairing	17
Costs	5	SIP server.....	6
Emergency calls	5	Tethering	5
Icons.....	13	Usage.....	18
Installation	14		