



Dencrypt Communication Solution

Operational User Guide

Dencrypt Connex for Android

v. 1.10



May 19, 2025
Public

Contents


- 1 Introduction 3**
- 2 Security instructions 4**
 - 2.1 General security measures 4
 - 2.2 Avoid acoustic coupling 4
 - 2.3 Avoid screen exposure 5
 - 2.4 Other security recommendations 5
- 3 Getting started 6**
 - 3.1 Installation 6
 - 3.2 Activation 6
 - 3.3 Import account 8
 - 3.4 Set permissions 9
 - 3.5 Revoked application 11
- 4 Using Dencrypt Connex 13**
 - 4.1 Favourites 14
 - 4.2 Recents 14
 - 4.3 Contacts 15
 - 4.3.1 Phonebook views 16
 - 4.4 Conferences 17
 - 4.4.1 Static conferences 17
 - 4.5 Messages 18
 - 4.5.1 Chatroom options 19
- 5 Making a secure call 22**
 - 5.1 Voice quality 24
 - 5.2 Group calls 25
 - 5.3 Incoming calls during a secure call 27
 - 5.4 Incoming secure calls 28

6	Sending a secure message	30
6.1	Create a direct chat room	30
6.2	Create a topic chatroom	30
6.3	Sending a secure message	32
6.3.1	Unable to decrypt message	32
6.4	Message context menu	32
6.4.1	Message delivery status	33
6.4.2	Reply to message	34
6.4.3	Copy messages	35
6.4.4	Edit message	35
6.4.5	Emoji reaction	36
6.5	Sending attachments	37
6.6	Push-to-Talk	38
6.7	Location sharing	39
6.8	Message expiry	40
7	Settings	42
	Appendices	44
A	Dencrypt Communication Solution	44
A.1	End-2-end encrypted VoIP calls	44
A.2	End-2-end encrypted instant messaging	45
A.3	Authenticated connections	45
A.4	Encryption keys	46
A.5	Secure phonebook	46
A.6	Push notifications	46

Version

This guide applies for:

- Dencrypt Connex v. 1.10 for Android devices.

The version number can be verified from the Settings menu by tapping the -symbol in the top-right corner on the Contacts screen. See Figure 38.

Support

Contact your local support for assistance and in case of security incidents.

Dencrypt support	
Phone	+45 72 11 79 11
Email	support@dencrypt.dk

1 Introduction

Dencrypt Connex is an application for making encrypted voice calls, videocalls and for the exchange of encrypted instant messages from:

- Android devices

It uses the patented Dynamic Encryption technology to apply state-of-the-art, end-to-end encryption between devices.

This guide is intended for end-users of the Dencrypt Connex application and provides instructions to operate and use the application securely.

The end-users of the Dencrypt Connex application shall have familiarized themselves with this document as given in Table 1 and have received instructions from the system administrator prior to taking the product into use.

Dencrypt Connex support selected local languages. However, this guide and screenshots are shown in the English language.

Section 2	Security instructions	Essential
Section 3	Getting started	
Section 4	Using Dencrypt Connex	User guidance
Section 5	Making a secure call	
Section 6	Sending a secure message	
Section 7	Settings	
Appendix A	Dencrypt Communication Solution	For reference

Table 1: Reading Guide

2 Security instructions

These security instructions shall be read and understood before taking the Dencrypt Connex application into use.

2.1 General security measures

Some precautions must be observed to use the application in a secure way and to avoid disclosure of confidential information. Please observe the following before taking the application into use.

Organizational security policies Before taking Dencrypt Connex into use, the security policies and instructions for secure usage shall have been received and understood. Be aware of the classifications allowed to be exchanged using Dencrypt Connex .

Server system security The system administrator is responsible for the daily and secure operation of the Dencrypt Server System . In case of critical security incidents or unresolved vulnerabilities, the system administrator may prevent communication between specific users or may take the entire system out of operation until the issues have been resolved. In such cases, it may not be possible to establish secure communication at all or with specific users.

Secure delivery Dencrypt Connex shall only be received from Google Play or a Mobile Device Management system.

Device security The system security depends on a correct and secure operation of the device and the operating system, and there are no critical side-effects. Therefore, the Dencrypt Connex application and the operating system 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 a certain user or make the entire system unavailable until the issue has been resolved.

Benign applications The Dencrypt Connex application protects information during the data transmission and when stored on the device. It does not protect against malware intercepting audio, video, or text before encryption. Therefore, only benign apps shall be installed on the device. Be aware of applications, which make use of the microphone, perform screenshots, listen to the earpiece or speaker or capture keyboard strokes. Contact your system administrator for advice.

Single user device The phonebook is personal and dedicated to a specific end-user. Therefore, the device is personal and shall not be shared.

Prevent unauthorized access Protect your device against unauthorized access by always enabling a passcode or biometric login. In case of lost or stolen devices, contact your system administrator immediately.

2.2 Avoid acoustic coupling

It is not recommended to use encrypted voice or video calls in hotel rooms and like, which cannot be considered secure. Never exchange classified information through the Dencrypt Connex application when other unclassified telephones, radio transmitters, or similar are being used in immediate proximity.

Locations that are well suited to making calls may be public spaces where the caller's presence has not been pre-arranged. Using secure messaging is an alternative communication in areas where an acoustic coupling is possible.

2.3 Avoid screen exposure

Consider the surroundings when using Dencrypt Connex for secure video calls and messaging to ensure that the screen can not be observed by others. Be aware of the location of windows and cameras.

2.4 Other security recommendations

- **Avoid using wireless headsets** - The data connection from the device to the headset is not protected by Dencrypt Connex . Use wired headsets as an alternative.
- **Avoid using hands-free car systems** - The data connection from the device to the hands-free car system is not encrypted. Disable Bluetooth to avoid automatic connection and use wired headsets as an alternative.
- **Avoid using loudspeaker** - Use the Dencrypt Connex loudspeaker only with care and in locations that are protected from an acoustic coupling.
- **Don't take screenshots** - Screenshots are saved unencrypted on the devices and are not deleted when the app is closed. Screenshots may be blocked by the system administrator.
- **Don't use copy/paste** - Don't use the copy/paste functionality during messaging. Copy/paste-functionality may be blocked by the system administrator.
- **Don't use voice recordings** - Voice recordings are saved unencrypted on the devices and are not deleted when the app is closed.
- **Avoid auto-correction and predictive text features** - Avoid using keyboards that include autocorrection or predictive text features. It is recommended to disable spell-checking and predictive text from the settings menu.
- **Avoid using apps with speech recognition** - Avoid using applications, that makes use of speech recognition features, such as speech-to-text applications.

3 Getting started

A few steps are required by the end-users to get started using Dencrypt Connex .

1. Installation
2. Activation
3. Set permissions

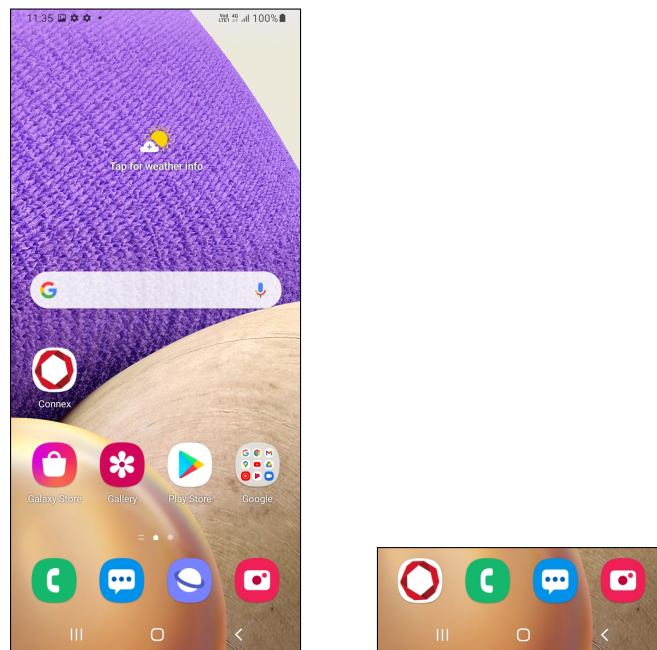
3.1 Installation

Dencrypt Connex is installed via:

- Public Google Play Store for direct installation on end-user devices.
- Google Enterprise, for installation to end-user devices via an MDM.

Links to Dencrypt Connex on the public app store are available from the Dencrypt webpage: <https://www.dencrypt.dk/downloads>

Once the app is installed, it is launched by tapping the Dencrypt Connex icon. For quick access, the icon can be dragged to the menu bar at the bottom of the screen as seen in Figure 1.



(a) Dencrypt Connex on the home screen. (b) Dencrypt Connex icon in the menu bar.

Figure 1: Home screen

3.2 Activation

Once installed, the Dencrypt Connex is unconfigured and shall be activated before it is taken into use. The system administrator is required to create a user account on the Dencrypt Server System and provide an activation

link.

The activation link is time-limited and can only be used once, and it comes in the form of a weblink (URL) or a QR code. The activation link may not be disclosed and shall be delivered in a secure way. The following options are possible:

- Email containing a weblink, send to the device.
- Email or physical letter containing a QR code to be scanned by the camera application.
- SMS containing a weblink sent to the device. ¹

Emails shall be encrypted or transmitted using encrypted connections.

Activating the link will start the provisioning process to configure the Dencrypt Connex with certificates and credentials to connect to the server system and download the phonebook. Only when the activation process has successfully completed the Dencrypt Connex is ready for use.

Activation process

- Step 1: The system administrator creates a user account on the Dencrypt Server System and provides an invitation message containing the activation link to the end user (Figure 2a).
- Step 2: The user activates the link by tapping the weblink or by scanning the QR-code using Dencrypt Connex (Figure 2b) or the camera application. The user may be prompted to open the link in the Dencrypt Connex .
- Step 3: The Dencrypt Connex opens to configure the account. This may take 1-3 minutes. **Do not close the app during the activation.**
- Step 4: Once completed, the Dencrypt Connex will open and is now ready for setup.
- Step 5: Two options for account setup is possible as described in [Import account 3.3].
- Step 6: Once completed, the app will request permissions to the device resources for full functionality. Tap Allow for each permission. See [Set permissions 3.4].
- Step 7: Dencrypt Connex will connect to the server system to download the phonebook.
- Step 8: Dencrypt Connex is now ready for use.
-

¹SMS activation is not recommended for security reasons.

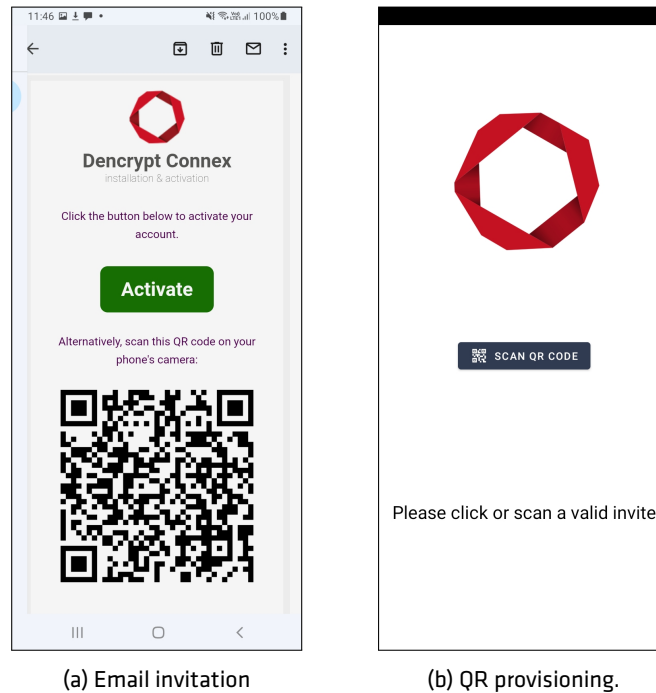




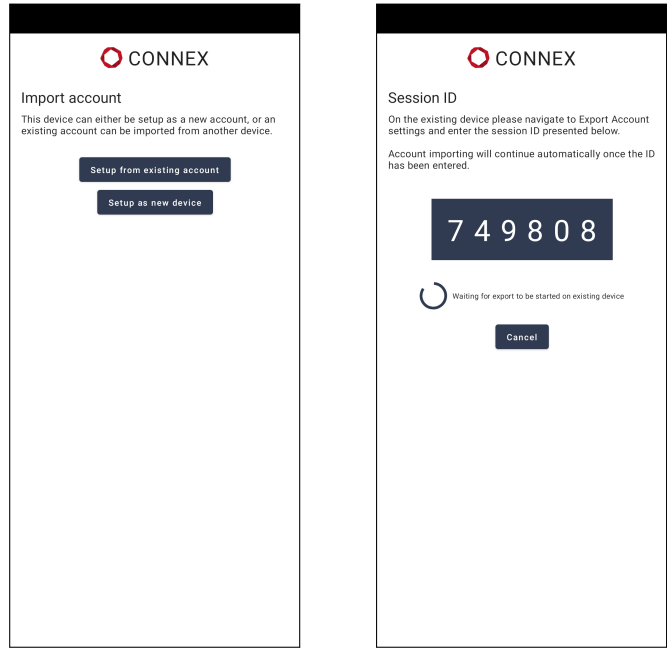
Figure 2: Invitations and activation.

