Operational User Guide

Dencrypt Talk v. 4.1 (Android)

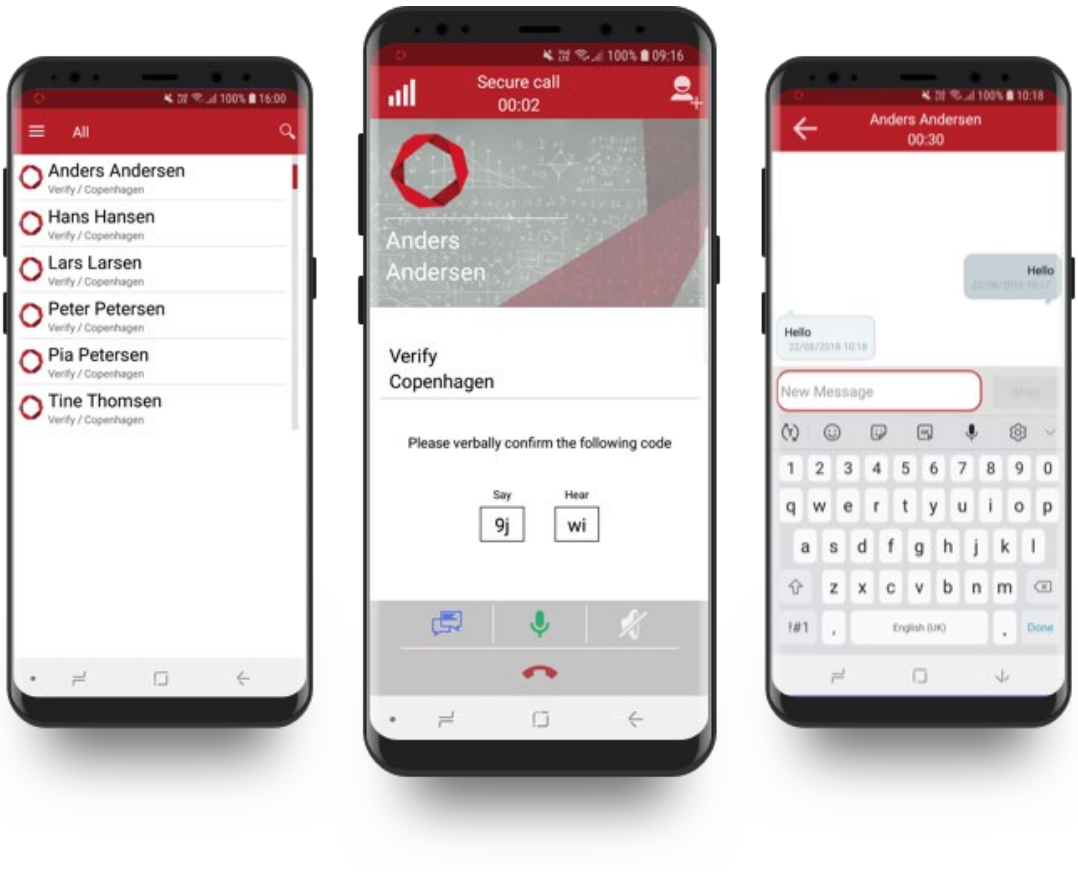


Table of Contents

Product version 3
Introduction 3
1 System overview 4
2 Security Functionalities 5
2.1 End-to-end encrypted VoIP calls 5
2.2 Mutual authentication 5
2.3 Encryption keys 5
2.4 Secure phonebook 5
3 Precautions 6
4 Provisioning 7
4.1 Configuration 7
4.2 Permissions and notifications 8
5 Making secure connections 9
5.1 Avoid acoustic coupling 9
5.2 Other precautions 9
5.3 Use of secure live chat 9
5.4 Establish a secure voice call 9
5.5 Establish a secure live chat 10
5.6 Establish a secure group call 11
5.7 Incoming calls 13
6 Settings 14
7 Version number 15
8 Reporting security incidents 15
9 Error and information messages 16
9.1 Provisioning 16
9.2 Phonebook and settings 17
9.3 Secure call and -chat 18
9.4 Other messages 20
10 Change History 21

Product version

This guide applies for DencryptTalk (Android), version 4.1.

Introduction

This guide is intended for end-users of the Dencrypt Talk application (Android version) and provides general instructions on how to operate and use the application in a secure way.

All end-users of the Dencrypt Talk application shall have familiarized themselves with this document and received instructions from the system administrator prior to taking the product in use.

This document contains:

- An overview of the security functionality offered (Section 2).
- A list of precautions to be observed for a secure operation (Sections 3 and 5).
- How to make a first-time configuration (Section 4).
- How to make secure calls and secure live chat (Section 5).
- How to report security incidents (Section 8).
- List of error messages (Section 9).

1 System overview

The Dencrypt Communication Solution is an encrypted Voice-over-IP based communication system, which offers mobile voice communication and live chat within well-defined user groups. Once installed and configured, it allows two or more persons to talk securely or two persons to chat securely.

