SecureScrypt

User's Manual (Generic Version)

SecureScrypt/Enigma® Client

Client for Mobile Phones / Android (2.3 or later),IOS, Blackberry, Windows, Nokia, Symbian .

SecureScrypt-Neoi TEC Systems– A brief Profile

Since well over 20 years SecureScrypt-Neoi TEC Systemsbelongs to the leading manufacturers of communication solutions in mobile applications, Hardware. We offer location independent, reliable and highly secure data communications for business environments. Enigma Soft- and Hardware is the SecureScrypt-Neoi TEC Systems offering for branch and application independent remote access to corporate networks that enable optimized business process modeling and integration and migration to new value-added services.

The comprehensive solutions and systems competence is provided for the benefit of our customers. Versatile cooperations with numerous partners (Swissbit, Neoi Technology, Aplus Technology) help our customers to enhance their value chains and address new growing target markets. As a technology leader SecureScrypt/Neoi TEC is active in research and development in order to develop new areas of technology applications and Hardware.

SecureScrypt-Neoi TEC Systems presents and understands itself to be your integral and single point of contact in IT questions – from conceptual development to sustainable operations. Success stories from project developments and general contractor ship in large-scale enterprises that comprise more than 10.000 installations worldwide over the past 20+ years, prove the expertise of SecureScrypt-Neoi TEC Systems in mobile and secure communications. References can be found in Credit Suisse, United Nations , Siemens, Huawei, Nokia, Motorola , to name only a few.

Copyright

Use of third-party products

The development of SecureScrypt/Enigma integrates the following third-party products:
Nokia QT (Shared Library),
Openssl (Shared Library),
OpenCode AMR audio codec, Version 0.1.2, http://sourceforge.net/projects/opencore-amr/

Application

Encrypted voice, Message , Video Call communications (focus: wireless networks)
1:1 calls and mobile conference calls (arbitrary number of participants)

Principles

VoIP based on UDP (connectionless)
State-of-the-art encryption mechanisms
No draw-backs in system integration and use of standard phone features
e.g. phone book / contacts, concurrent operation with other
applications, common phone calls (not encrypted)

Handling

Intuitive graphical user interface and use of the standard function keys
Automatic connection establishment

Supported Networks

Mobile: WiFi, UMTS, EDGE, GPRS
Fixed line: LAN (where suitable)

System Requirements - Operating Systems / Platforms / Memory:

Client: Symbian 9.2, 9.3 and 9.4 – 2.1 MB for installation;
Windows Mobile 6.x – 14,0 MB for installation;
Apple iPhone, iPad, iPod 3G – 4,0 MB for installation;
Android 2.3;
Microsoft Windows XP, Vista, 7 – 5,0 MB for installation
Linux, MacOS.
Server: Linux SuSe, RedHat and other Linux derivates (kernel 2.4 or
higher); Unix: FreeBSD
Windows server systems: Windows 2000 or later (on demand)
Available disk space > 5 MB, Minimum 256 MB RAM
Internet connection with fix IP address

Secure Data Transmission

Key exchange: Diffie-Hellmann 1024-4096 Bit

User data encryption: AES 256 Bit
Secured end-to-end connectivity (man-in-the-middle prevention)
Authentication: IMEI, verbal feedback of individual session fingerprints)
Centralized session management
Dynamic access control at the routing server

Voice Quality

Realtime full-duplex voice data transmission
Audio Codec: AMR-NB 12.2 kbps
Experience in voice quality: very good, like in standard mobile calls

Server Functionality

Centralized management overcomes insufficient mobile device ressources
Routing and session management
License management and logging

Scalability

Automatic choice and connect to the best-performing server

Scalability of the number of servers for voice quality optimization

- In 2008 Tino Gendrullis, Ruhr-University Bremen (Germany) has finished his thesis “Hardware-based crypto analysis of the GSM A5/1 Encryption” and he managed to break the encryption with a dedicated hardware and the knowledge of just a very few clear text information pieces. And the whole intrusion did not take him longer than 6 hours.
- The legal definition of what is considered “electronic surveillance” has changed or is about to do so. The new law allows US government to eavesdrop on conversations without warrants as long as the target of the government’s surveillance is “reasonably believed” to be overseas.
- Telecom Italia in 2006 was in the middle of a huge scandal regarding the illegal wiretapping and surveillance of the telephone networks. An entire system called “Radar” was capable of recording sensitive information about millions of Italians.
- Already way back in 2007 members of the hacker group THC worked on a „GSM Software Project“ that should enable to decrypt a tapped calls on GSM within a maximum of 2 hours – not on the fly, but afterwards.
- Messages that just popped up on T-Mobile and German Rail (DB AG) and police tracking of individuals show that already tracking of connection data can be quite dangerous (such tracking could be prevented in using a privately controlled gateway server with VoIP)

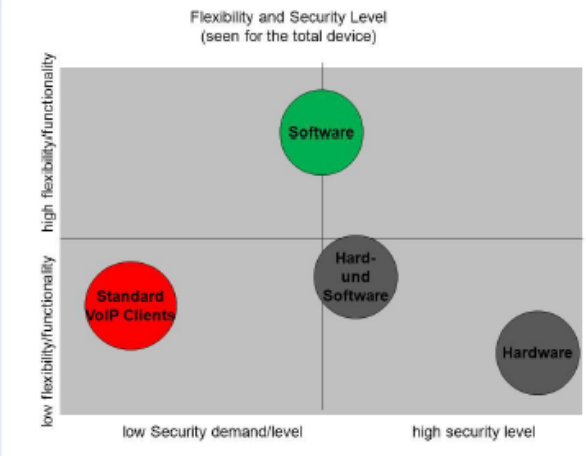
- GSM calls (encryption according to A 5/1 and A 5/2 standard) can be decrypted using a usual standard PC (was already possible in year 1999 with a standard 128MB RAM and 2x73GB hard disk PC).
- Communication between GSM cell and landline is not encrypted (compared to the interface between mobile phone and GSM cell). Furthermore exactly that interface is often based on directional radio systems which can be intercepted with minimal efforts.
- Úsing a so called „IMSI-Catcher“ (GSM cell simulation, e.g. http://pgis.4t.com) GSM encryption (of mobile devices) can be switched off.
- Several system are existing which can passively interecept GSM calls (without poviding any information to mobile device).
- Estimated industrial spying damage in Germany → > 10 billion EUR per year
  → mainly price and (product) development information

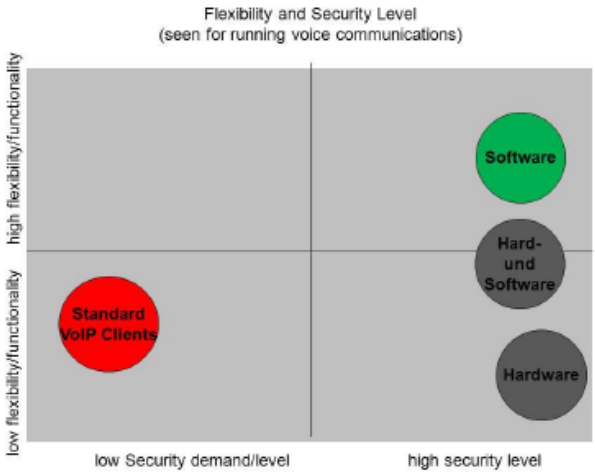
Privacy protection by using

- strong authentication and
- end-to-end encryption

Solution/implementation approaches

	Hardware	Hardware and Software	Software
+	security ex factory device secúrity	modular boundary certification	device flexibility price (investment) device management
-	few devices only limited functionality device management price	portability limited functionality device management	interaction with device full device security
→	Military	combined	Business