3.3 Import account

During the account setup, it is possible to either setup the device as a new device or from an existing account (Figure 3a). If Setup as new device is chosen, the account will open as new with no message or call history. If Setup from existing account is chosen, a session ID is shown on the receiving device (Figure 3b). The migration is then initiated by exporting the account from the device with the existing account:

Exporting existing account

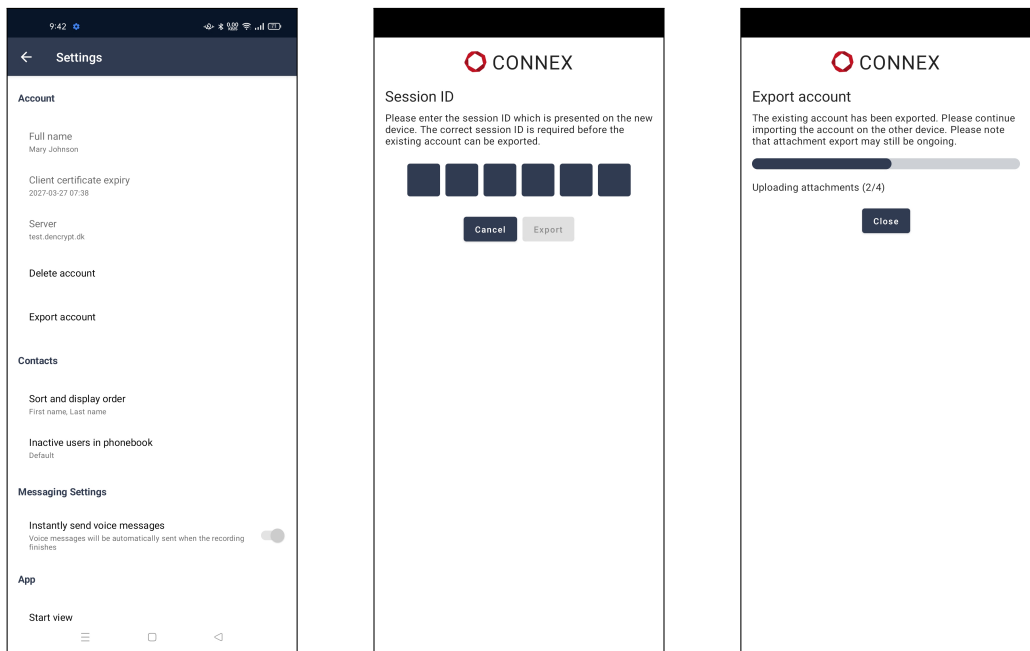
- Step 1: Navigate to the Export Account settings, by tapping the -symbol in the top-right corner on the Contacts screen, followed by the -icon to open settings.
 - Step 2: Tap Export account (Figure 4a).
 - Step 3: Enter the session ID from the receiving device and tap Continue (Figure 4b).
 - Step 4: The account is being exported. A progress bar shows the level of completion (Figure 4c).
 - Step 5: When the process is done tap Close.
-



(a) Import account options.

(b) Session ID.

Figure 3: Migration process for receiving device.



(a) Account settings.

(b) Enter Session ID.

(c) Progress bar for account export.

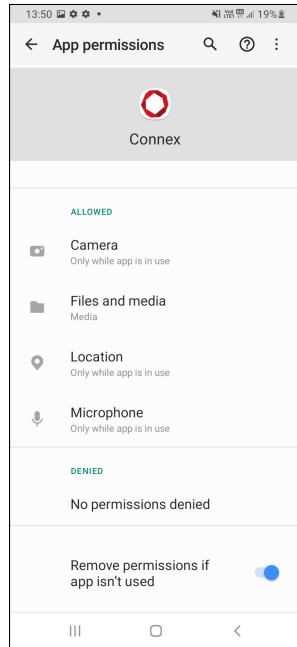
Figure 4: Migration process for device with existing account.

3.4 Set permissions

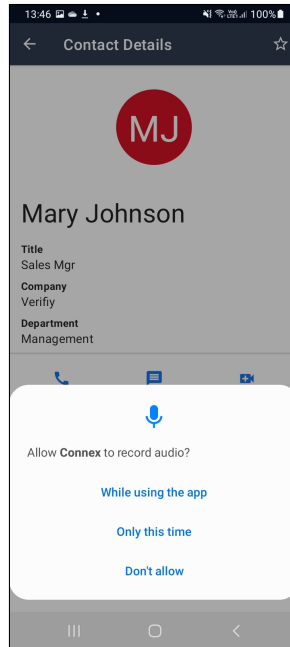
Dencrypt Connex requests access to some of the device resources. Permission to the microphone and notifications shall be granted to perform secure voice calls. For messaging, the requested permissions are optional but will limit the functionality of the app if not granted.

When Dencrypt Connex requires access to a restricted resource or actions, the user will be requested to grant permissions. App permissions can always be managed from the systems App Info menu for Dencrypt Connex .

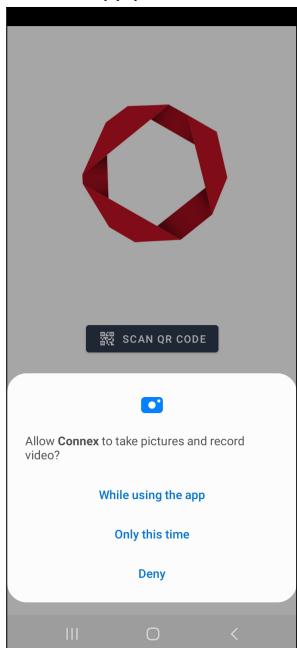
During the account setup, Dencrypt Connex will ask for permissions as listet in Table 2 and shown in Figure 5.



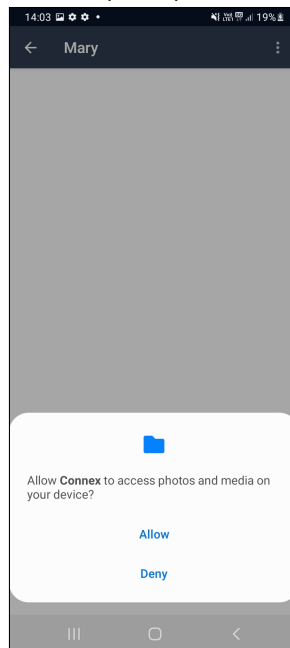
(a) App permissions



(b) Microphone permission.



(c) Camera permission.



(d) File access permission.

Figure 5: Permissions

Permission	Reason	
Camera	For scanning a QR-code invitation and for capturing images to attach to messages	Optional
Microphone	Required for voice calls.	Mandatory
Notifications	Required to alert for incoming calls and messages.	Mandatory
Location	Required to include GPS locations in messages.	Optional
Photo and media	Required to attach images and videos from library.	Optional

Table 2: Permission usage.

3.5 Revoked application



The system administrator may revoke the Dencrypt Connex access to the server system, which will result in a Security Issue message (Figure 6). This may happen if:

- The device has been reported lost or stolen, in which case the administrator will temporarily deactivate access.
- The account has been deleted, in which case access is permanently blocked.

In both cases, contact the system administrator to regain access to the services. The administrator may:

- Re-activate the device, in which messages and call history are preserved. This usually happens in case a lost phone is found again.
- Send a new invitation to provision the Dencrypt Connex app again, in which messages and call history are **NOT** preserved. Before using the new invitation, the account should be deleted:

Delete account

Step 1: Tap the -symbol in the top-right corner on the Contacts screen, followed by the -icon to open settings.

Step 2: Tap Account

Step 3: Scroll to the bottom and tap Delete account

Step 4: Provision Dencrypt Connex app again using the invitation received.

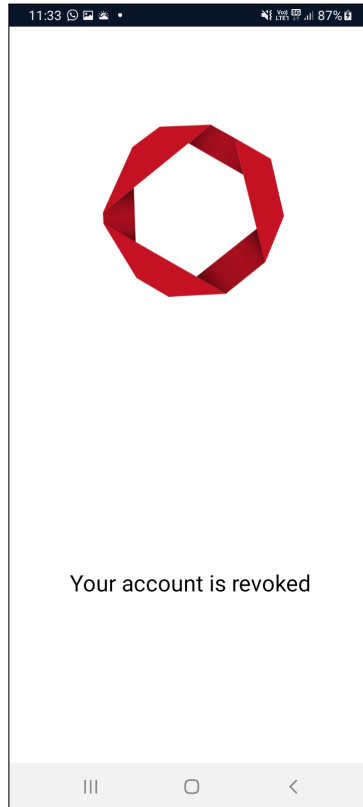


Figure 6: Revoked access to the server system.


4 Using Dencrypt Connex

Dencrypt Connex offers two main functionalities:

- Secure voice/video communication.
- Secure instant messaging of text and content (attachments).

The functionalities are accessible from the main screen. The icons in the menu bar at the bottom (See Figure 7) provide quick access to the following screens:

- Favourites: For quick access to selected contacts.
- Recents: For accessing the call history.
- Contacts: For accessing the entire phone book.
- Messages: For accessing the message inbox.

Settings are accessed from the -symbol on top-right corner of the Contacts screen (See Figure 7).

Dencrypt Connex launches per default with the Contacts screen. The launch screen can be set from: Settings →App →Start view (See section 7).

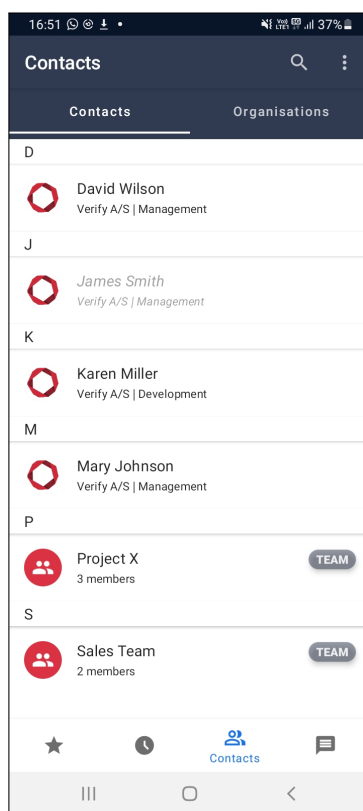


Figure 7: Contacts screen.

4.1 Favourites

The Favourites screen shows a contact shortlist created by the user (Figure 8a). Initially, the Favorite screen is empty. Contacts can be added to the Favourites screen by tapping the star icon found in the Contact Details (Figure 8b). The ★-icon is filled for favorite contacts.

A contact can be removed from Favorites by tapping the ★-icon again.