The system consists of Dencrypt Talk, a smartphone application (app), installed on the end-user's smartphone and a Dencrypt Server System as illustrated below. The Dencrypt Server System is responsible for setting up encrypted calls and for distributing an individual phonebook to each device defining to whom calls can be made. The server system is also responsible for initiating the provisioning process for the first-time configuration. The server system only facilitates call setup and routing of chat messages. It is not capable of decrypting voice- or chat data as these are end-to-end encrypted between devices.

The Dencrypt Talk application is provided by the organisation's Mobile-Device-Management (MDM) system. The Dencrypt Server System is managed by a system administrator appointed by the organization.

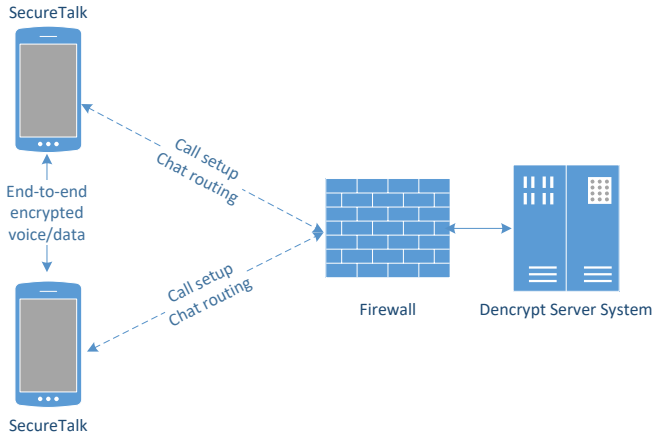


Figure 1 Dencrypt Communication Solution overview.

2 Security Functionalities

2.1 End-to-end encrypted VoIP calls

An end-to-end encrypted Voice-over-IP (VoIP) connection between the communicating devices is established using the mobile internet and/or Wi-Fi networks. Only the data transmission over this connection is protected. Sound entering/leaving the device's microphone/speaker remains unprotected as illustrated below. This applies to accessories such as Bluetooth headsets as well.

Once a connection is established, the exchange of encryption keys occurs automatically and directly between the two mobile devices. The key exchange is initiated when a call is answered and a data connection established. At call termination, keys and chat data are permanently removed from the devices and cannot be recovered.

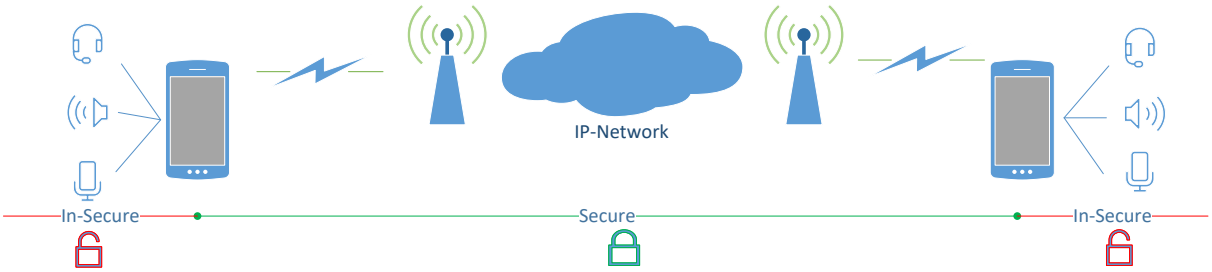


Figure 2 Area of protection

2.2 Mutual authentication

The Dencrypt Communication Solutions applies mutual authentication between the Mobile Client(s) and the Dencrypt Server System. This protects against attackers using 'fake' server systems and ensures that only authorized mobile devices can connect to the server system. The authentication is automatic and does not require any interaction from the end-users.

2.3 Encryption keys

Generation of encryption keys for authentication, signing, and data encryption happens automatically and does not require any user interaction.

2.4 Secure phonebook

To ensure that only authorized persons can communicate, the Dencrypt Talk application contains a centrally administered individual phonebook, which defines to whom calls can be made. The phonebook is provided automatically by the Dencrypt Server System. The application will check for updates each time it is opened and able to register to the server system. Phonebook updates, if any, will be downloaded automatically.

It is only possible to establish calls and live chats with persons listed in the phonebook. The phonebook is defined by the system administrator and it is not possible for the end-user to modify the phonebook. The phonebook system supports individual group settings, which means that it is possible to allow user A to call user B, but not vice versa. Hence, it is possible to receive a call from a person not listed in the phonebook, but it is not possible to call back.

3 Precautions

A number of precautions must be observed in order to use the application in a secure manner and to avoid disclosure of information. Please observe the following prior to taking the application into use.

- **Organisation's security policies –** Ensure that the security policies and instructions on how to use the application have been provided by the system administrator. Be aware of which types of classified information are allowed to be exchanged using the Dencrypt Talk application.
- **Server System security -** The System Administrator is responsible for the operation of the Dencrypt Server System and to ensure the system is kept updated and is working correctly and securely. In case of critical security incidents or unresolved vulnerabilities, the System Administrator may prevent calls to certain individuals or make the entire system unavailable until the issues have been resolved. In this case, it may not be possible to make secure calls to all or selected entries in the phonebook.
- **Handset security –** The security of the system depends on correct operation of the Android operating system and that there is no security critical side-effects. Therefore, the Dencrypt Talk application and the Android system software shall always be kept updated to the latest versions. In case of critical security incidents or unresolved vulnerabilities, the system administrator may prevent calls to certain individuals or make the entire system unavailable until the issue have been resolved.