- ➔ Privacy for mobile voice calls and communications
  - ➔ authenticated and encrypted communications
  - ➔ 1:1 dialogues + conferencing capabilities
- ➔ VoIP Application
  - ➔ pure software
  - ➔ full-duplex real-time audio streaming
  - ➔ client/server architecture
  - ➔ using only *session-less* UDP/IP sockets
    - ➔ no VoIP protocol (spec. PDUs)
    - ➔ no need for SIP
- ➔ Maximum Flexibility in Handling
  - ➔ no need to be always online
  - ➔ no need to have it always running
  - ➔ may not even be installed at calling-time
- ➔ Highly scalable architecture

- Security for mobile voice communication
  - Mobile phones, smart phones
  - Notebooks, desktop PCs
- Secure mobile conferencing
  - Unlimited number of participants
- 100% secure and reliable → end-to-end encryption/security
- High speech quality
- Intuitive usage

Mobile VoIP application with enhanced voice protection and conference call support

Technical Characteristics:

- → End-to-end encryption
- → Cryptography: AES-256 bit data encryption using Diffie-Hellman key exchange (1024-4096 bit)
- → Protection against man-in-the-middle-attacks
  - → Individual, bilateral session keys
  - → Verbal fingerprint acknowledgement/confirmation

- → Audio: AMR 12.2kbps
- → Transport: UDP/IP - GPRS, EDGE, UMTS, WiFi

- → GUI: re-brandable, platform independent, skin support
- → Full integration with mobile device
  - → No restriction for other applications
  - → Access to standard address book

State of the art encryption

- AES-256 bit data encryption
- Diffie-Hellman 1024-4096 bit code for key exchange

Approvals

- Security audit performed by

HISOLUTIONS

- and in preparation by

Fraunhofer SIT Institut Sichere Informations-Technologie

Security Test Lab

Management of (conference) calls

➔ **Scalable architecture**

➔ More servers → better quality

➔ **Automatic load balancing**

➔ Automatic detection and association/usage of the most performant server

➔ **Simple server structure**

➔ **Open Source – no back doors**

➔ **Various server platforms:**

➔ Linux, Unix, Windows

- **Symbian 9.2**
  - Nokia : E71, N95, E63, E66, 6124, N82, E51, N81, 6121, 6120, 5700, 6110, E90, N76, 6290, …
- **Symbian 9.3**
  - Nokia: N78, N86, 6720, E75, E55, 6710, 5630, N79, N85, N96, 5320, (5730), 6650, 6210, 6220, …
- **Symbian 9.4**
  - Nokia: N97, N97mini, 5800, X6, …
- **Maemo 5**
  - Nokia: N900
- **Certified product**
- **Windows Mobile 6.5**
  - Samsung Omnia
- **Android 2.2, 2.3, 4.1**
- **Apple iPhone/iPAD/iPod Touch 3G**
- **Desktop/Notebook-Versionen**
  - **Windows XP, Windows Vista, Windows 7**
  - **Apple MacOS X**
  - **Linux**
- **Roadmap: Blackberry, Web-Client**

for symbian OS

Diversity of devices met by just one application!