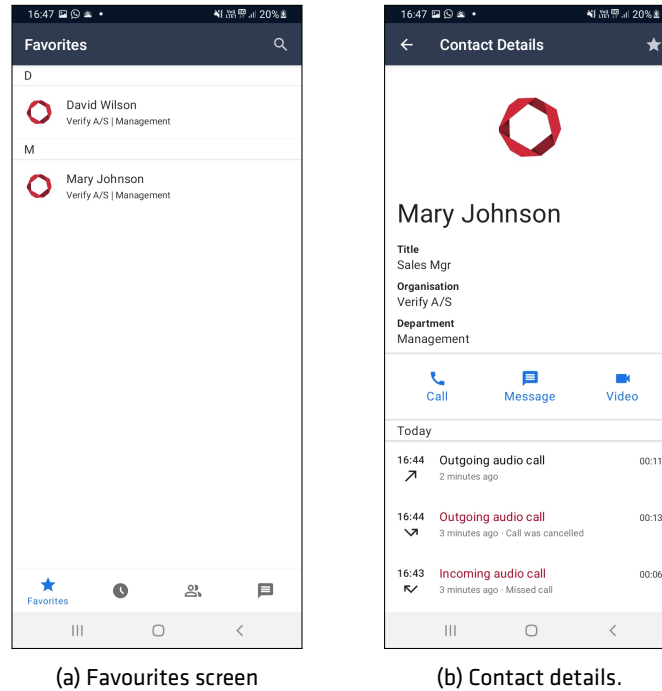
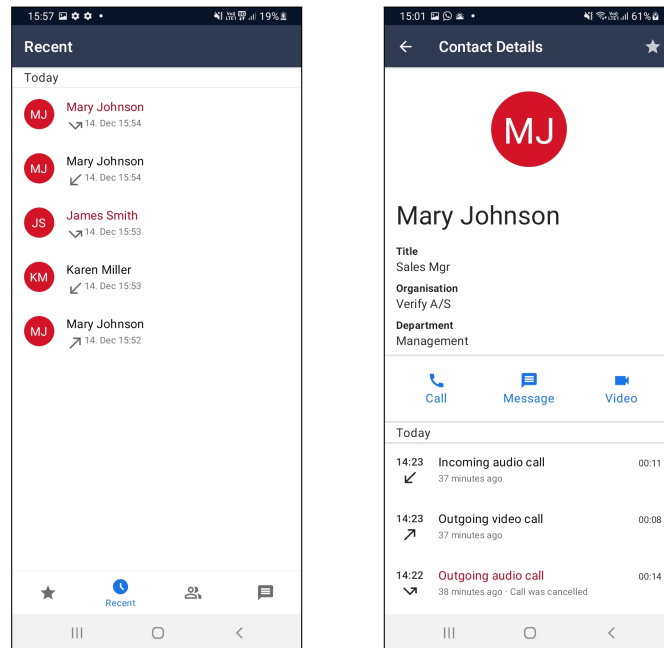


Figure 8: Favourites.

4.2 Recents

The Recent screen shows the call history in chronological order (Figure 9a). Tapping an entry will open the Call Details screen, which contains the call history for that contact (Figure 9b).



(a) Recents screen

(b) Recent call detail from contacts.

Figure 9: Recents.

4.3 Contacts

The Contacts screen shows the entire phone book consisting of individual contacts and team rooms (Figure 10a). The content of the phone book is centrally managed from the Dencrypt Control Center and is not editable from within the app.

Contacts are listed in alphabetic order, sorted by first name per default. Changing the sorting order can be done from the Settings menu. Locating contacts can be done in the following manners:

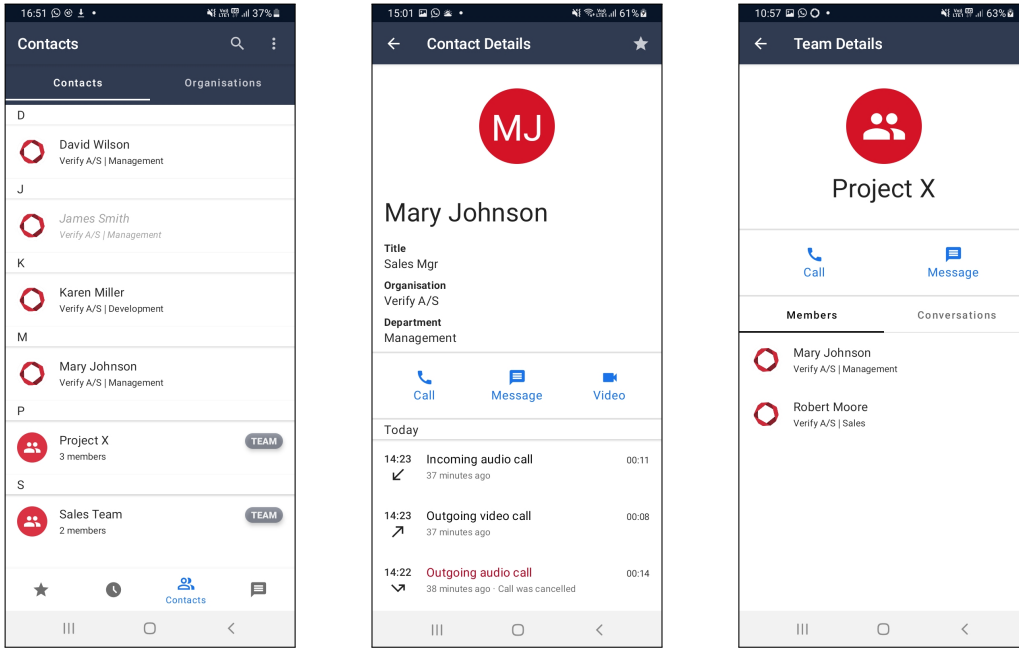
- Skip to a specific letter using the index on the right-hand side of the screen.
- Search for contacts via the search menu.
- Toggle between an All contact view or Organisation view by tapping the buttons above the list [Phonebook views 4.3.1].

Inactive contacts are indicated by grey coloring. An inactive contact is created on the system but may not have activated his/hers account yet, or has been deactivated by the system administrator. It is not possible to call or message an inactive contact. Display of inactive contacts can be enabled and disabled from the settings menu (See section 7).

Selecting a contact will open the Contact details (Figure 10b) and allow the user to start a secure call, a secure video call, or send a secure message. The Contact details screen also displays the recent call list.

Selecting a team room will open the Teamroom details (Figure 10c). This screen allows the user to list the members and/or exchange messages or start a group call with the team.

A contact can be added/removed as a Favorite by tapping the star icon.



(a) Contacts screen.

(b) Contact details.

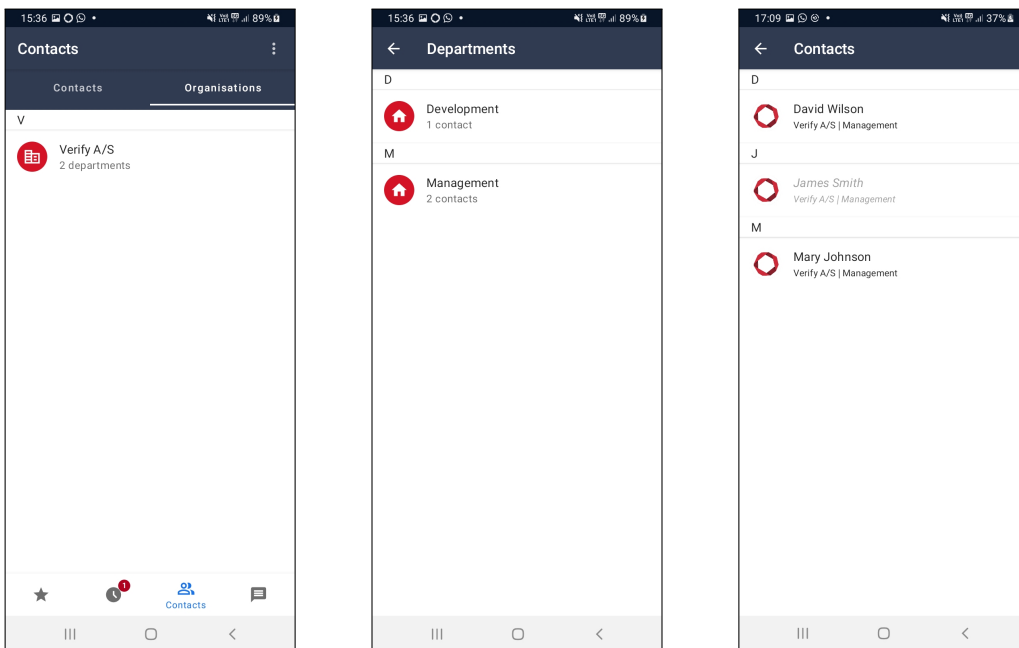
(c) Teamroom details.

Figure 10: Contacts.

4.3.1 Phonebook views

Two phonebook views are available:

- The Organization view structures the contacts by two levels: By organization and department (Figure 11).
- The Contacts view shows all contacts in a flat alphabetically ordered list (Figure 10a).



(a) First layer: Organization

(b) Second layer: Departments

(c) Contacts in departments

Figure 11: Contacts in organization view.

4.4 Conferences

The Conferences screen shows the conferences available to the user. The available conferences are centrally managed from the Dencrypt Control Center and are not editable from within the app.

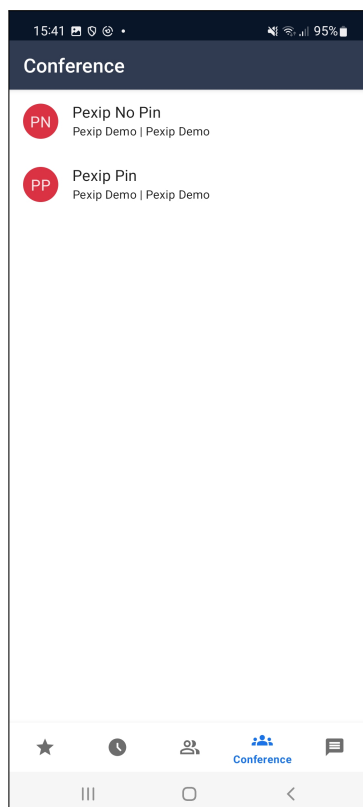


Figure 12: Conferences screen.

4.4.1 Static conferences

The static conferences are configured from the Dencrypt Control Center and do not require any additional information to join, other than an optional pin. Once a call is established, and a pin is needed, the user will verbally be prompted to enter it.

Before initiating a conference call, the user has the option to enable video.

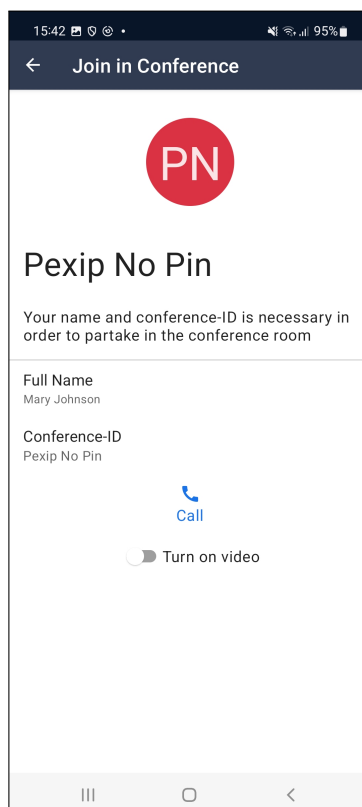


Figure 13: Conferences screen.


4.5 Messages


The Message screen is used for sending and receiving text messages and attachments, such as photos, videos, audio clips, files, and GPS location. The system administrator may limit the available choices for security reasons.



Three types of chatrooms are available:

- Direct chatrooms - for direct messaging with a single contact. The title of the message is set to the name of the contact and cannot be changed. There is only one Direct chatrooms per contact.
- Topic chatrooms - for group messaging or topic specific conversations. A title for the chatroom must be specified when creating a Topic chatrooms. It is possible to have a Direct chatroom and multiple Topic chatrooms with the same contact. Group messages are indicated by multiple avatars to the left of the room title (Figure 14a).
- Teamrooms - persistent chatrooms defined by the system administrator, who also manage the participants. Team rooms are usually created for departments, project teams, o.l. Team rooms are indicated with a TEAM label (Figure 14a).

The initial Messages screen shows a list of chatrooms containing ongoing conversations. Initially, the message inbox will be empty and shows only a placeholder text.

A user can start composing a new message, close the app and the text and attachments will be stored as a draft for the given conversation. When the user enters the conversation again the saved draft text and attachment will be restored. Conversations with such draft messages will presented with a small -icon in the inbox. Draft messages are local to the device and will not be synchronised to the user's other devices.

Tapping an entry (chatroom) will open up the messages in the conversation (Figure 17b). Tapping the -icon opens a menu for showing a list of participants, changing the chatroom title (not available for direct chatrooms), and pinning the chatroom to the top (Figure 14c).

From the chat room: Tap the -icon or -icon to call all chatroom participants. Video calls are only possible for chatrooms with a single contact.