  Software updates for the application are provided by the system administrator through a Mobile Device Management system. If in doubt, please contact your system administrator.

  Go to the Android settings menu to check for Android software updates and update if needed. The exact path to the menu item that checks for updates differs between Android manufacturers and across Android OS versions, but it is usually found by navigating to a path similar to '*Settings/System/Advanced/System update*'.
- **No backup –** The Dencrypt Talk application data, such as phonebook and settings files, will not be included in any backup of the device. This means that the end-user needs to be re-provisioned by the system administrator, if he/she re-installs the application to receive settings and updated phonebook
- **Benign applications –** The Dencrypt Talk application only protects the data transmission over the mobile- or Wi-Fi networks. It does not protect against malware intercepting audio- or chat data before encryption or after decryption. Therefore, only benign apps shall be installed on the device.

  Beware of any application that:

  - Makes use of the microphone
  - Listens to the earpiece
  - Records keyboard strokes

  If in doubt, contact your system administrator.
- **Single user device –** The phonebook entries are directly linked to the end-user's device. Therefore, the device shall be strictly personal and may not be shared with anyone.
- **Prevent unauthorized access –** Protect your device against un-authorized access by locking it whenever it's not in use. Require a passcode to unlock it and make sure you select a non-trivial passcode, which is difficult to guess. Contact your system administrator immediately, if the device has been lost or stolen.

  Go to the Android settings menu to configure your screen lock. On Android devices the exact path to the menu item for configuring the screen lock differs between Android manufacturers and across Android OS version, but it can usually be found by navigating to a path similar to: "*Settings/Security & location/Screen Lock*"

4 Provisioning

4.1 Configuration

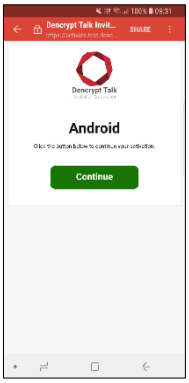
Provisioning is the process of first-time configuration and activation of the Dencrypt Talk application and consists of two steps:

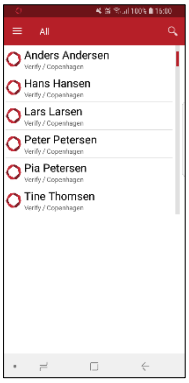
1. Installation of the Dencrypt Talk application.
2. Configuration of user credentials, server system domain, client certificates.

The application is made available by the system administrator through the organisations MDM system. The user must accept the installation request to complete the installation. Notice, that the application's functionality is restricted until the provisioning process has been successfully completed.

The provisioning process is a follows:

1. The system administrator will create the user on the Dencrypt Server System and provide an invitation email with an activation link (URL) shown as a green "Activate" button.
2. The end-user taps the activation link, which activates a web browser. The user may prompted to select which application to use for this type of link. Select Dencrypt Talk. If prompted about whether or not to always use Dencrypt Talk for this type of link, select "always". Furthermore, if this is the first time the Dencrypt Talk is opened, the user will be requested to give permissions to access the microphone, phone, and storage. These permissions are required for Dencrypt Talk to work. Please see section 4.2 for more information about the required permissions.
3. Dencrypt Talk opens to configure the account. This process may take a couple of minutes.
4. When setup is completed, the user is presented with a small guide. After reading and swiping through the guide, the Dencrypt Talk phonebook will appear. Dencrypt Talk is now ready for use.





Notice:

The invitation email shall be delivered in a secure way using encrypted emails through a mail server controlled by the organisation. If the invitation link is delivered in any other way, do not activate the link and contact your system administrator.

The activation link can only be used once and will expire after limited time period. Contact your system administrator, if provisioning is unsuccessful.

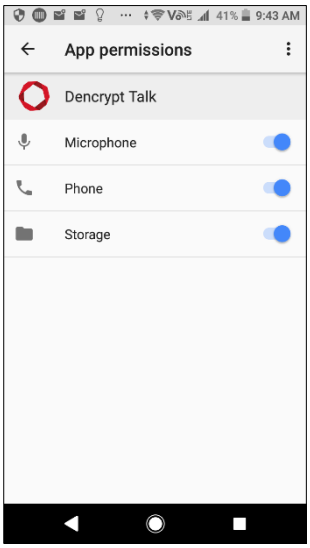
4.2 Permissions and notifications

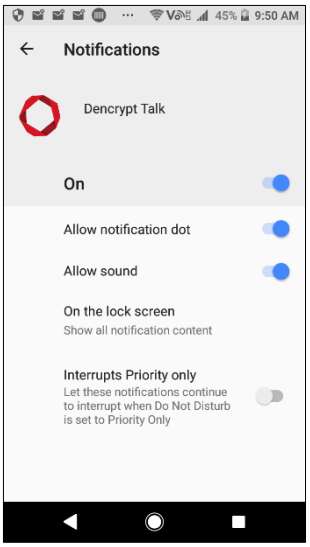
The first time the Dencrypt Talk application is launched the user will be asked (and required) to allow access to the microphone, phone, and storage. These permissions are required to enable voice communication, to react when there's an incoming GSM/LTE calls, and for storing app-related files on the device. The standard wording used by the Android OS to describe the requested permsissions is very broad and does not specify what the Dencrypt Talk app is specifically using the permsions for. To be clear, the Dencrypt Talk application:

- will **not** be used to access any photos, media, or other files that are not generated by the app itself
- will **not** be used to make or administer GSM/LTE phone calls

Permissions can be verified from: *Settings/ Apps & notifications / App info/ Dencrypt Talk / Permissions* and shall be similar to the left figure below.