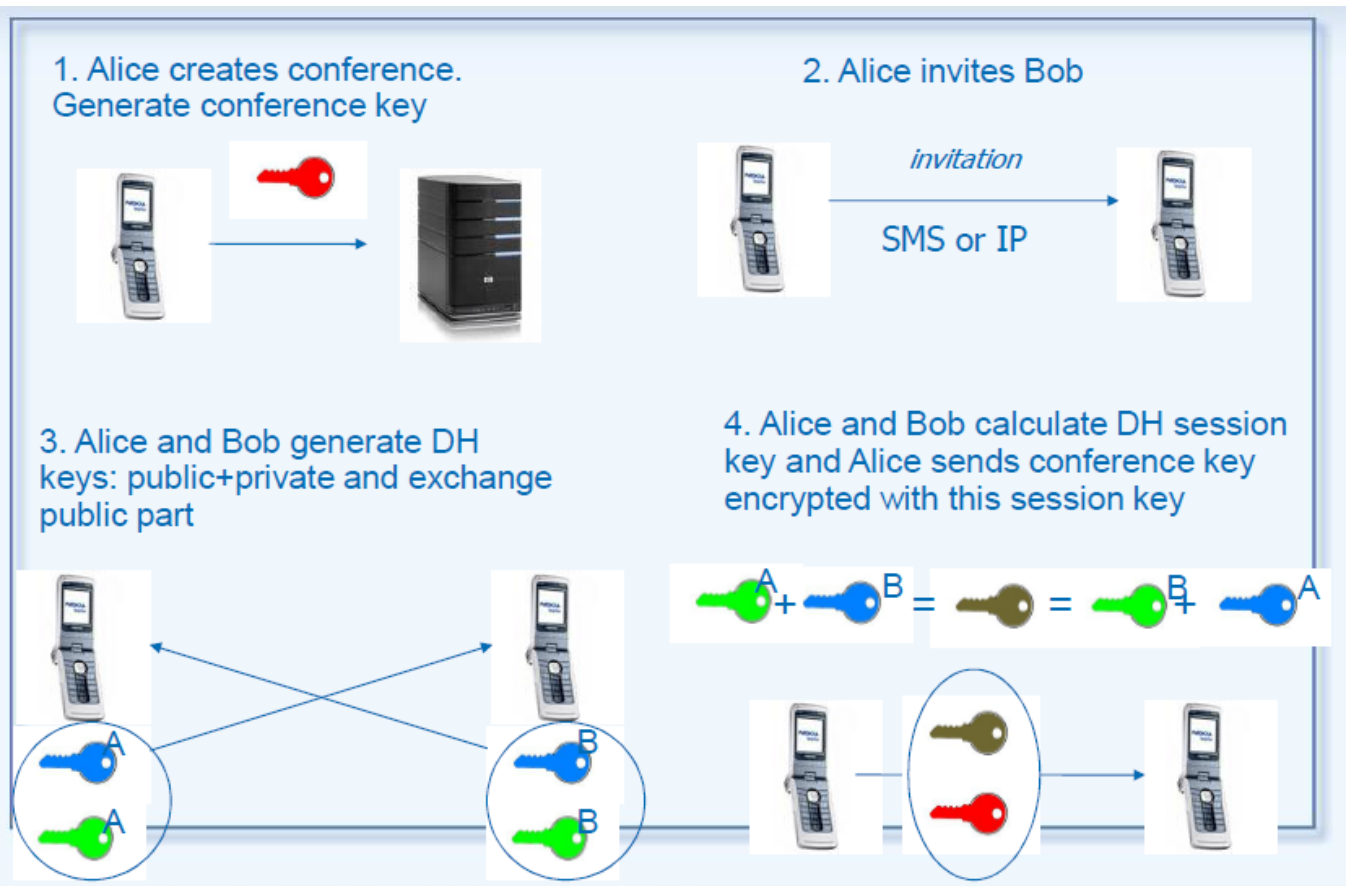
Index

1 Introduction

SecureScrypt/Enigma® is a plain software-based solution that provides encrypted voice calls in cell networks. The application enables 1:1 calls as well as conference calls. It applies an Internet connection via UMTS, EDGE, GPRS or WiFi in order to establish a voice over IP (VoIP) between the communication partners. All data crossing the line from the caller to the called parties and vice versa is transmitted fully secure. In state-of-the-art manner SecureScrypt/Enigma® prevents telephone tapping (or wiretapping as it is called in the USA).
The audio input from a microphone and data compression are handled by an audio codec1. The generated data packets become encrypted before transmission to the communication partners.
1 In Nokia mobile phones this is Audio Codec AMR-NB 12.2 kbps.
The application SecureScrypt/Enigma® applies the „Shared Library" <VoIPAudioSrv>, which is why it cannot co-exist with other data transmissions that use VoIP, e.g. „Fring", „Skype mobile" or similar.
The use of SecureScrypt/Enigma® .provides the capability to run wiretapping-safe voice calls and conference calls secured by state-of-the-art technologies.
Attention:
The application SecureScrypt/Enigma® is not recommended for the use in emergency call environments (like call numbers 112, 911 in the USA or others). The time-critical data transmission cannot be guaranteed.
This manual describes how to handle the SecureScrypt/Enigma® client that provides access to the world of encrypted voice communications on the mobile phone or smartphone.
It is meant to overcome questions concerning the program package and of general understanding in wireless applications used with SecureScrypt/Enigma®. It is meant to provide the SecureScrypt/Enigma® system administrator and user with all information that is required to install, configure and run the SecureScrypt/Enigma® client software.
The figures used in the following descriptions may differ from device to device. Please, consider them as examples which document the general process.

The Structure of this Manual

Besides the introduction, this administrator's manual is structured into the following chapters:
Chapter 2 Installation & Configuration explains the presumptions for the installation and configuration of the software product SecureScrypt/Enigma® and the installation procedure itself.
Chapter 3 Operations explains how to start the application and how to make encrypted calls.
Chapter 4 Uninstall shows how to remove the software from your device.
Chapter 5 Hints and FAQs some helpful information for you…
Chapter 5.11 Support names contact references for support and consultancy concerning technical issues.
Chapter 6 Glossary shall help to decode the technical language and abbreviations throughout this document. **2 Installation & Configuration**



2 Installation & Configuration

2.1 Requirements

The following preconditions have to be met by the system in order to install the SecureScrypt/Enigma® client software on your mobile phone:

- A mobile phone or smartphone with operating system Android 2.3 or later,
- 4,0 MB of free memory for installation.

This manual explains the use of the SecureScrypt/Enigma® Client for Android devices. Corresponding documentation for other platforms is available on demand.

Furthermore, the given conditions need to be met by the operations' environment:

- Some data-enabled contract with a service provider. Most preferable would be a flatrate agreement concerning the data volume;

alternatively an active WiFi connection;

- An inserted and activated SIM card in reference to the mentioned contract,
- A working Internet access through your mobile phone (pre-configured internet access point),
- At least one SecureScrypt/Enigma® server that is currently reachable via the Internet.

2.2 Preparation and Start of the Installation

Before installing the software you need to get hold of the software installation package. To do so, you may choose from a couple of different access processes:

- Download from the Internet directly into your mobile device,
- Download from the Internet into a PC,
- Use of a delivered CD on a Windows PC.

Obviously, the installation procedure will be different depending on the choice of software provision. In case the installation shall be run via a PC a corresponding access software has to be installed prior to the SecureScrypt/Enigma® installation. Please download the appropriate software for your device platform2

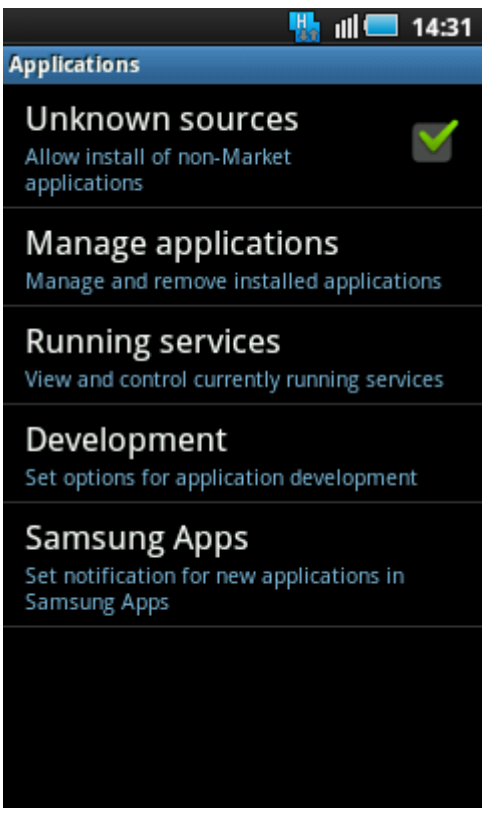
2 Typically such synchronization software tools are device and manufacturer specific, e.g. „Kies" for Samsung devices or HTC Sync for HTC devices.

Please start the installation process by activating the installation software package from your download directory. Just confirm the introduction question on whether you want to install the software - select **<Yes>**.

In order to install applications on the mobile phone/device the security settings must allow applications which are not listed in the Android marketplace.

Please activate the permission for applications from **<Unknown sources>** under ***Applications*** · ***Settings*** · ***Applications***.

Please carry on with the installation procedure as requested by the screen dialogue. **2 Installation & Configuration**



2.3 Installation

2.3.1 Preparation for Installation when Downloading to Mobile Phones

First step of the installation will be to connect your mobile device to the Internet. Then, use the systems' browser software of your mobile device in order to download the application software SecureScrypt/Enigma® directly into your mobile phone. You can access the download link on http://www.SecureScrypt/Neoi TEC.de/SecureScrypt/Enigma.html
Just click on the "Download" link to store the installation file on your mobile phone.
The installation can be performed directly on your mobile device now. Just follow the on-screen instructions. Start by confirming that the software package SecureScrypt/Enigma® is the one to be installed.
Please continue the installation process in ***chapter 2.3.4***.

2.3.2 Preparation for Installation when Downloading to a PC

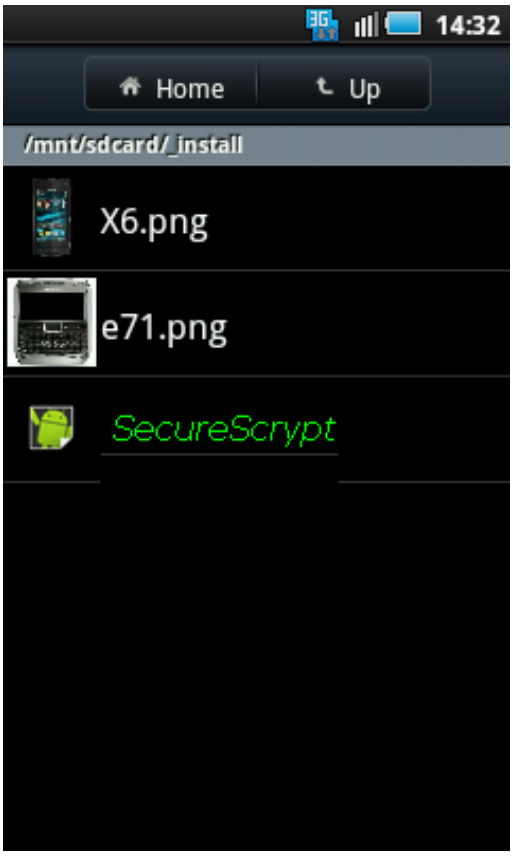
First step of the installation will be to connect your PC to the Internet. Then, use the systems' browser software of your PC in order to download the application software SecureScrypt/Enigma®. You can access the download link on http://www.SecureScrypt-Neoi TEC.de/SecureScrypt/Enigma.html (This link will only be available to licensed customers)
Just click on the "Download" link to store the installation file on your PC.
Please copy the downloaded installation file <SecureScrypt/Enigma_*Version_Number*.apk> to your mobile device by using the file explorer.
Please continue the installation process in ***chapter 2.3.4***.