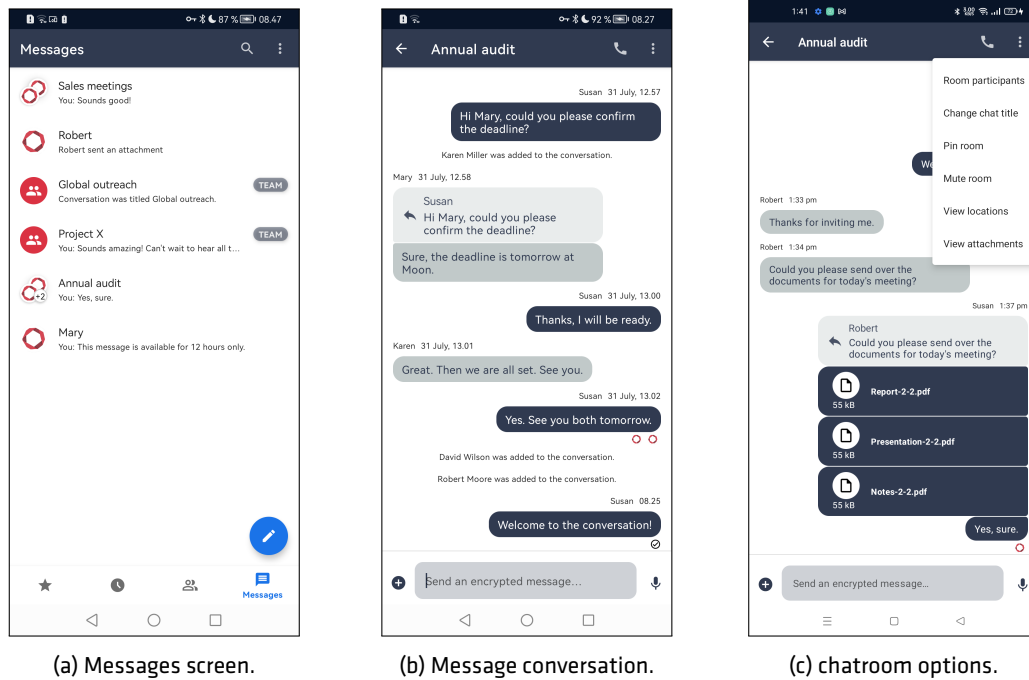
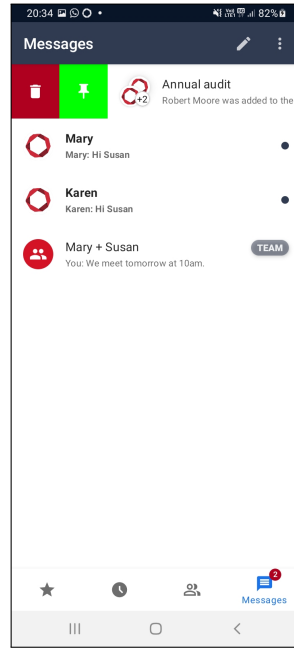


Figure 14: Messages

4.5.1 Chatroom options


Chatrooms can be deleted or marked as favorites (pinned). In the chatroom list: Swipe right on the chatroom title to reveal a hidden menu for deleting or pinning chatrooms. Favorite chatrooms are always shown at the top of the list. Mute room will prevent notifications from being displayed for the selected duration. Muted rooms can be identified by a small icon shown in the conversation topic. Rooms can be unmuted from the options menu Figure 14c.



(a) Chatroom options.

Participants can be added or removed from a topic chatroom:

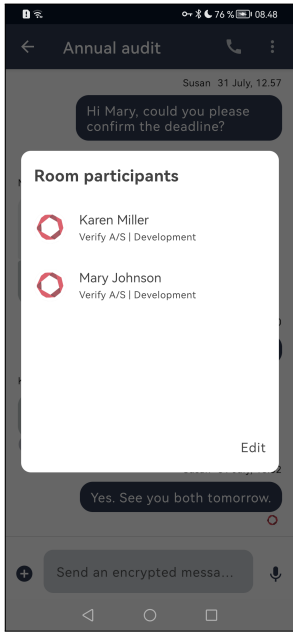
Add/remove participants

Step 1: Open the chatroom and tap .

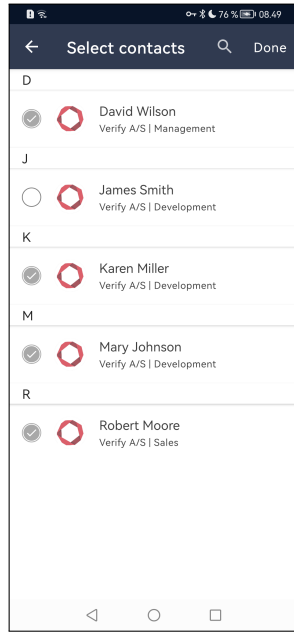
Step 2: Tap Room Participants to display a list of chatroom members (Figure 16a).

Step 3: Tap Edit to select or deselect participant (Figure 16b).

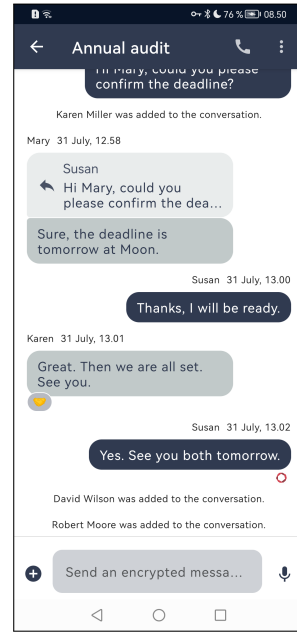
Step 4: Tap Confirm. The participants of the chatroom will be notified about the change (Figure 16c).



(a) Chatroom members.



(b) Select members.



(c) Member Updated.

Figure 16: Add/remove participants.

5 Making a secure call

Be aware of the security instructions and the surrounding before making a secure call. Refer to [Security instructions 2].

A secure call is initiated from the Contacts screen, Favourites, the call history on the Recents screen, or from inside a message conversation (Figure 17).

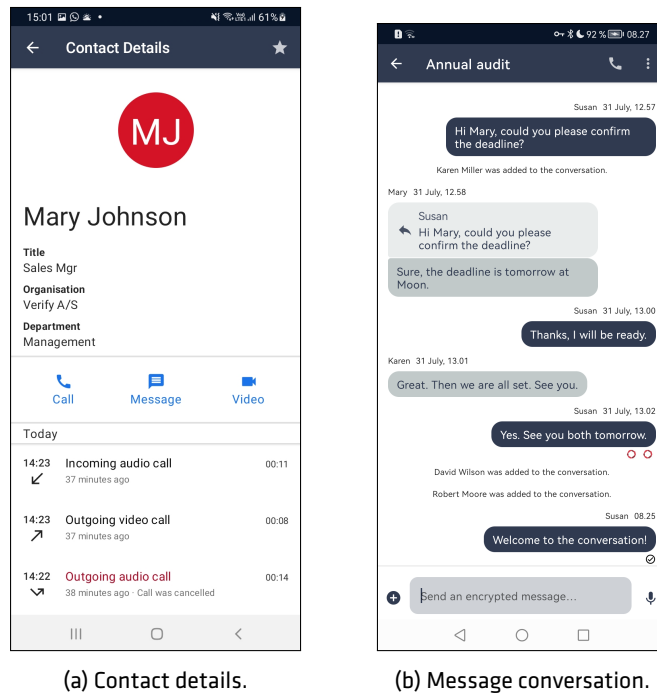


Figure 17: Making calls.

A secure call can only be made when Dencrypt Connex has a working internet connection. Secure calls are not possible during flight mode and with a poor data connection.

A secure audio call is initiated by tapping the Dial button, which opens the Call screen. A secure video call is started by tapping the Video button.

During the call setup, a status message will show the progress of the call setup. The call setup process is active until the call is answered, the call is timed out, or the receiving party rejects the call.

Once the call is answered, Dencrypt Connex authorizes the calling parties, exchanges encryption keys, and establishes a secure connection. When a secure connection is established, an audible notification is played, and the screen will display "AUTHENTICATED" as shown in Figure 18. Audio is only transmitted when the connection is secured.

The usual call functionalities are available during a secure call, such as microphone muting, enabling speaker mode, and pausing the call. During a secure video call, switching between the front- and the rear camera and disabling the camera is also possible.

If a Bluetooth device is connected to the device, the speaker button will show a Bluetooth icon (Figure 18b). Tapping it will bring up a menu where the audio output can be selected. Be aware of the security risks by applying wireless headsets [Other security recommendations 2.4].

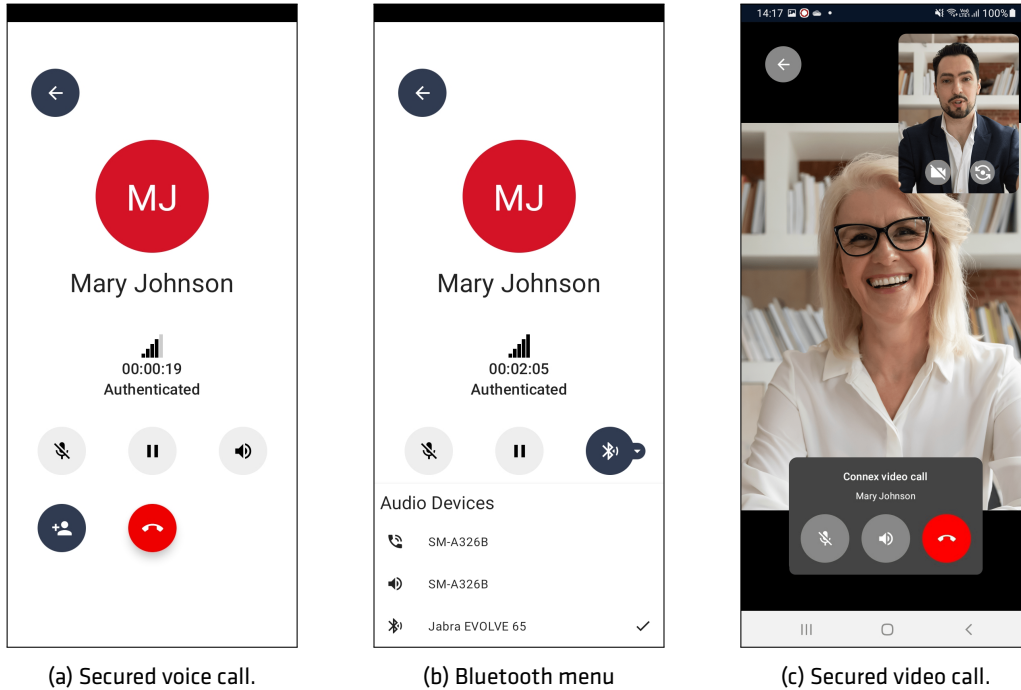


Figure 18: In call screens.

A voice call is put on hold by tapping the Pause button (Figure 19). The receiving party will hear a pause tone. Tap Pause again to resume the call.

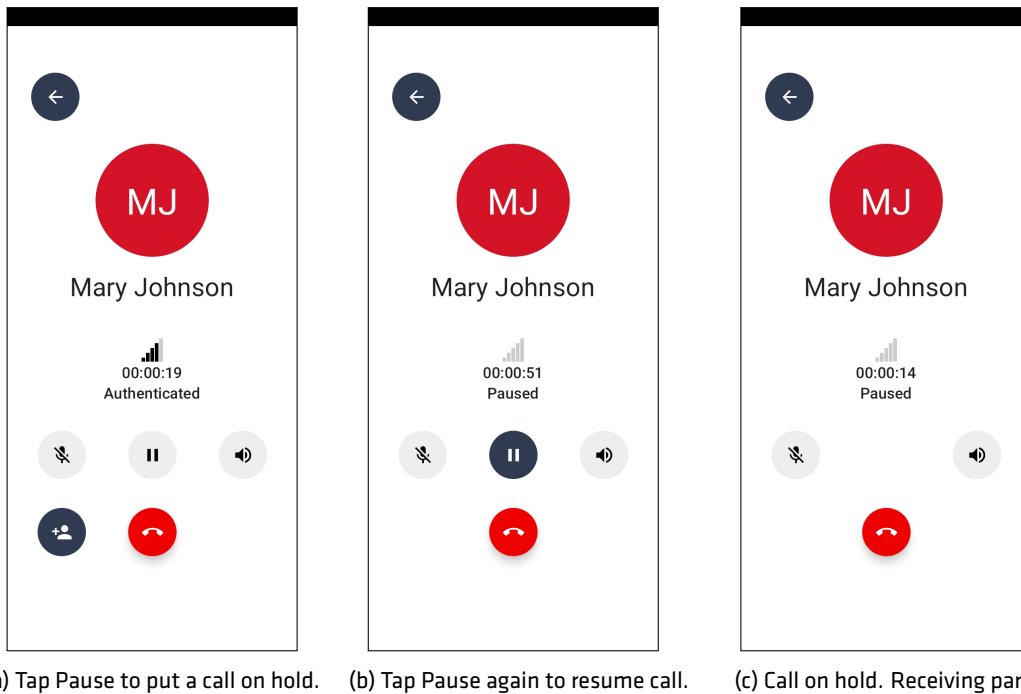


Figure 19: Call hold

Having navigated away from the Call screen during a call, the user can return to the call from the Contact details screen, by pressing Return to call (See Figure 20).