Notifications shall be enabled to receive incoming calls, when the app is not running. Notifications can be verified from: *Settings/ Apps & notifications / App info/ Dencrypt Talk / Notifications and shall be similar to the right figure below.*





IMPORTANT – don't forcefully kill Dencrypt Talk:
If Dencrypt Talk is forcefully killed, the Android OS will prevent any incoming calls from being received until the user restarts Dencrypt Talk.
Both the Android OS and the user can trigger an app to be force killed. The Android OS may do it e.g. if the app uses too much battery. The user may do it explicitly from the Android settings menu or – on some devices – simply by swiping an app from the app history.
The threshold used by the Android OS to decide when an app should be force killed varies across different Andoid OS versions and brands. Therefore, Dencrypt Talk offers an option to enable battery saving, which can be done by putting a checkmark next to the "Settings / Battery / Minimize Battery Usage" option. However, this still requires the user to refrain from manually force killing the app.

5 Making secure connections

The Dencrypt Talk application supports encrypted voice call and encrypted live chat. Secure voice calls may be used when alone and in locations without acoustic coupling (see below). Secure live chat may be used as an alternative in public areas or in areas where an acoustic coupling is possible. Ensure that no one can observe the screen while exchanging encrypted chat messages.

A number of precautions shall be observed prior to making a secure voice call or secure live chat:

5.1 Avoid acoustic coupling

It is not recommended to use encrypted voice calls in hotel rooms and the like, which cannot be considered secure. Never exchange classified information through the Dencrypt Talk application when other unclassified telephones, radio transmitters or similar are being used in the immediate proximity. Locations, which are well suited to making calls, may be public spaces where the caller's presence has not been pre-arranged. Use secure live chat as an alternative way of communicating in areas, where acoustic coupling is possible.

5.2 Other precautions

- **Avoid using wireless headsets** - the data connection from the mobile device(s) to the headset is not protected by the Dencrypt Talk application. Use only wired headsets.
- **Avoid using handsfree car system –** the data connection from the mobile device(s) to the handsfree car system is not protected by the Dencrypt Talk application. Disable Bluetooth to prohibit the mobile device from automatically establishing a connection to the handsfree car system.
- **Avoid using loudspeaker -** Use the Dencrypt Talk loudspeaker with care and only in rooms, which are protected from acoustic coupling.
- **Don't take screenshots –** Screenshots are saved unencrypted on the devices and are not deleted at call terminations.
- **Don't use copy/paste –** Don't use copy/paste functionality during chat.
- **Don't use voice recordings –** Voice recordings are saved unencrypted on the devices and are not deleted at call terminations.

5.3 Use of secure live chat

A secure live chat can be established in two ways:

1. During an ongoing voice call with audio transmitted (section 5.4) or
2. As a chat only connection with constantly muted audio (section 5.5)

Option 1 is intended to supplement a secure voice call with secure text messaging. Further, it may be used to maintain a secure communication in cases where the voice quality is deteriorated due to poor network conditions. Option 1 shall not be used if there is a possibility for acoustic coupling.

Option 2 is intended to be used in locations where acoustic coupling may be possible.

Always ensure that the device screen is not visible to others during a secure live chat.

5.4 Establish a secure voice call

Prior to establishing a secure call: Ensure that you are alone and that there are no possibilities for acoustic coupling (see section 5.1).

Open the Dencrypt Talk application by tapping the icon. The procedure for establishing a secure call is shown in Figure 3 and contains these steps:

1. Find your contact in the phonebook and open the call screen.

2. Select secure voice call using the green call button.
3. The call will be established. Screen reads: *Dialling*. If answered, the call will be secured.
4. When the connection has been secured, a 4-character security code appears, which shall be identical on both devices. The security code shall be exchanged orally with the calling party immediately after the secure connection has been established.
    1. Say the characters, which are displayed under "say" and confirm with your peer that these are identical to the character shown under "hear"on his/hers device.
    2. Confirm that the characters under "hear" are identical to the characters said by the peer.

    This confirms that the process of securing the call has not been compromised.

    Important
    - If the codes are not identical, it may be an indication that the call has been compromised.
    - If the counterpart does not sound as expected, someone may have gained unauthorized access to the device.

    Terminate the call immediately and contact your system administrator!
5. Secure live chat during an ongoing call is possible by using the blue chat button.
6. The call is terminated by tapping the red hangup button. This will permanently delete the encryption keys and chat data.