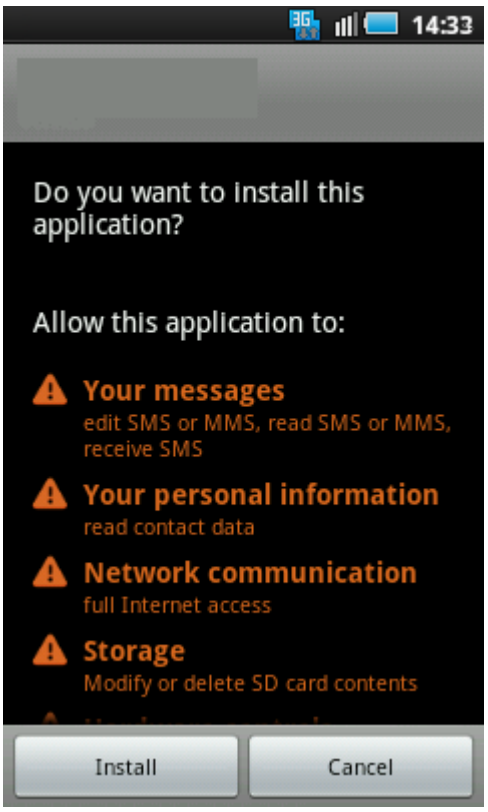
2.3.3 Preparation for Installation using some physical Installation Medium

Please insert the delivered CD „SecureScrypt/Enigma®" into the CD-ROM drive of your PC after Windows is fully booted.
In case the "Autostart" feature of your CD drive is deactivated, please use the Windows task bar and the "Start" button in particular, to go into the "Execute" mode. Then enter the given command:
<Drive>:
<Drive> has to be substituted by the appropriate drive letter on your system. E.g. if your CD-ROM drive in mapped to drive letter <D> the command will be „D:".
You will find a file name with the suffix ".apk" and this manual on the CD. There may be additional files there which are of no meaning to the discussed installation process.
Please copy the installation file to your mobile device. You can use the file explorer for this purpose.
Please continue the installation on your mobile device as explained in following ***chapter 2.3.4***.

2.3.4 The Installation Process to be Executed on the Mobile Phone

After the given installation preparations you may run the SecureScrypt/Enigma® installation routine on the mobile device according to the screen instructions. **2 Installation & Configuration**





Run the installation of SecureScrypt/Enigma® by clicking on the file presentation of **<SecureScrypt/Enigma_*Version_Number*.apk>**.
During the installation you will be asked to allow specific access rights for SecureScrypt/Enigma® on the Android operating system level. SecureScrypt/Enigma® requires these access rights for the Android components

- Your messages,
- Your personal information,
- Network communication,
- Storage,
- Hardware controls,
- Services that cost you money,
- Phone calls

in order to work as expected.
Select **<Install>** to continue unpacking and providing the SecureScrypt/Enigma® application on your device.
After successful termination of the installation routine you will find the SecureScrypt/Enigma® program icon on the last page under **<Applications>**.
At the first start of SecureScrypt/Enigma® it shows the license agreement. Please read and accept the End User License Agreement (EULA).

2.4 Configuration

Before users can apply the SecureScrypt/Enigma® client to run encrypted calls, the software typically has to be configured to match the individual and company-specific requirements.

Since the important operations parameters for SecureScrypt/Enigma® will (already) be set by your wireless network operator/provider or by settings of your mobile device, e.g. phone book contacts, you will not need to do additional configurations for SecureScrypt/Enigma®. SecureScrypt/Enigma® can select contacts from your phone book on the mobile device but alternatively you may type phone numbers directly or call people from the call history. Thus, even the generation of phone book contacts is not a mandatory issue for running encrypted voice calls.

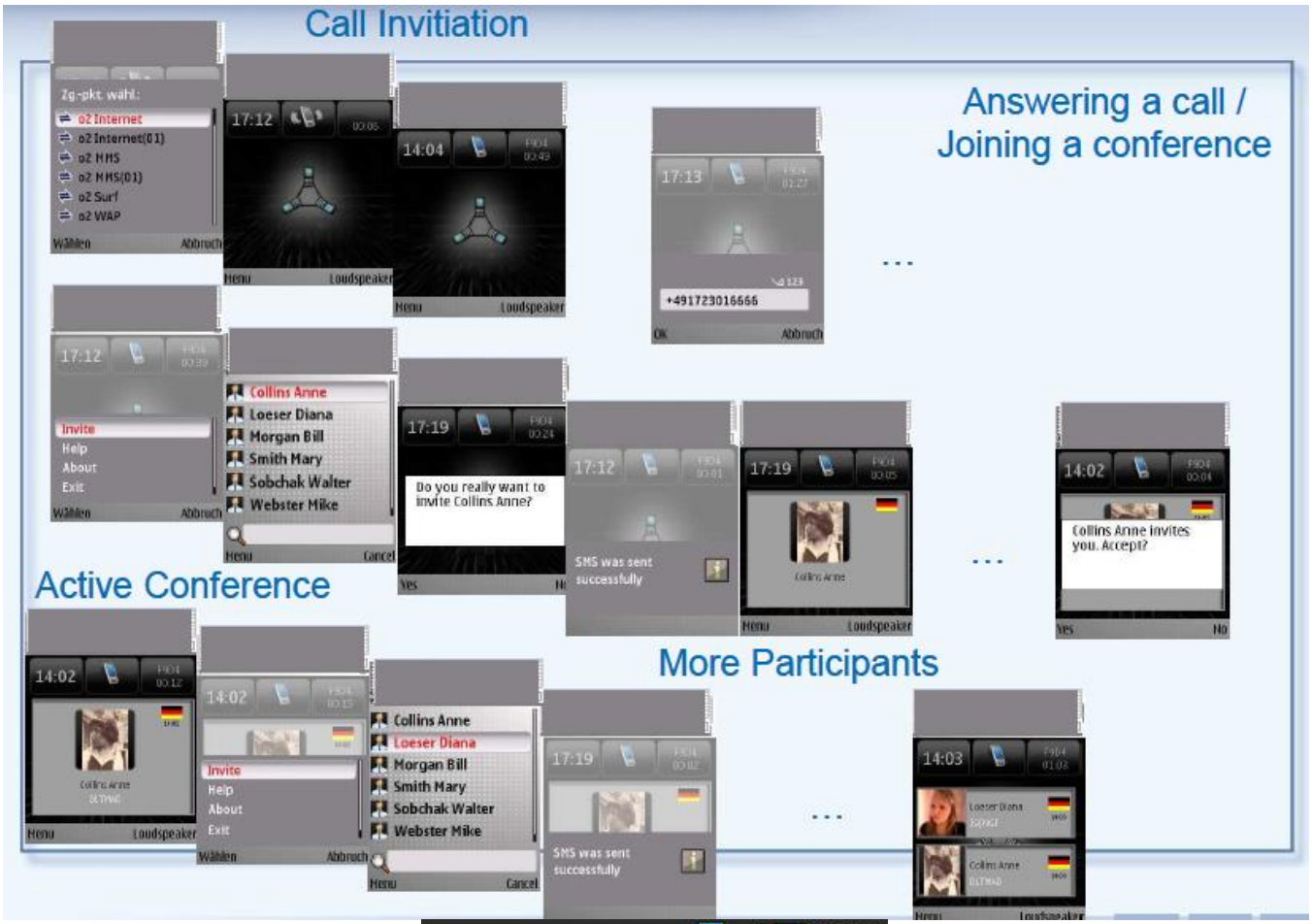
2.5 A First Check

If you want to make sure that your SecureScrypt/Enigma® software works correctly you may call a service number. Please refer to chapter to get connected to #1

You will be connected to a SecureScrypt/Enigma® server that offers an echo function. So once you are connected just speak some text. If you can hear the echo alright, your installation was successful.