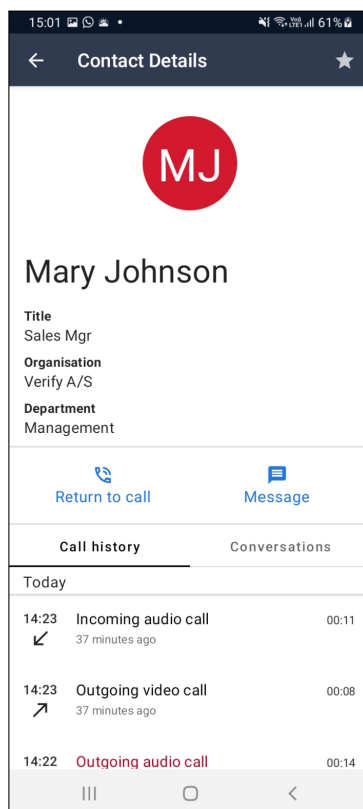


Figure 20: Return to call

5.1 Voice quality

The call quality is indicated by the signal bars as seen in Table 3. The call quality depends on the network conditions, such as available bandwidth and latency. Buildings, natural obstructions, and travel speed may impact the data connection and hence the voice quality. Poor voice quality may be improved by:

Steps for improving a poor voice quality

- Step 1: Switch the network from wifi to mobile internet or vice-versa. Network switching is possible without interrupting the call.
 - Step 2: Move to another location.
 - Step 3: Hang up and try calling again.
-

A call will automatically terminate when no audio data has been received for 30 seconds.





Quality	Reason
	Good network conditions → Voice quality is high.
	Some audio artifacts may be heard, but the voice quality should still be understandable.
	Severe audio artifacts and dropouts. Voice quality may be hard to understand.
	Data connection is poor → Voice is interrupted.

Table 3: Voice quality indicators

5.2 Group calls

Group calls can be established in two ways:

1. Add additional contacts to an ongoing conversation.
2. Call all members of a chatroom.

Add participants to an ongoing secure call.

Step 1: Establish a secure call. Refer to [Making a secure call 5].

Step 2: Tap the -icon to open the phonebook (Figure 21a).

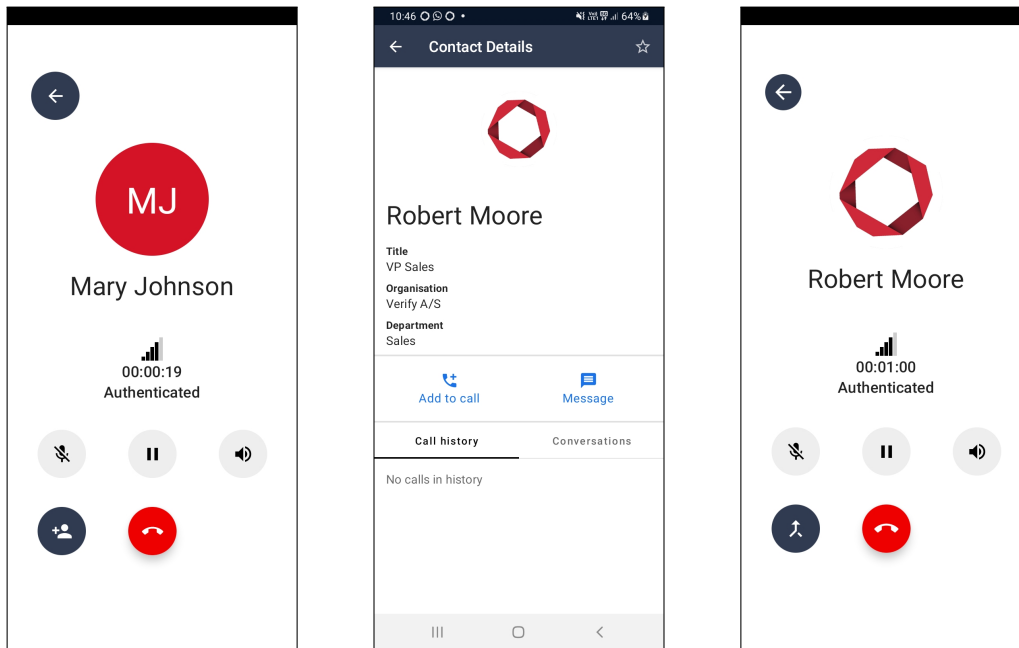
Step 3: Locate a contact in the phonebook and tap Add to call (Figure 21b). This will pause the ongoing call and establish a new secure call.

Step 4: Combine the two conversations by tapping Merge (Figure 21c). The first call is resumed and merged with the second call.

Step 5: The In-call screen displays a list of participants (Figure 21d).

Step 6: Repeat step 2 - 4 to add more participants.

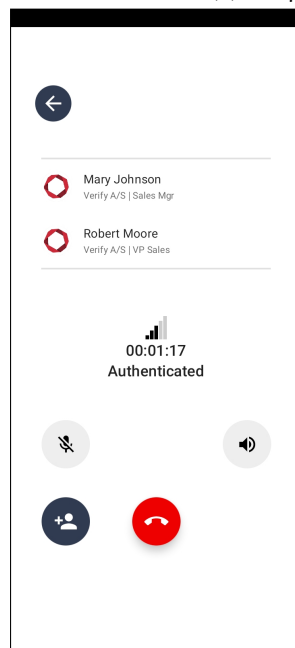
Step 7: Swipe right on the participant avatar to hang up (Figure 21e).



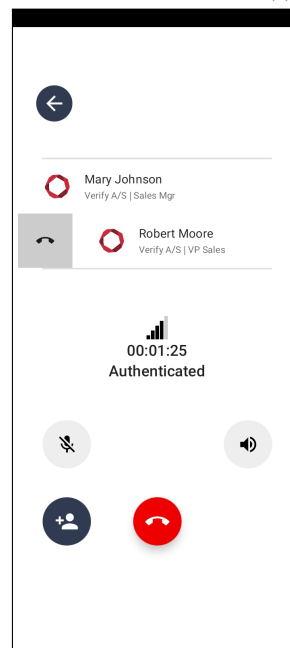
(a) Tap Add contact icon.

(b) Add participant to call.

(c) Merge calls.



(d) Group call established.



(e) Swipe right on the avatar to hang up the participant.

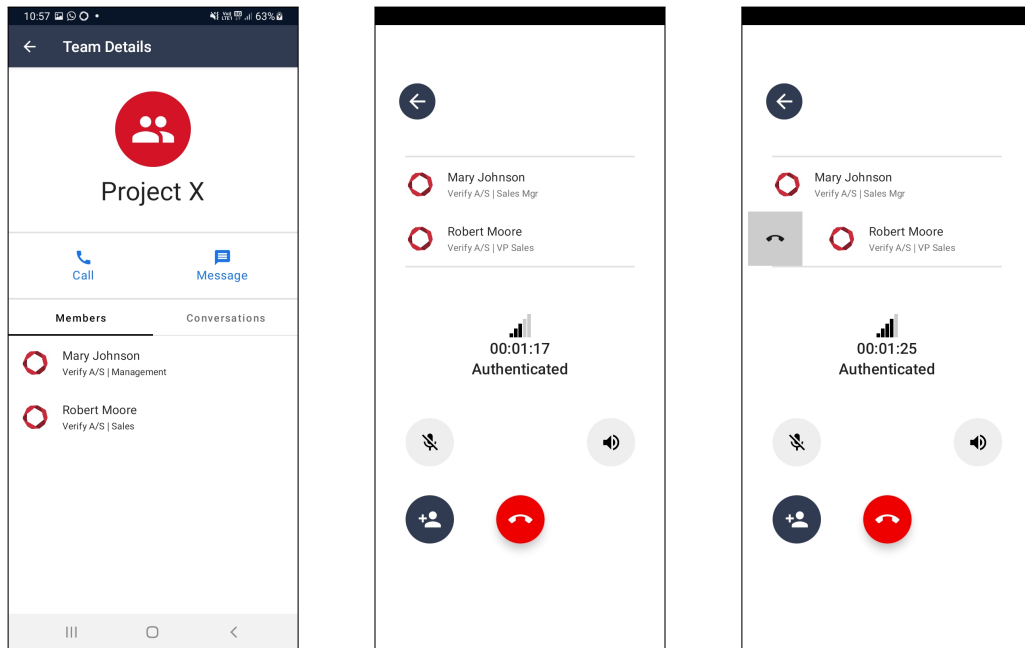
Figure 21: Group calls

Call all participants in a message room

Step 1: Go to Messages and select a chat room, or goto Contacts to select a team room.

Step 2: Tap Call to dial the participants (Figure 22a).

Step 3: Swipe right on the participant avatar to hang up (Figure 22c).



(a) Open team-/chatroom. Tap Call.

(b) Group call

(c) Swipe left to hang up participant.

Figure 22: Group calls to members of team room or message room.

The available data bandwidth limits the practical number of participants in a group call. Under normal conditions, at least 5-10 contacts should be able to participate in a group call. The user who made the first call becomes the group call host and can add additional participants.

Video group calls are not supported.

5.3 Incoming calls during a secure call

Secure voice calls have the same priority as normal mobile calls. A secure call is not interrupted by an incoming normal mobile call, and the user has the usual options for handling incoming calls as seen in Figure 4 and given in the following table:

Menu	Action
Answer	The active secure call is paused. The secure call is resumed by tapping the Pause button. (Require Call waiting is enabled for the device.)
Decline	Reject the incoming call.

Table 4: Actions for incoming calls during a secure call.

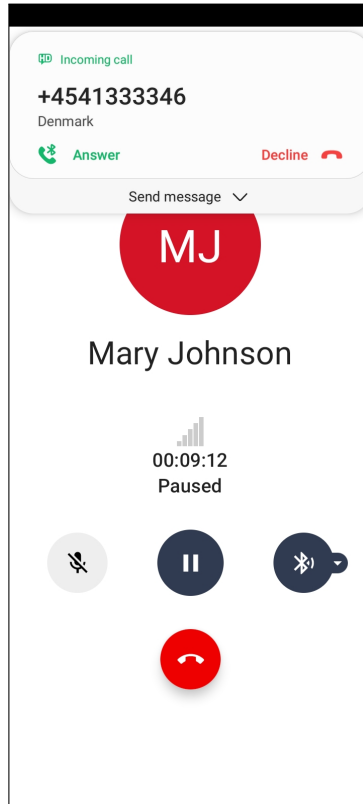
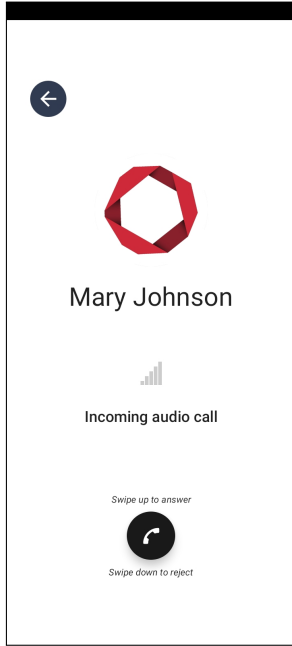


Figure 23: Incoming call during a secure call

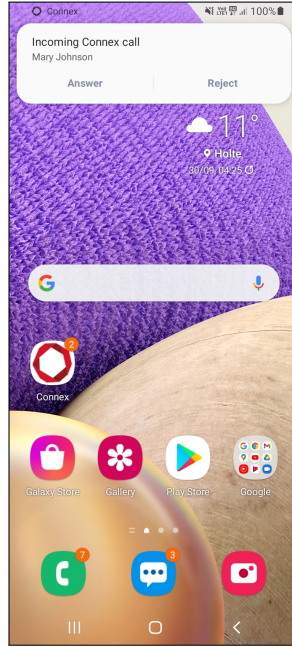
5.4 Incoming secure calls

Incoming secure voice calls are alerted using VoIP push notifications. The incoming call screen is displayed, where the caller's name is shown, followed by incoming audio call indicating a secure voice call (Figure 24a) or by incoming video call indicating a secure video call. The call is accepted by swiping up the "phone" icon and declined by swiping down.