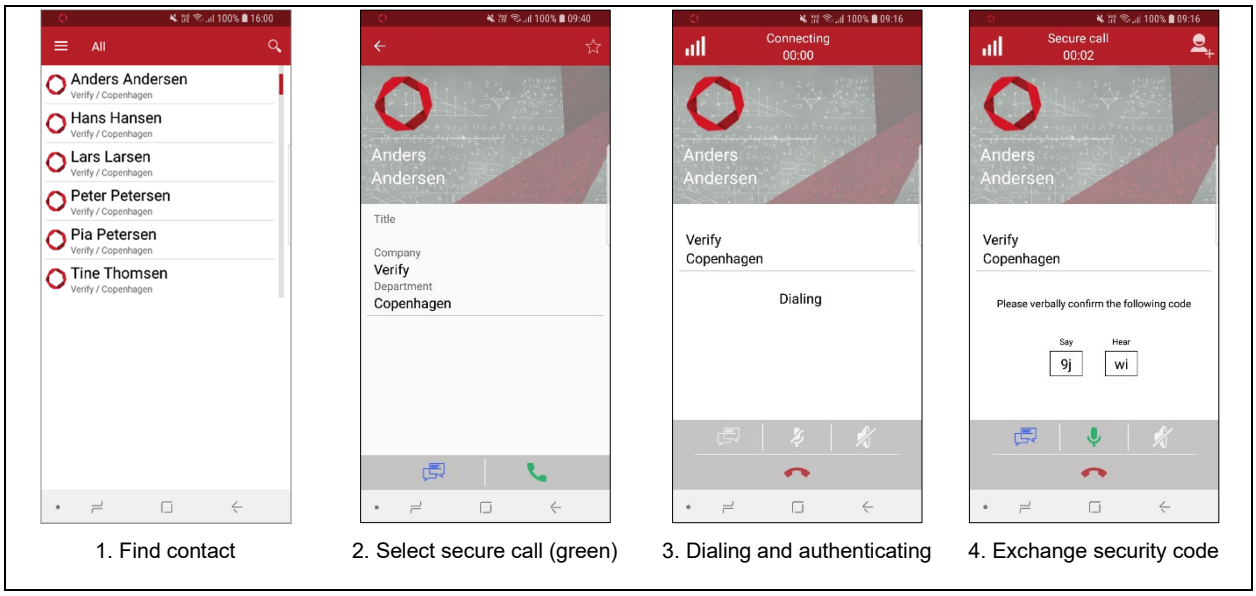


Figure 3. Procedure for establishing a secure voice call

5.5 Establish a secure live chat

A secure live chat can be established during a secure audio call (see section 5.4) or as a chat only connection without audio as described below.

Prior to establishing a secure live chat: Ensure that no one can observe your screen.

To establish a secure live chat connection without audio, open the Dencrypt Talk application by tapping the icon. The procedure for establishing a secure live chat is shown in Figure 4 and contains these steps:

1. Find contact in phonebook and open the call screen.

2. Select secure live chat using the blue chat button.

3. A connection will be established. Screen reads: *Dialling*. If answered, the connection will be secured. Screen shows: *Authenticating*

Notice: For secure live chat without audio there is no exchange of security code[1].

4. The secure live chat is terminated by tapping the white arrow in the upper, left-hand corner. This will permanently delete the encryption keys and chat data.

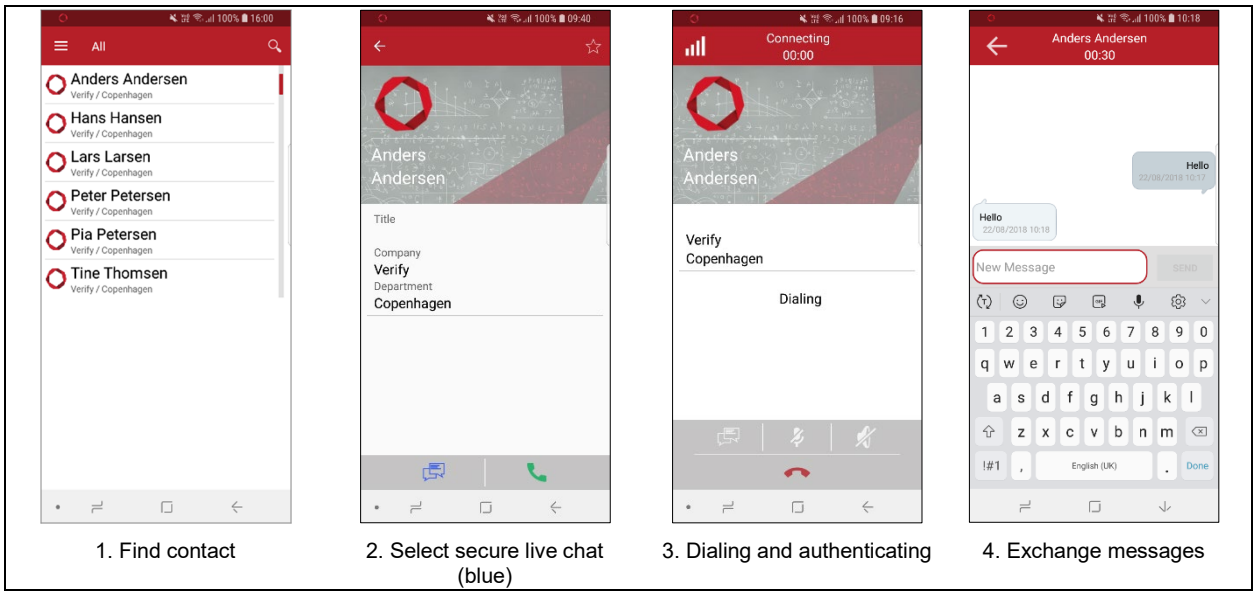


Figure 4 Procedure to establish a secure live chat.