3 Operations

After the configuration settings you are ready to use SecureScrypt/Enigma® for your secure and confidential calls and conferences via mobile networks.



3.1 Starting the Program

The SecureScrypt/Enigma® client will be executed like all other applications on your Android device, i.e. by a click on the corresponding program icon in the **<Applications>** list.
If your Android device is not connected to the Internet when starting SecureScrypt/Enigma®, the application will (try to) establish an Internet connection using the currently selected Android standard method for Internet access, i.e. UMTS/GPRS or WiFi.

3.2 Connection Status

Once the SecureScrypt/Enigma® Client comes active you will see its user interface in a full screen display. Somewhere left on the top of the screen you will find the current time, and on the right there is a runtime counter that displays how long SecureScrypt/Enigma® has already been running or the time since beginning or terminating the last call, respectively. In the middle position you will find a status icon in the shape of a smartphone. This icon is a status indicator that reflects the current connectivity to a SecureScrypt/Enigma® server.

Semantics of the icons:

Icon	Status	Bedeutung
	not connected / offline	The SecureScrypt/Enigma® client is running but there is no active connection to a server. You might see this status directly after starting the application or in areas with weak or no coverage. (Grey smartphone.)
	connecting	SecureScrypt/Enigma® tries to connect to some server. (Grey smartphone with radio signal indicators on the sides)
	connected / online	Your mobile device is connected to the SecureScrypt/Enigma® infrastructure and can be used for encrypted communication. (Smartphone coloured monitor.)

If your Android device is not connected to the Internet when starting SecureScrypt®, the application will (try to) establish an Internet connection using the currently selected Android standard method for Internet access, i.e. UMTS/GPRS or WiFi.
Directly after starting the application you might see the connection establishment icon in the status display. During this display your mobile device tries to connect to a SecureScrypt® Server.

3.3 The Command Menu

Whenever SecureScrypt® is shown as the active application of your mobile device, i.e. when the screen shows the SecureScrypt® application you can press the left function key to pop-up the SecureScrypt® command menu or press icon **<Menu>**.
Select this key to have access to the commands:

Invite..
Call a partner by selecting him from the phone book contacts.

Help
Read a brief explanation on how to handle the application.

About
Provide information on the installed program: program name, version and manufacturer.

Exit
Terminate SecureScrypt®

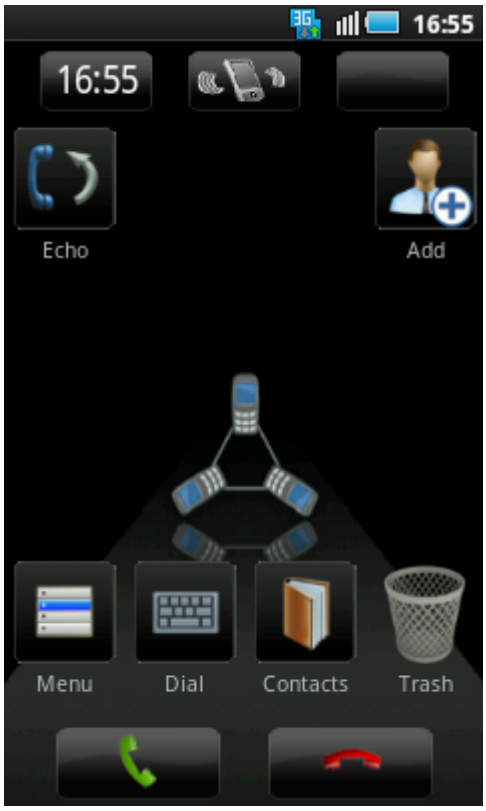
3.4 Encrypted Phone Sessions

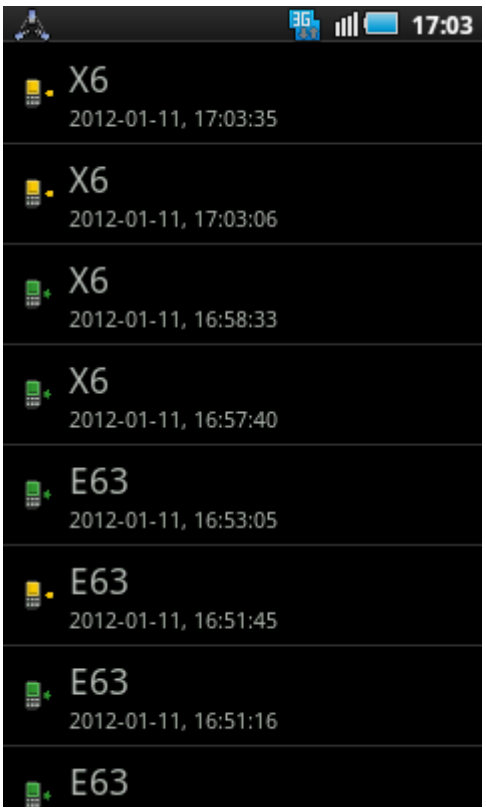
All calls and conference sessions run by SecureScrypt® are save from wiretapping; your data is always encrypted in transfers.

3.4.1 Call your contacts

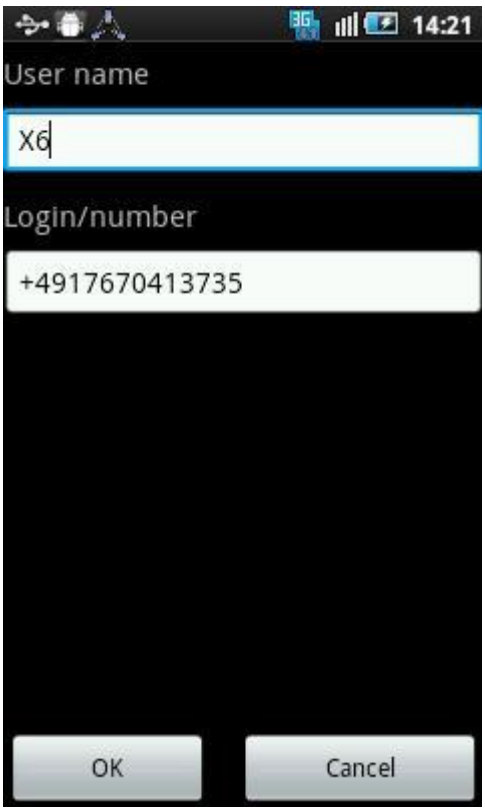
As known from normal calls you can directly type the number to be called while the SecureScrypt® application is displayed.
Please use the given address modes for call invitations depending on the type of device you want to reach:
Android: phone number
iPhone: user name (login name/online ID) or
email address
Symbian: phone number
Windows Mobile: phone number