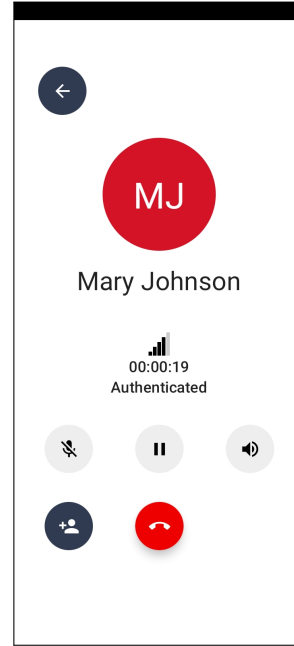
When the device is in use, the secure incoming call is alerted using a push notification, where the call is answered or rejected (Figure 24b). When answering the call, the Dencrypt Connex authorizes the calling parties, exchanges encryption keys, and establishes a secure connection. A waiting tone is played during the setup process, indicating that the secure channel is being established. Audio feedback is played when the channel is secured and available. Voice data is only transmitted when the secure channel is established (Figure 24c).



(a) Incoming secure call.



(b) Incoming secure call on an unlocked device.



(c) Ongoing secure call.

Figure 24: Incoming secure call.

6 Sending a secure message

The Messages screen shows all the ongoing conversations (chatrooms). Initially, the message inbox is empty and shows only a placeholder text.

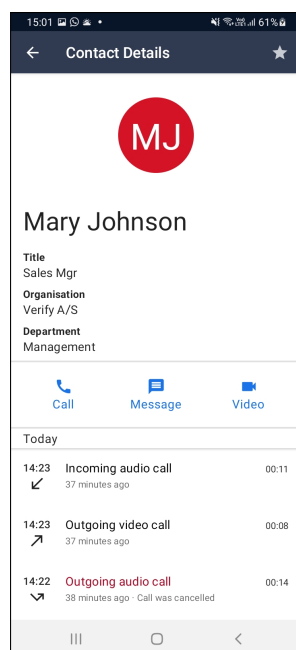
6.1 Create a *direct chat room*

A direct chatroom is the default chatroom for conversations with a single contact. Only one direct chatroom per contact exists, and the title is fixed to the contact name.

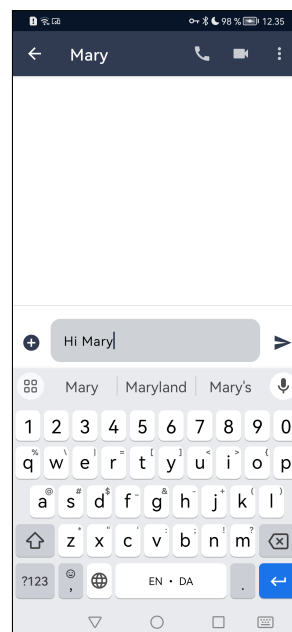
Create a *direct message* conversation

Step 1: Select contact details and tap the Message icon (Figure 25a).

Step 2: If an existing conversation exists, the chatroom opens to continue the conversation. If not, a new chatroom is created (Figure 25b).



(a) Select Message.



(b) Start typing the first message.


Figure 25: Create a Direct chatroom.

6.2 Create a *topic chatroom*

A topic chatroom is used for group messaging and for conversations with a single contact on a specific topic.

Creating a conversation

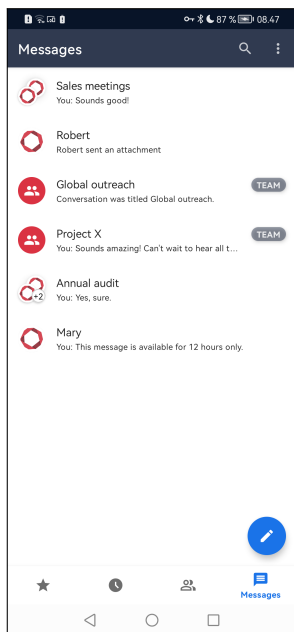
Step 1: Goto the the Messages tap.

Step 2: Tap the -icon in the top-right corner.

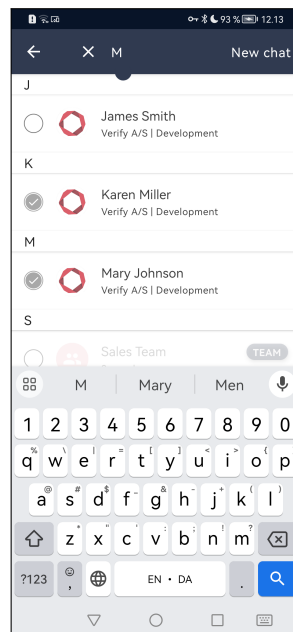
Step 3: Search and select one or more recipients to add them to a conversation (Figure 26b). Tap New Chat.

Step 4: Set a title for the chat room and tap Confirm (Figure 26c).

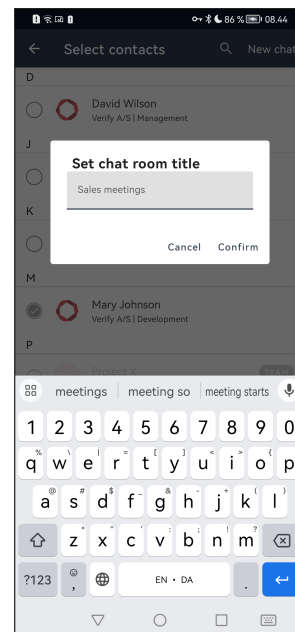
Step 5: Start writing the first message (Figure 26d).



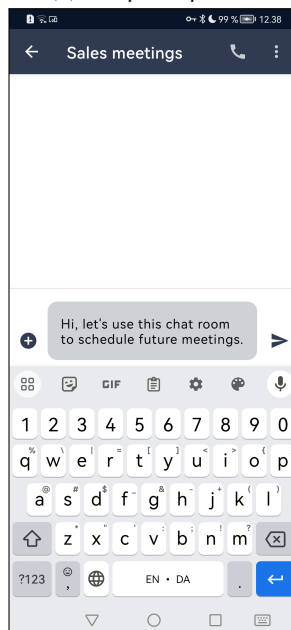
(a) Message inbox.



(b) Add participants.



(c) Set title.



(d) Write the first message.


Figure 26: Create a topic room.

6.3 Sending a secure message

Sending a secure message

Step 1: Select an existing Chatrom from the Message tap.

Step 2: Enter text and tap Send.

The message is encrypted and transmitted immediately when an active data connection exists. A successful transmission is indicated by a  -icon.

A message pending transmission is indicated by a "spinner" icon next to it. The message is stored encrypted, and automatic retransmission will be attempted while the app is open. A notification is received if the app is closed while having pending transmission. Once opened again, the app will attempt to resend the message.

Encrypting and sending large-size attachments may take longer.

6.3.1 Unable to decrypt message

If a recipient is unable to decrypt a message, the sender's device will be notified, and retransmission will be attempted automatically. Whilst the message is not able to be decrypted, the recipient will be presented with: Message could not be decrypted. Please contact sender.

Attachments are not supported for automatic retransmission, and the sender should be contacted manually.

6.4 Message context menu

Long pressing on any message will bring up a context menu (Figure 27) presenting the following options:

Delivery status Message delivery status. Refer to [Message delivery status 6.4.1].

Reply Reply to message. Refer to [Reply to message 6.4.2].

Copy Copy messages and/or attachments from one conversation to another [Copy messages 6.4.3].

Show Show message.

Delete Delete message. Warning: The message is permanently deleted.

Edit Edit message. Refer to [Edit message 6.4.4]

Emoji reaction React to message. Refer to [Emoji reaction 6.4.5]

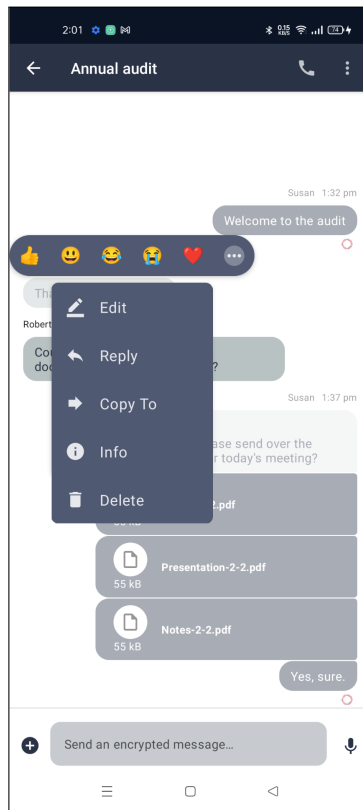


Figure 27: Long pressing on a message

6.4.1 Message delivery status

A delivery status for sent messages is displayed under each message in the conversation screen:


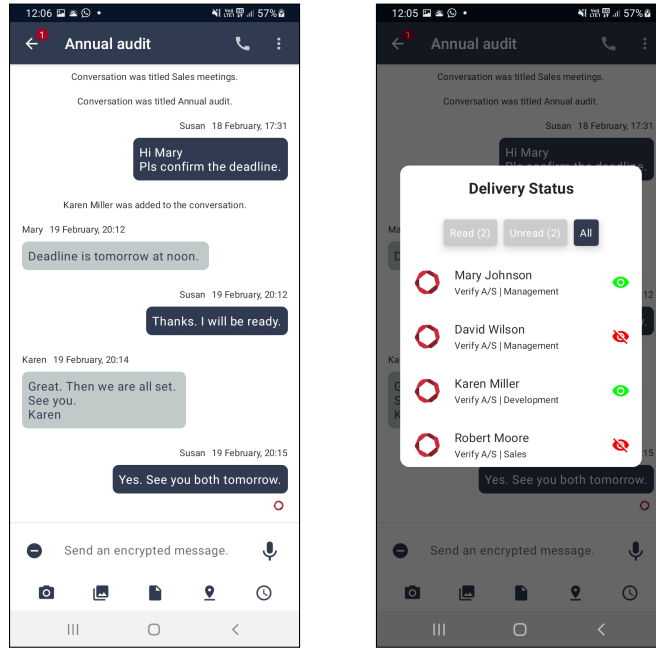
- The -icon indicates that the message has been delivered. Tapping the icon will open the Delivery Status screen.
- An avatar indicates who has read the messages. Tapping the avatar will open the Delivery Status screen.

Figure 28 gives a conversation example with all color codes. Detailed delivery status is available when long pressing on a message.



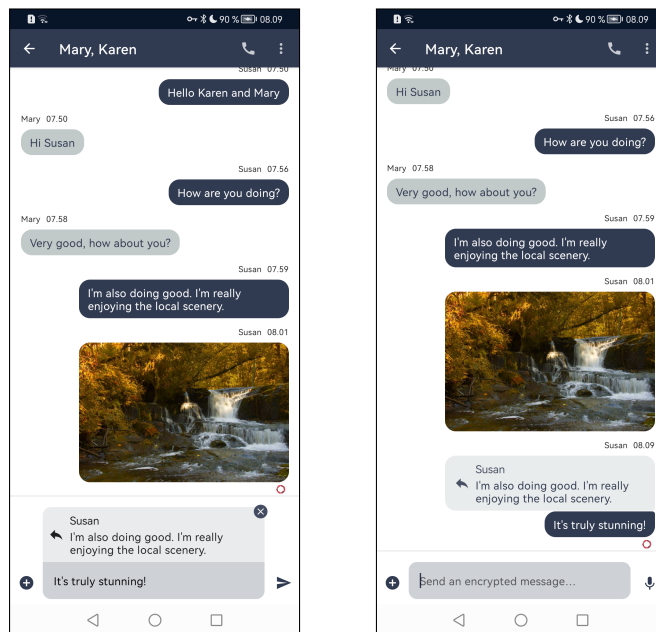
(a) Conversation screen.