5.6 Establish a secure group call

Group calls are established by adding participants to an existing call one-by one. Only the initiator of the first established call can add persons to the group call. A secure voice connections is established from the initiator to each of the parties in the group call. Secure live chat is not available during a group call.

Follow these steps to establish a secure group call:

1. Establish a secure call as described in Section 5.4.
2. Tap the '+'-button in the upper right corner of the call screen to invite additional persons to the call.
3. The phonebook opens and the new participant can be selected and called. The already established connections are paused.
4. When the connection has been secured, a 4-character security code appears, which shall be identical on both devices. The security code shall be exchanged orally with the calling party immediately after the secure connection has been established.
    a. Say the characters, which are displayed under "say" and confirm with your peer that these are identical to the characters shown under "hear" on his/hers device.

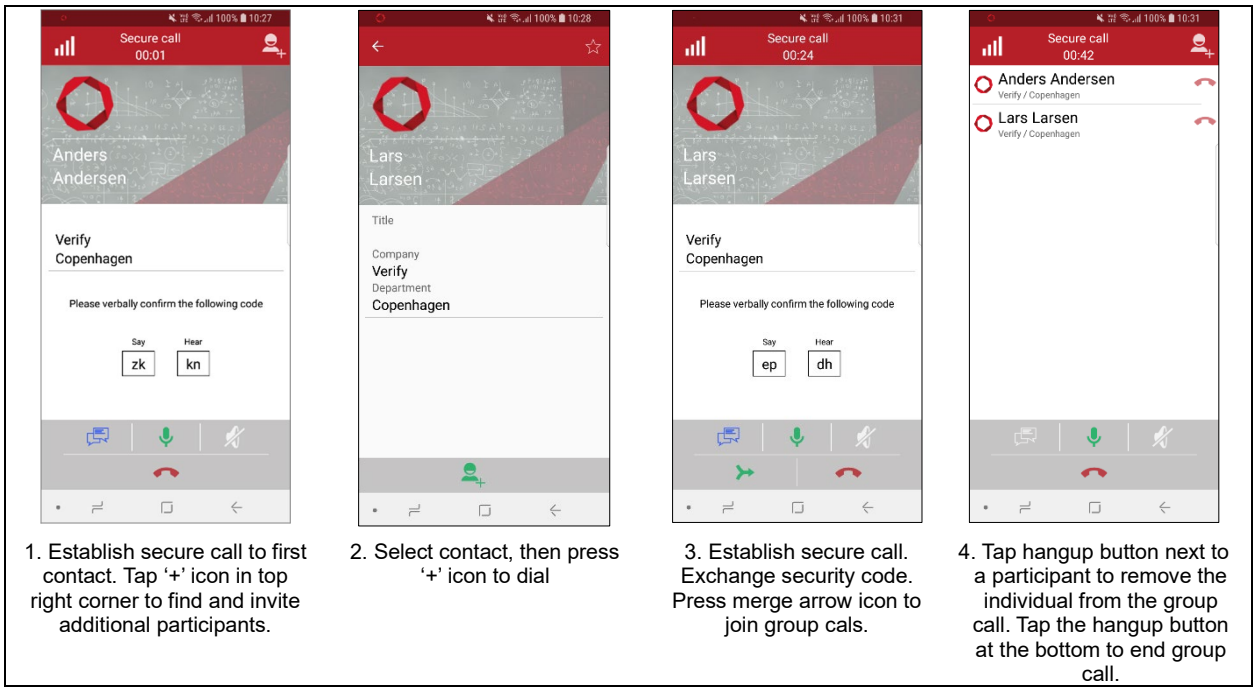
[1] For a secure live chat there is no voice data transmitted and hence no secure way to exchange a security code.

b. Confirm that the characters under "hear" are identical to the characters said by the peer.

This confirms that the process of securing the call has not been compromised.

> **Important**
> - If the codes are not identical, it may be an indication that the call has been compromised.
> - If the counterpart does not sound as expected, someone may have gained unauthorized access to the device.
>
> Terminate the call immediately and contact your system administrator!

5. Tap the green merge button to merge the calls.
6. Repeat steps 2 through 5 for each new participant.
7. The call is terminated by tapping the red hangup button. This will permanently delete the encryption keys.



1. Establish secure call to first contact. Tap '+' icon in top right corner to find and invite additional participants.
2. Select contact, then press '+' icon to dial
3. Establish secure call. Exchange security code. Press merge arrow icon to join group cals.
4. Tap hangup button next to a participant to remove the individual from the group call. Tap the hangup button at the bottom to end group call.