Windows Desktop: user name (login name/online ID) or email address



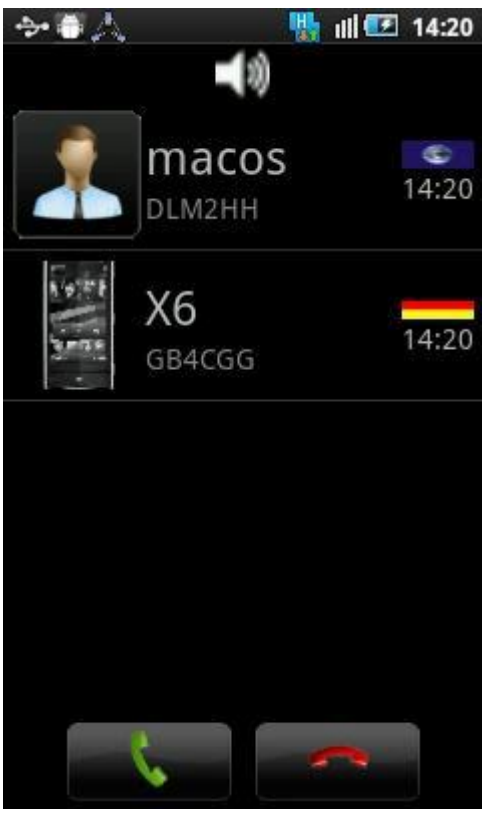


Please enter the phone number including the country code even for local calls.
After completing the call address information select **<OK>** to initiate the call.
In addition, you can select your communication partner from the call history. Just click the green button (showing the phone receiver) to see this list. Select the desired entry and hold your finger on it.
A submenu provides the means to either place a shortcut for this contact on your desktop by selecting **<Add to desktop>** (***please refer to chapter 3.7***) or call the named party by using **<Invite>**. If you click on **<Cancel>** the call history is closed and you are taken back to the initial SecureScrypt® screen display.
And, of course, partners can be invited by means of the phone book or stored contacts.
For calling a partner from the phone book please press the **<Menu>** icon at the SecureScrypt® desktop and open the phone book by selecting **<Invite>** from the pop-up menu and scroll to the desired contact.
Alternatively and somewhat faster you can reach stored contact entries by clicking on the icon **<Contacts>**.



Please select the corresponding contact to initiate the call. If there are multiple phone numbers and/or email addresses assigned to that contact, you need to select from them again.
Similar to the selection from the call history you will see a new dialog screen that offers **<Invite>** to confirm your call initiation.
Invited partners that use SecureScrypt® on Symbian devices (e.g. Nokia mobile phones), Windows Mobile or Android clients will be informed by an SMS. This way invitations can be sent to and answered by partners that have no mobile network coverage or have their mobile devices turned off. Invitations can be accepted within a time period of up to 5 minutes.
SecureScrypt® users running a desktop or iPhone client will receive on online message when they are called. If SecureScrypt® is up and running in this situation the online message is automatically interpreted and the incoming call is signaled by the SecureScrypt® user interface. Otherwise, the user can start SecureScrypt® or wait until potential network problems in his Internet access are fixed.
While you wait for the call to be answered you will hear a calling signal and the called party is displayed[3].

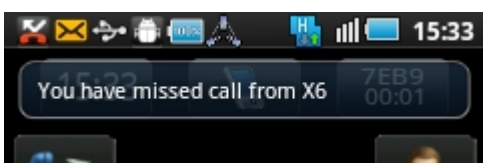
[3] If your phone book or contacts list has stored a photo for the participant, this photo will be displayed. Otherwise, you will see some phantom picture.

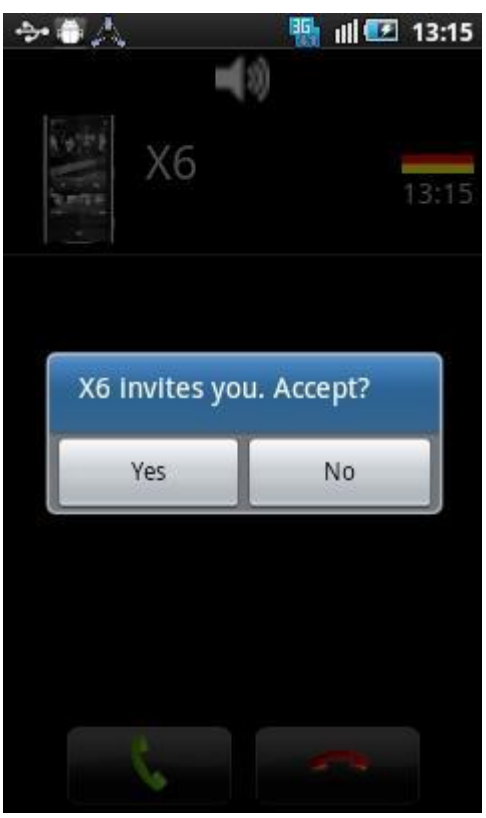


As soon as your partner answers the call, you will find the ringing tone stops and your display will show the individual session key fingerprint beside the called name. Ask to confirm this session key in order to make sure that your partner is really authentic.
Now you can run a tapping-secure communication.

3.4.2 Answering a Call

An incoming conference invitation will be displayed immediately if SecureScrypt® is running.
You can now decide whether to join the call or whether to reject the call. Just press **<Yes>** or **<No>**.
If you do not run SecureScrypt® when an invitation is received you will be informed by an SMS. Once you start SecureScrypt® - assumed that this does not take you longer than 2 minutes – you will see the conference invitation without additional steps. In case the calling party has cancelled the request in the meanwhile, SecureScrypt® will show one missed call. You can use this history entry to return the call.





3.4.3 Initiate phone conferences

Please choose your first conference partner as described in ***section 3.4.1*** first. Afterwards, i.e. while in a call with this first participant, you can press the Android **<Back>** key to return to the initial screen display of SecureScrypt®.

As for the first communication partner you can apply the phone book **<Contacts>**, the call history which can be reached by pressing the **<green call button>**, or by directly keying in the recipients ID by invoking the **<Dial>** icon.

As soon as your second partner answers the call, your display will show the individual session key fingerprint beside the called name. Ask to confirm this session key in order to make sure that your partner is really authentic.

During invitation and waiting for a news conference participant there is no interruption of the running conference you can continue talking to those that have already joined.

3.4.4 Hang-up and Leaving a Conference

As common for unencrypted mobile calls and phone calls in general the **<red hang-up button>** is used to terminate a 1:1 session as well as to leave a conference.

When a participant leaves a conference the conference call will still be active, i.e. the remaining participants just continue the session – independent whether the leaving user has been the initiator or just an ordinary participant.

3.5 Loudspeaker

During call invitation waiting periods or within a session a click at the loudspeaker button on the top of the SecureScrypt® desktop switches between „headset" and „loudspeaker" (hands-free).

For security reasons you should not run loudspeaker mode during a session. The best encryption technology cannot hide your confidential messages from others sitting around you in a bar if your loudspeaker provides this information to everyone.

3.6 Volume Control

During SecureScrypt® conferences you can tune the sound level by using the standard hardware buttons of your device.

3.7 Using Shortcuts

SecureScrypt® allows you to tune your user interface according to your personal treatment. Contacts that you call often can be mapped to shortcuts. These shortcuts can be applied to call the associated partner by just clicking the shortcut.

Due to limitations in device screen size SecureScrypt® for Android clients allows to create a maximum of 11 shortcuts. If you have reached this number already, please delete an entry from the SecureScrypt® desktop before creating a new shortcut (see ***chapter 3.7.5***. **3 Operations**)

3.7.1 Define new Shortcuts manually

A click on the icon **<Add>** of the SecureScrypt® user interface opens a dialogue that shows the required definitions.
Just enter a character string to identify the shortcut under **<User name>**.
Enter the call information for your partner as explained in the sequel:
Please use the given address modes for call invitations depending on the type of device you want to reach:
Android: phone number
iPhone: user name (login name/online ID) or
email address
Symbian: phone number
Windows Mobile: phone number
Windows Desktop: user name (login name/online ID) or
email address
Confirm your input using the **<OK>** button to generate the corresponding shortcut on the SecureScrypt® user interface.