(b) Delivery status details.

Figure 28: Message delivery status

6.4.2 Reply to message

A user can reply to a specific message by long pressing on a given message and selecting Reply. This will show the original message and allow the user to send a response to it. Tapping the -button will cancel the reply feature, tapping Send will send the reply (Figure 29). Both the senders and receivers conversation screen will show both the original message and the reply message. Tapping the original message will scroll the conversation so the original message is shown.



(a) Writing a reply.

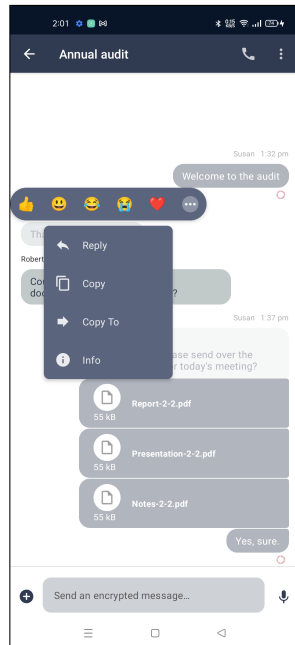
(b) Reply sent.

Figure 29: Message with a reply.

6.4.3 Copy messages

Messages can be copied from one conversation and inserted into another.

Long pressing a message and selecting Copy To from the context menu will allow the user to select the rooms to which the text message should be sent.



(a) Selecting messages for copying.



(b) Selecting copy destination.

6.4.4 Edit message

From the message context menu [Message context menu 6.4] it is possible to edit a message. Press Send to confirm changes. Alternatively the ✕-icon can be pressed to discard changes (Figure 31).

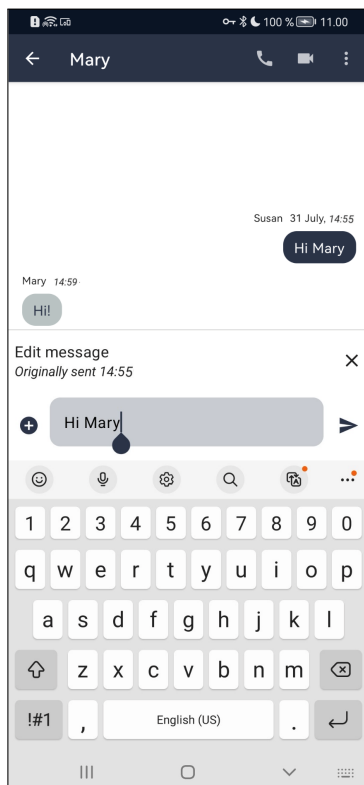


Figure 31: Editing message

The option is only present during the first 5 minutes after the message has been sent. Furthermore all devices in the conversation must be updated to a version which supports message editing.

6.4.5 Emoji reaction

Emojis can be assigned to messages from the context menu [Message context menu 6.4]. The most recently used emojis are available directly in the context menu. Pressing **•••** will present a wider selection of emojis (Figure 32).

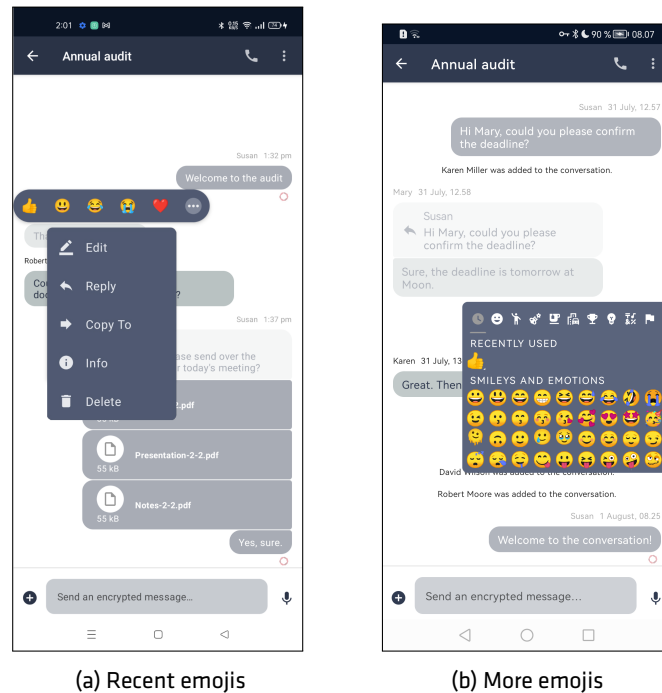


Figure 32: Emojis






6.5 Sending attachments

Sending attachments

Step 1: Expand the Attachment menu by tapping the **+**-icon the lower-left corner (Figure 33a).

Step 2: Select the source for attachments.

Options as seen in Figure 33b are:

-  Open the camera for in-app capturing of images and video.
-  Open the gallery for attaching images and videos.
-  Open the file manager for attaching files.
-  Open Google Maps to select and share a location.
-  Set time constraints on a message availability.

The system administrator may disable some options to comply with local policies.

Attachments will be added above the compose text field. Attachments can be removed from the message by tapping the **-**-icon on the top-right corner of each attachment (Figure 33c). Photos, videos, audio clips, and shared locations generated from within Dencrypt Connex will permanently disappear and cannot be recovered once removed.

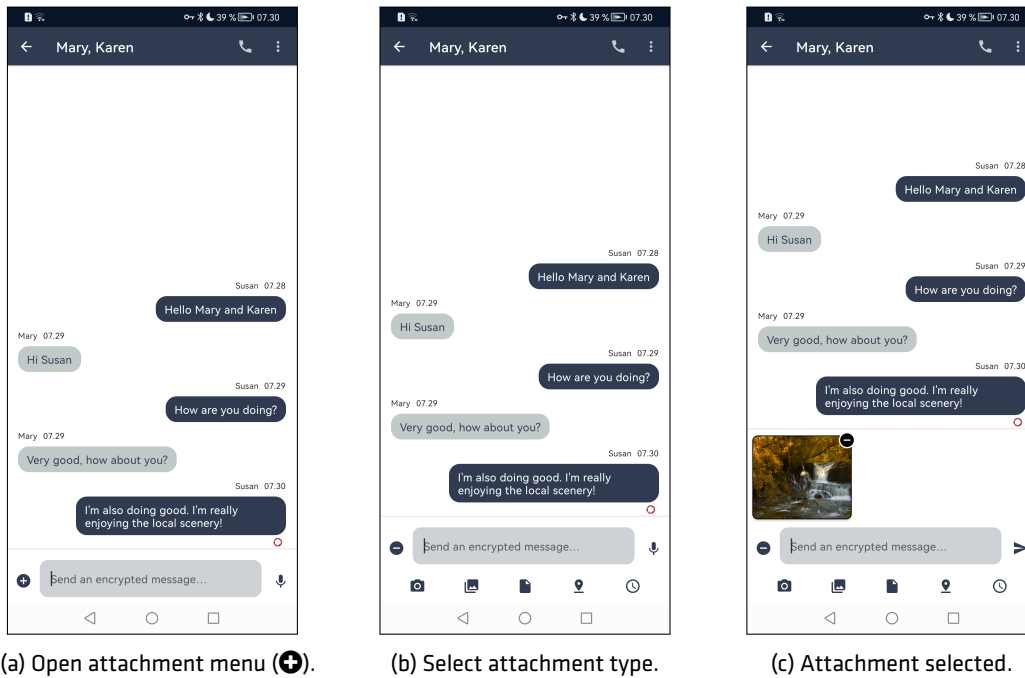





Figure 33: Sending attachments.

6.6 Push-to-Talk

Push-to-Talk functionality is available through the -icon in the compose field (Figure 34).

Send an instant audio message

-
- Step 1: Tap and hold the -icon in the compose field.
 - Step 2: Record audio message.
 - Step 3: Release the -icon to send the audio message.
-

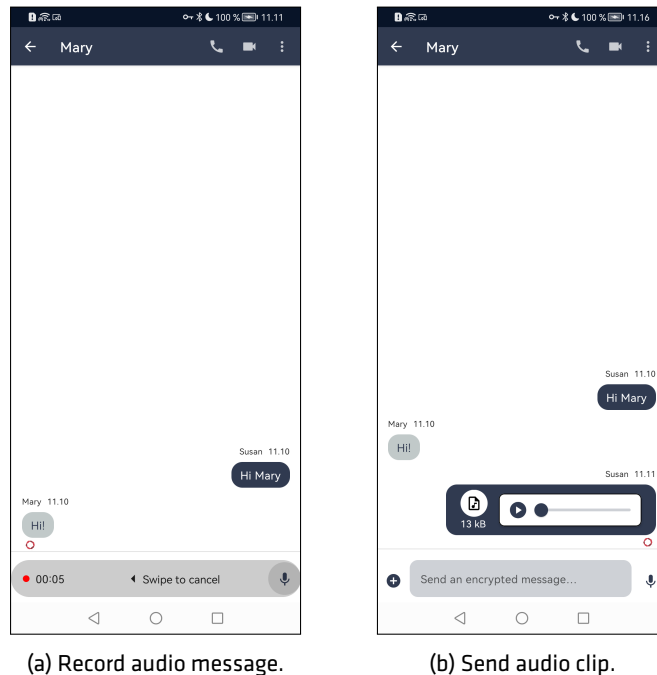




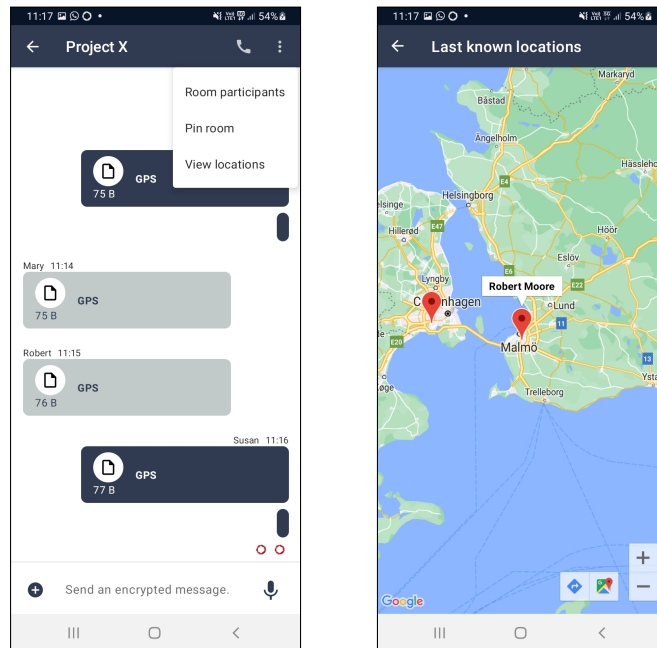
Figure 34: Push-to-Talk messaging

6.7 Location sharing

Participants in a chat room can share their location as an attachment. The last known location of the participants, who have shared a location, is displayed on a single map (Figure 35).

View last known locations

-
- Step 1: Open the chatroom. Tap any of the shared GPS-messages to see the location of a single participant.
 - Step 2: Tap →View locations to open a map with all shared locations.
 - Step 3: Tap a pin to see the name of the contact.
 - Step 4: Alternatively locations are also saved as attachments and can be found by tapping  followed by View Attachments.
-



(a) Shared locations.

(b) Map view.

Figure 35: Location sharing

6.8 Message expiry

Message expiry is used to set time constraints on a message making it available for the receiver in defined periods only. Expired messages will still be available to the sender. The time constraints can be set in the attachment menu [Sending attachments 6.5] as seen in Figure 37.