Figure 5 Procedure for secure group calls

5.7 Incoming calls

Incoming calls are alerted using push notification, which will automatically open the Dencrypt Talk application and show the incoming call screen. See section 4.2 for important information about how to ensure that you receive a notification when an incoming call is received.

Answering an incoming call is shown in Figure 6:

1. Tap the green Dencrypt Talk answer button
2. When the connection has been secured, a 4-digit security code appears. The security code shall be identical on both devices and exchanged orally with the calling party.

Important

- If the codes are not identical, it may be an indication that the call has been compromised.
- If the counterpart does not sound as expected, someone may have gained unauthorized access to the device.

Terminate the call immediately and contact your system administrator!

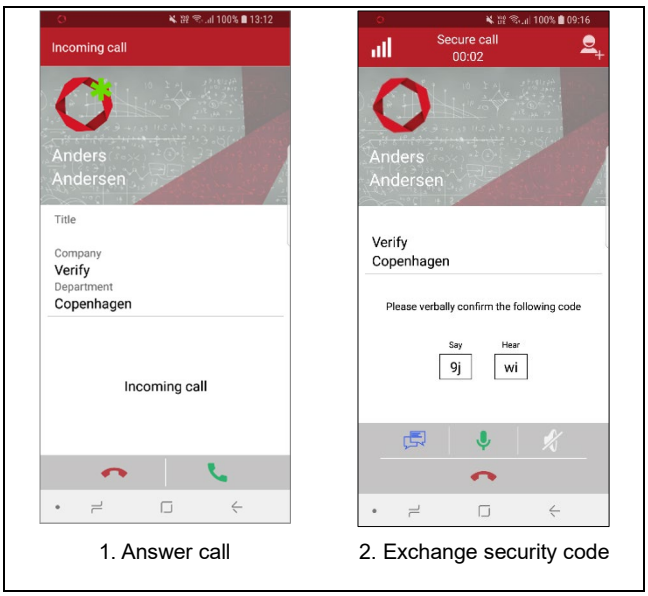


Figure 6 Procedure for answering secure call

6 Settings

Settings are accessed from the main menu (≡) and used to view information about and customize the behavior of the mobile client. The options are lised in Table 1.

Table 1 Settings.

Category	Setting	Description	Default value
Account	Logins	List system accounts and registration status.	-
	Manual Provisiong	Offers a way to manually enter a provisioning link to be used for provisioning the Dencrypt Talk application	-
Phonebook	Preferred phonebook	Defines whether phonebook is displayed when opening the application	All
Energy Saving	Battery	Allows the user to enable "Minimize Battery Usage", which will cause the app to automatically shut down when not in use and backgrounded. If not enabled, the app will run as a background service that maintains a constant connection to the Dencrypt Server System.	Disabled
	Keep screen on during call	When enabled, the screenlock will not be activate during a call.	Disabled
Audio	Enable Echo Cancellation	If enabled, the Dencrypt Talk app will use software echo cancellation if no hardware supported echo cancellation is available.	Disabled
	Microphone Gain	Allows adjustment of the microphone gain. This is useful if the default microphone gain, which varies across devices, makes it hard for peers to hear what is said. Higher values mean more gain.	0.0
	Playback Gain	Allows adjustment of the speaker gain. This is useful if the default speaker or earpiece gain makes it hard to hear what peers are saying. Higher values mean more gain.	0.0

7 Version number

The app version can be examnined from Settings by scrolling to the buttom as illustrated in Figure 7.

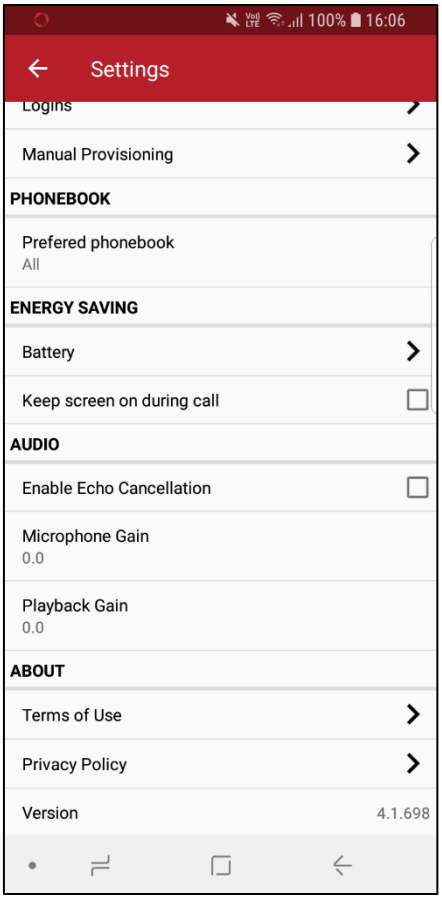


Figure 7 App version number

8 Reporting security incidents

Report security incidents to your system administrator. The following events shall be reported immediately:

- Device lost, stolen or compromised.
- Security code do not match.
- Invitation email received through a non-secure email connection.
- Suspicion that the counterpart may not be the expected person.
- Suspicion that the call has been compromised in any other way, i.e. through acoustic coupling.