3.7.2 Form Shortcuts from Call History Entries

Press the green call button of your mobile phone to open the call history and select the entry that shall be represented by a shortcut. Then click on **<Add contact to desktop>** to place the corresponding shortcut on the SecureScrypt® desktop. In order to return to the desktop view click on **<Cancel>**. This will leave the call history.

3.7.3 Shortcuts out of Phone Book Contacts

Go to the phone book by clicking on **<Contacts>**. Then select the desired contact entry and use **<Add contact to desktop>** to create the corresponding shortcut on the SecureScrypt® desktop. You will leave the phone book and return to the desktop by **<Cancel>**.
When creating shortcuts from phone book contacts that have a picture stored with the entry, this picture will be displayed on the desktop. Shortcuts that have no pictures associated will show some anonymous graphics.

3.7.4 Edit existing Shortcuts

If you need to change online ID or phone number to a shortcut you can open the parameter box by selecting that shortcut and applying **<Edit...>**. Simply overtype the old values that need modifications (see ***chapter 3.7.1***). To finish the redefinition click on **<OK>**.

3.7.5 Delete Shortcuts

Once a shortcut is no longer needed or screen space is required to generate a new one, drag the shortcut to the wastebasket **<Trash>**.
A security question shall prevent shortcut deletion by accident. Confirm your action by clicking **<Yes>** if you really want to delete the considered shortcut.

3.8 Language Settings

The standard delivery version of SecureScrypt® comes with english language for the user interface. In addition, you may load additional national language files in order to switch to your favourite language.
Please contact your administrator to find out which language sets are available.
Optional language support require downloads of the corresponding language files, unless they are pre-installed for some customized deliveries. These files need to be installed on your mobile device after you downloaded them to your PC. First, connect your mobile phone to your PC; then proceed according to ***Chapter 2.1*** for downloads that shall be transferred to your mobile device. Afterwards, please use the file manager application to copy the new language files to the target directories on your mobile device as given below:

<Phone|Android|data|com.SecureScrypt>

Once additional language support is installed, you can switch between the installed languages. Select your language of choice by keying the code from the table shown here in the SecureScrypt user interface and execute the code by pressing Return.

Country code Language

#8 English
#822 German
#827 Spanish
#834 French
#890 Portuguese
#85 Arabic
#882 Dutch
#852 Italian
#895 Russian
#8138 Chinese

For a complete list of all supported language codes please refer to ***chapter 5.10***.

SecureScrypt will confirm your request and ask you to terminate and restart the application. After restarting SecureScrypt the user interface will be presented in the chosen national language.
In case SecureScrypt displays the error message "Can not apply new language" here, please check whether the used language code is associated to an optional language support given by installed language files on your mobile device. If you are sure to have the correct files available, please contact your administrator.

4 Uninstall

4 Uninstall

In order to remove the software application SecureScrypt® from your mobile device just invoke the standard procedure in application removal
Menu · Settings · Applications · Manage applications · SecureScrypt® · Uninstall
and follow the screen advices.

5 Hints and FAQs

5.1 Data Transmission Costs

The application SecureScrypt® will (besides license costs and/or usage fees) generate additional costs when used.
Pre-requirement for running SecureScrypt® on a mobile device is some enabled Internet access capability that is charged as an extra by most of the network operators and providers. And, it does not matter whether this access is achieved via public hotspots or private hotel access points on WiFi, via UMTS, EDGE, or GPRS – in all cases you will have extra costs.
Ideally, you should go for a contract with the mobile network operator or provider that covers all data traffic (unlimited) by a flatrate payment. Since SecureScrypt® digitizes your voice data and transfers them after encryption via packet-oriented data protocols potentially generated data traffic may become quite high and expensive when paid by on-demand agreements.

5.2 Lab-Tested Devices

The application SecureScrypt® is meant to run on all Android-based devices on Android version 2.3.
Examples for explicitly SecureScrypt lab-tested devices are:
Huawei X3
Motorola MB632
Samsung Galaxy (GTi 9000)
Samsung Galaxy S (GTi 9001)

5.3 Using other Programs while SecureScrypt® is running

After the application SecureScrypt® is started its user interface will be displayed in full screen format. The standard hardware command buttons of the mobile device will be associated with program–and context-specific semantics in this status.
In order to start or control a different application SecureScrypt® needs to be terminated or to be shuffled into background execution.
One way to force background execution is to invoke the <HOME> key of the mobile device. The screen display will switch to the initial presentation while SecureScrypt® is still executed. Now, you can type input to other programs and still be available for encrypted calls.
To bring back SecureScrypt® as the active application you simply invoke the same command input as if starting the application from scratch.
Other applications that use Voice-over-IP, e.g. Fring and Skype. May in general be run concurrently with SecureScrypt®. However, in case these programs access the some system resources like the codec you may observe unorderly behaviour in these applications.
So we do recommend using such applications exclusively.

5.4 Non-Secure Calls

The most important and basic functionality of a mobile phone or smartphone will always be the capability of unencrypted calls. Therefore, even in active SecureScrypt® session and while the application is running you can still take unencrypted calls and even initiate unencrypted calls while SecureScrypt® Is not the topmost application.
In order to move SecureScrypt® to the background just press the <HOME> key of your mobile device. If you see your initial screen layout you are free to use the phone book contacts or directly type digits for initiating an unencrypted call. Of course, you will control this call by means of the green calling and the red hang-up button.
Please make sure that you run confidential calls only when SecureScrypt® is visible on your monitor. Otherwise, you may still communicate with the correct partner but your dialogue will not be encrypted.

5.5 Termination of Conference Calls on Incoming Unencrypted Call

For SecureScrypt® that means that even during runtime and active conferences in SecureScrypt® other incoming calls must be signaled.

whenever receiving an incoming GSM call SecureScrypt® is forced into the background and the basic system screen is displayed.
The decision whether this call shall be accepted or rejected is completely up to the user.
Accepting this GSM call will automatically abort active SecureScrypt® sessions; they can be re-established after terminating the GSM call.
The application SecureScrypt® itself remains active in the background although the current session is aborted. Thus, there is no need to restart it after some normal GSM call.

5.6 Use of SMS

With reference to chapter 7.1 we have to point out that each call invitation in SecureScrypt® sends an SMS to the called party.
Please keep in mind that the mobile network usage contract that you look for should cover a sufficient number of free SMS in addition the calculated data transfer.

5.7 How Secure is SecureScrypt®?

SecureScrypt® provides privacy on the highest level.
Based on currently world-wide accepted standards of IT security you will authenticate your communication partner, and will provide some unique and one-time session token for verbal confirmation. This method prevents so-called „man-in-the-middle attacks".
In order to deny inadmissible access and interpretation of the transmitted data in public data networks between your mobile device and the corporate network or partner's device, SecureScrypt® uses fast and resource-preserving encryption algorithms for your voice/data transmissions. In general, these encryption procedures allow the definition of a suitable encryption key length. Thus, following today's understanding of security and encryption the power of these mechanisms will protect your confidential data for a couple of decades to come.
The key exchange procedure between the communicating parties is secured by Diffie-Hellman procedures (1024–4096 bit[4]). For data encryption of the transmitted content the highest available standard AES (Advanced Encryption Standard) is applied with a key length of 256 Bit.