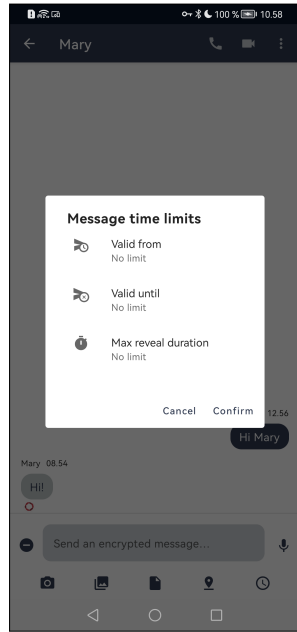
Set time constraints on messages

-
- Step 1: Tap ⌚ to open the configuration screen to set time limits.
 - Step 2: Tap Valid from or Valid until to set start and end date and time.
 - Step 3: Tap Max reveal duration to set a duration.
 - Step 4: Tap Confirm
 - Step 5: Type and send message
-

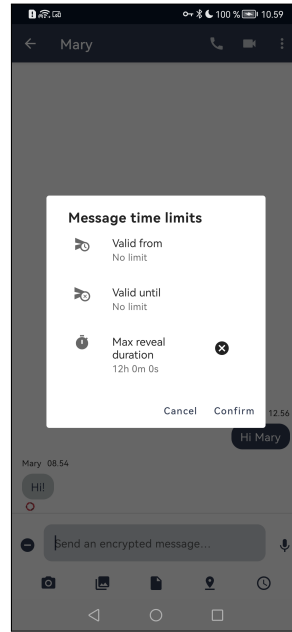
Valid from The message will not be available for the recipients before this date. The receiver will get a notification when the message becomes available.

Valid until The message will not be available for the recipients after this date.

Max reveal duration The message will only be available for the receivers for a limited time period. A timer will start a countdown once the message is opened and the message becomes unavailable at timeout.

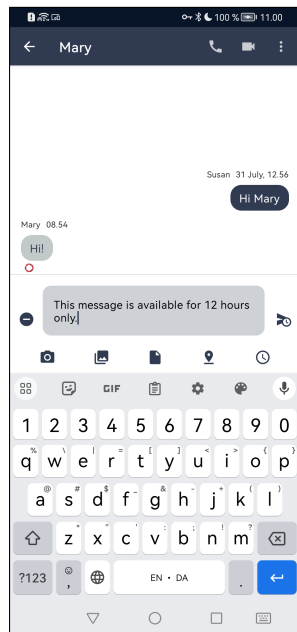


(a) Message expiry options.

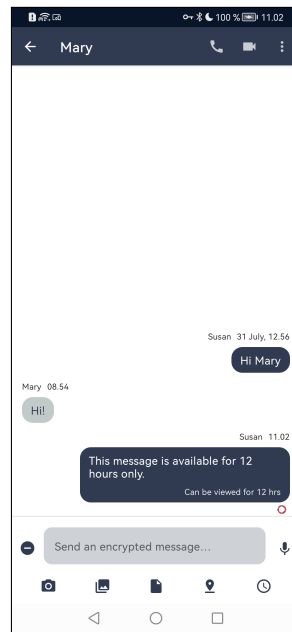


(b) Message with time constraints.

Figure 36: Set message expiry.



(a) Typing message.




(b) Time limited message.

Figure 37: Message expiry

7 Settings

Most of the configuration of Dencrypt Connex is performed centrally by the system administrator.

Dencrypt Connex settings are opened by tapping the  -symbol in the top right corner of the Contacts screen iOS-Devicescreen. The Settings menu gives access to the following options and information:

- **Account**

- Fullname - The display name of the end-user
- SIP ID - Unique user identifier.
- Client certificate expiry - Timestamp for certificate expiry.
- Server name
- Delete account. Warning: This will permanently delete all messages and data.

- **Contacts**

- Sort and display order [Firstname Lastname/Lastname, Firstname].
- Show inactive users [Default/Show/Hide].

- **Messaging Settings**

- Instantly send voice messages [On / Off].

- **App**

- Start view [Last used/Favorites/Recent/Contacts/Messages].
- App version - The version number of the app.
- Core version - The version number of the core SDK.
- Privacy policy - Links to the privacy policy.
- Open source licenses: Displays a list of used open source licenses. Tap a library name to display the licensing terms.

- **Support**

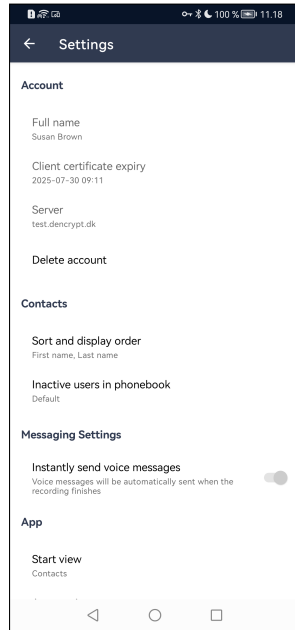
- Send a support email: The end-user can share logs with Dencrypt Connex Developers.

- **Server policy**

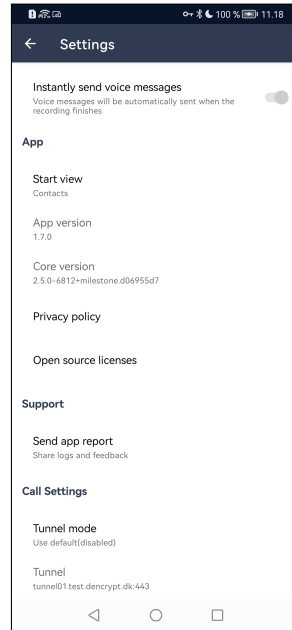
- Biometric Authentication.
- Video calls.
- Instant messaging.

- **Call Settings**

- Enable Opus [Enabled, prefer Speex / Enabled, prefer Opus / Disabled, use Speex].
- Tunnel mode: - Toggle Tunnel mode. Used in VoIP blocking regions (Default: Off) [Default/Auto/Enabled/Disabled].
- SIP mode [Default / Enable / Disable].
- Tunnel: - Address for tunnel server.



(a) Settings menu - Part 1.



(b) Settings menu - Part 2.

Figure 38: Settings

Appendices

A Dencrypt Communication Solution

The Dencrypt Communication Solution is an encrypted Voice-over-IP-based communication system that offers encrypted mobile voice/video communication and instant messaging within closed user groups. Once Dencrypt Connex is installed and provisioned, it allows for two or more persons to talk securely or exchange instant messages securely.

The solution consists of Dencrypt Connex , a smartphone application (app) installed on the end-users smartphone, and a Dencrypt Server System as illustrated in Figure 39. The Dencrypt Server System is responsible for setting up the encrypted calls, routing messages, and distributing an individual phonebook to each device, defining to whom calls and messaging can be performed. The server system is also responsible for initiating the provisioning process for the first-time activation.

The server system only facilitates call setup and message routing. It is not capable of decrypting voice calls or messages as these are end-to-end encrypted between devices.

The Dencrypt Connex application is installed from Google Play or pushed by a Mobile-Device-Management (MDM) system. The Dencrypt Server System is managed by a system administrator.

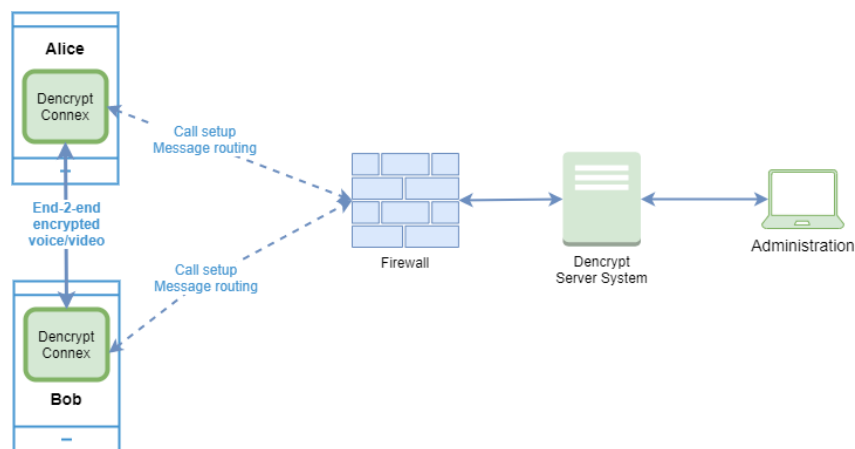


Figure 39: Dencrypt Communication Solution .

A.1 End-2-end encrypted VoIP calls

For secure voice and video calls, an end-to-end encrypted connection between the devices is established using the mobile internet or wifi-networks. Only the data transmission between the devices is protected. The audio/video connection between the user and the device through the microphone, speaker, headset, or screen is not protected as illustrated in Figure 40

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

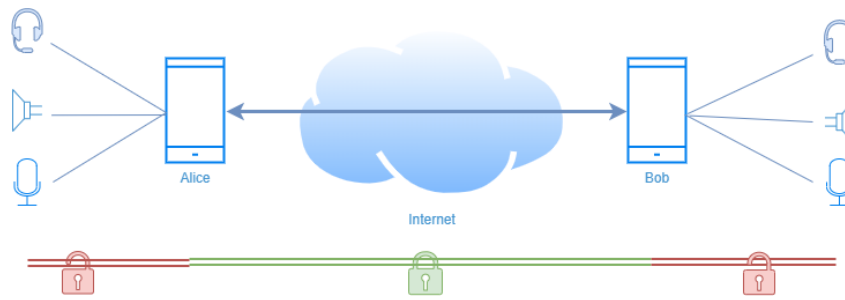


Figure 40: Area of protection for voice/video calls.

A.2 End-2-end encrypted instant messaging

Also, instant messaging is encrypted end-2-end between devices and transmitted, via the Dencrypt Server System, over the mobile internet or wifi-networks. Both the message exchange and the storage on the device (chat history) are protected, whereas the connections to external keyboards or screens are not protected, as shown in Figure 41.

The key exchange happens directly between the communicating devices but is facilitated by the Dencrypt Server System, which also queues the encrypted messages for delivery.

The message history is stored encrypted on the device and requires two keys for decryption: 1) A local key protected by the trusted platform module on the device and 2) a remote key stored on the server system. Hence, the chat history is only accessible when a data connection to the server has been established. The remote key is destroyed when the app is closed.

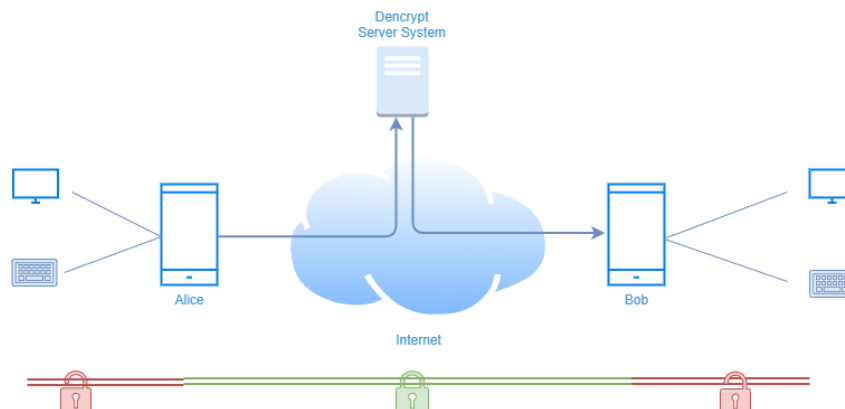


Figure 41: Area of protection for instant messaging

A.3 Authenticated connections

All communication between the Dencrypt Connex and the Dencrypt Server System takes place over mutually authenticated connections. Hence, the server system will only accept connections from authenticated users, and the app will only connect to authorized server systems. The authentication is automatic and does not require user actions besides the initial provisioning.

A.4 Encryption keys

All encryption keys for voice/video calls and for instant messaging are generated automatically when a new conversation is initiated and does not require user actions. Encryption keys are overwritten in memory when a call is terminated or when the app is closed or put in the background.

A.5 Secure phonebook

To ensure that only authorized persons can communicate, the Dencrypt Communication Solution applies a centrally managed and individual phonebook. The phonebook defines with whom a user can communicate. The phonebooks are generated by the system administrator, and updates are pushed to the apps when they connect to the server system. Hence, the phonebook is always up-to-date without any user actions required. The phonebook is stored encrypted on the device using the same key management as for the chat history [End-2-end encrypted instant messaging A.2].

The phonebook concept supports two-way and one-way conversations. Hence, it is possible to receive calls from persons not listed in the phonebook and without being able to call back. Messages received from not listed contacts can be answered.

A.6 Push notifications

Push notification services from Google are used for alerting on incoming secure calls and messages. The push messages are sent either with empty content or with encrypted content.