Please provide the version number of the App when reporting issues.

9 Error and information messages

This section lists possible error/information messages and possible required user actions.

9.1 Provisioning

Type	Message	Trigger	User actions
Error	Invalid provisioning The provisioning data are invalid	The user attempted to provision the app using an invalid provisioning link.	Contact your system administrator
Error	Invite Error <ErrorCode> <ErrorText> Please contact administrator for a new invite	The user attempted to provision the app but the provisioning process failed.	Contact your system administrator and report this error because it might be a security incident. Your administrator might request you to provide your invite mail. Some operators may truncate the invite SMS.
Error	Invite Error Please contact administrator for a new invite. (error code: <ErrorCode/ErrorText>)	The user attempted to provision the app but the provisioning process failed.	Contact your system administrator and report this error because it might be a security incident. Your administrator might request you to provide your invite mail. Some operators may truncate the invite SMS.
Error	Registration The account is already installed on this device. Error code: R04	The user attempted to provision the app using an invite for a user account that was already provisioned.	The account was already installed on your device, so trying to provision the same account once more would have no effect. No further action required.
Error	Invite Error The account data are invalid. Error code: Rxx	The user attempted to provision the app using invalid account information.	Contact your system administrator and report this error because it might be a security incident. Your administrator might request you to provide your invite mail. Some operators may truncate the invite SMS.
Error	Invalid provisioning The provisioning data are invalid	The user attempted to provision the app using an invalid invitation link (wrong domain, protocol, or content)	Contact your system administrator and report this error because it might be a security incident. Your administrator might request you to provide your invite mail. Some operators may truncate the invite SMS.
Info	Setup Confirmation Dencrypt Talk will be set up for user X on server Y	Provisioning for user X on system Y was successful. The associated account will be created and configured.	None

9.2 Phonebook and settings

Type	Message	Trigger	User actions
Info	User not accessible It is not possible to see the selected user, because you can not contact this user any more.	User taps a contact from the phonebook or history view.	None

9.3 Secure call and -chat

Type	Message	Trigger	User actions
Error	Cannot make secure call Another app is using the microphone. Please stop that app in order to initiate a secure call	User tries to make a call	Stop all apps that is currently using the microphone or wait for it to stop using the microphone. Then make the secure call.
Error	Not possible The maximum number of participants have been reached for this call.	User tries to add another group call participant.	Call additional participants separately, hang up one of the other participants prior to adding the new one, or (if possible, and there's no acoustic coupling) make room for additional participants by having two or more exisiting participants share a single phone.
Error	Call failed It is not possible to call the user, because connection to the server has been lost.	User tries to initiate a secure call while there's no connection to the server	Check connectivity: • Make sure flightmode is not enabled (if possible). Calls cannot be made while flightmode is enabled. • Wait 1 minute to see if the problem can be automatically resolved • Disable wifi and enable 3G/LTE data • Disable 3G/LTE data and enable wifi • If problem persists, contact your system administrator.
Error	Cannot make secure call Please terminate GSM call	User tries to initiate a call while an existing (insecure) voice call is active.	Wait for the existing GSM call to finish before trying to establish a secure call.
Error	Cannot start secure chat Please terminate GSM call	User tries to initiate a chat while an existing (insecure) voice call is active.	Wait for the existing GSM call to finish before trying to establish a secure chat.
Info	Call Paused Your call has been put on hold, please wait	The user at the other end has paused the call (e.g. he accepted an incoming GSM call, or he is in the process of adding another participant to the secure call)	Wait for the user at the other end to resume the call.
Info	Call declined	The user tries to make a call, which is declined by the user at the other end.	Try again later.

Type	Message	Trigger	User actions
Info	User not found	User attempts to call another user, whom the server cannot find (e.g. due to a recent change of the user's call permissions).	Try again later or contact your system administrator.
Info	Incompatible media parameters	User attempts to make a call. There was a technical issue establishing the call.	Make sure your Dencrypt Talk app is up-to-date. If problem persisits, contact your system administrator.
Info	No Answer	User attempts to make a call. The user at the other end didn't pick up.	Try again later.
Info	User busy	User attempts to make a call. User at the other end is already in another call.	Try again later.
Info	The user is currently not available	User attemtps to make a call. Server couldn't reach user at the other end.	Try again later.

9.4 Other messages

Type	Message	Trigger	User actions
Error	System notification There is no connection to server: X.Y.Z	User clicks warning sign on title bar.	Check connectivity: • Make sure flightmode is not enabled (if possible). Calls cannot be made while flightmode is enabled. • Wait 1 minute to see if the problem can be automatically resolved • Disable wifi and enable 3G/LTE data • Disable 3G/LTE data and enable wifi If problem persists, contact your system administrator.
Error	Dynamic Encryption Error Incompatible Dynamic Cipher versions in call. Please hang up	The Dynamic Encryption version used by peer does not match version used by this device	Hang up. Update your app and retry. If problem persists, contact your system administrator.

10 Change History

Revision	Date	Author	Comment
1.0	2018-08-27	JH	Released for version 4.1