[4] The default installation package is limited to 1024 bit.

5.8 SecureScrypt® Status Information during Operations

During SecureScrypt® runtime the user interface will display status information by means of changing icon presentations and potentially messages. Some of them are given here in order to help you understand their semantics and potentially required actions.

<Internet not found>

SecureScrypt® could not establish a connection to any SecureScrypt® Server. There are several reasons that may cause this message display, primarily:
1. The mobile phone could not access any Internet service. Please check the settings for the Internet Access on your mobile phone. It may be a good idea to

try some public Internet access using the phone's browser.
2. The SecureScrypt® Server given in the internal configuration settings of the client is not reachable. If you have made sure that your Internet connection is working (see bullet point 1) please contact your systems' administrator.

<Serverlist updated>
Typically, you may notice this message directly after starting SecureScrypt®. It informs you that the SecureScrypt® Server has deployed an updated list on all available servers to your client. This list is automatically merged into the operational client code; no user interaction is required.
<Force Server: xxxx>
You will notice this message text when your SecureScrypt® Client has been forced to switch to a different server. The reason for this may be some network congestion. The ID **<xxxx>** is a code that uniquely identifies the new server and server location.

5.9 Known Restrictions / Problems

5.9.1 National Language Support

5.9.2 Use of WiFi Internet Access

We would not recommend selecting "Search for WiFi" from the menu "Internet Access Point" inside SecureScrypt®. Please use the "Connection Manager" of the mobile device to register your Internet Access Points before running SecureScrypt®.
Experience reveals that Internet Access Points need to be preset before their use by applications. Otherwise, some devices may report an error.
During your first approach to UMTS/EDGE/GPRS networks such initialization for Internet Access Points will typically be run by your GSM operator. WiFi networks usually require manual setup.

5.10 Language Codes

The table given below summarizes all language codes that are currently supported by the implement. Please make sure that you have copied the corresponding language files to your mobile device before switching to a new target language (refer ***chapter 3.8***).

Code	Language
1	Afar
2	Abkhazian
3	Afrikaans
4	Amharic
5	Arabic
6	Assamese
7	Aymara
8	Azerbaijani
9	Bashkir
10	Byelorussian
11	Bulgarian
12	Bihari
13	Bislama
14	Bengali
15	Tibetan
16	Breton
17	Catalan
18	Corsican
19	Czech
20	Welsh
21	Danish
22	German
23	Bhutani
24	Greek
25	English
26	Esperanto
27	Spanish
28	Estonian
29	Basque
30	Persian
31	Finnish
32	Fiji
33	Faroese
34	French

35	Frisian
36	Irish
37	Scots
38	Galician
39	Guarani
40	Gujarati
41	Hausa
42	Hebrew
43	Hindi
44	Croatian
45	Hungarian
46	Armenian
47	Interlingua
48	Indonesian
49	Interlingue
50	Inupiak
51	Icelandic
52	Italian
53	Inuktitut
54	Japanese
55	Javanese
56	Georgian
57	Kazakh
58	Greenlandic
59	Cambodian
60	Kannada
61	Korean
62	Kashmiri
63	Kurdish
64	Kirghiz
65	Latin
66	Lingala
67	Laothian
68	Lithuanian
69	Latvian
70	Malagasy
71	Maori
72	Macedonian
73	Malayalam
74	Mongolian
75	Moldavian
76	Marathi
77	Malay
78	Maltese
79	Burmese
80	Nauru
81	Nepali
82	Dutch
83	Norwegian
84	Occitan
85	(Afan)
86	Oriya
87	Punjabi
88	Polish
89	Pashto
90	Portuguese
91	Quechua
92	Rhaeto-Romance
93	Kirundi
94	Romanian
95	Russian
96	Kinyarwanda
97	Sanskrit
98	Sindhi

99	Sangho
100	Serbo-Croatian
101	Sinhalese
102	Slovak
103	Slovenian
104	Samoan
105	Shona
106	Somali
107	Albanian
108	Serbian
109	Siswati
110	Sesotho
111	Sundanese
112	Swedish
113	Swahili
114	Tamil
115	Telugu
116	Tajik
117	Thai
118	Tigrinya
119	Turkmen
120	Tagalog
121	Setswana
122	Tonga
123	Turkish
124	Tsonga
125	Tatar
126	Twi
127	Uighur
128	Ukrainian
129	Urdu
130	Uzbek
131	Vietnamese
132	Volapuk
133	Wolof
134	Xhosa
135	Yiddish
136	Yoruba
137	Zhuang
138	Chinese
139	Zulu

5.11 Support

In case of technical problems with the product please contact us either way you want to:

Phone: +49 1711638089 - +65-65249086

E-Mail: support@SecureScrypt.com

Please make sure that you can pass the listed information concerning your problem:

- product name and version
- phone number and IMEI
- used operating system and version
- used data services and configurations
- used application software.

Information concerning our products SecureScrypt® and Enigma ® can be obtained via our Internet site

www.SecureScrypt.de http://www.securescrypt.com

6 Glossary

AP	Access Point. Central access node of WIFI networks, This access point serves for the coverage of a defined region and operates as a bridge or gateway to other networks, e.g. the company LAN running twisted pair cabling or the Internet which is access via PSTN modem or ISDN dial-up..
Connection	Consider in the context of data connections: a permanent association of two devices enabling them to exchange data. This connection may be wireless or wired; it may be direct or indirect via some relay stations and gateways.
GPRS	General Packet Radio Service. GPRS, available since 2000, support packet-switched GSM data traffic. Billing in GPRS is based on the transmitted volume of data.
GSM	Global System for Mobile Communications. The basic service and international standard digital cellular networks. The German operators T-Mobile and Vodafone rely on this technology.
Hotspot	Public WiFi access point which typically requires explicit user data depending on the provider for this hotspot.
IMEI	World-wide unique hardware identifier for mobile devices with UMTS/EDGE/GPRS/GSM modules. The International Mobile Station Equipment Identity (IMEI) is a 15 digit serial number.
IP address	A standard IP address consists of 4 bytes (IPv4) or 4 Quads, respectively. These are separated by colons, e.g. 193.96.28.72. These addresses identify computer systems on networks, e.g. in the Internet. Resources computers, Web servers and even Web cameras can be identified. Typically, these Ip addresses are only used program internally. User interfaces typically use mnemonic names that are mapped to these IP addresses by so-called domain name services (DNS).
LAN	Local Area Network; typically a regional network that connects devices of one authority.
Port	The physical or logical interface to some device or network.
Provider	Company that provides service access points – either for wireless protocol services or to the Internet.
Protocol	A set of rules and data formats implemented to allow data exchange between different computing systems.
TCP/IP	Transmission Control Protocol/Internet Protocol; the most common network protocol for heterogeneous networks. A connection-oriented transport protocol for the Internet and Intranets.
UMTS	Universal Mobile Telecommunications Systems. UMTS is the 3rd generation of wireless networks; in the future, it may be the reason for closing the GSM services down.
VoIP	Voice-over-IP. A data transmission protocol especially designed

	for the transmission of voice in packet-oriented networks.
WAN	Wide Area Network; network to connect systems which are placed far apart from each other.
WiFi	Wireless Local Area Network (so wird es auch genannt: Wireless LAN, WLAN, WiFi) bezeichnet ein drahtloses lokales Funknetz – üblicherweise nach den Standards der IEEE 802.11-Familie.