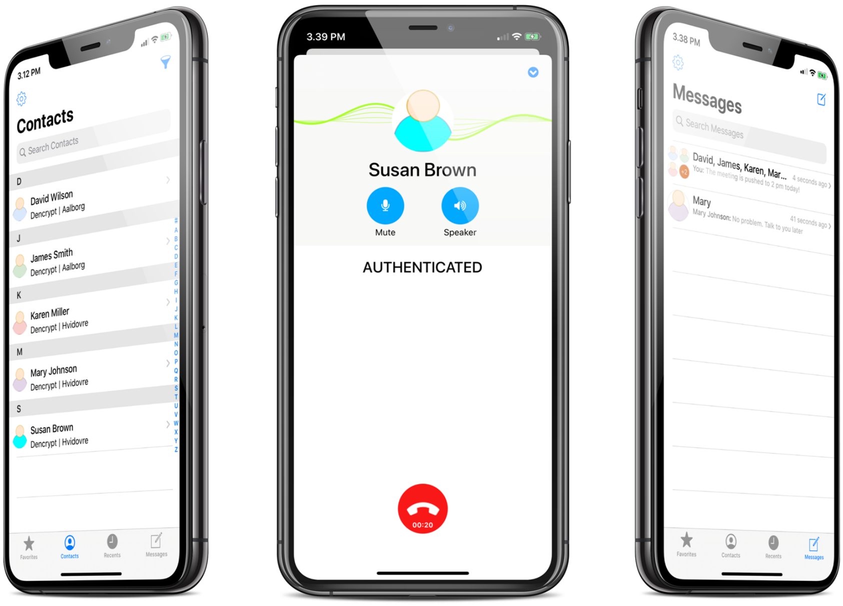
DENCRYPT

Dencrypt Communication Solution

Operational user guide

Dencrypt ConnexR

v. 6.2



March 21, 2022

Public

Contents

Version

This guide applies for:

- Dencrypt ConnexR v. 6.2 for iOS devices.

The version number can be verified from the *Settings* menu by tapping the clog-wheel in the upper-left corner of the screen. See Figure 27a.

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 ConnexR is an application for making encrypted voice calls, video calls, and for exchange of encrypted instant messages from iOS 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 ConnexR application and provides instructions to operate and use the application in a secure way.

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

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

Table 1: Reading Guide

2 Security instructions

These security instructions shall be read and understood before taking the Dencrypt ConnexR 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 the app into use, the security policies and instructions for secure usage shall have been received and understood. Be aware of the classifications, which are allowed to be exchanged using the app.

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 ConnexR shall only be received from 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 that there are no critical side-effects. Therefore, the Dencrypt ConnexR 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 ConnexR 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 enable 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 ConnexR 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. 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 ConnexR 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 ConnexR . Use wired headsets as an alternative.

- **Avoid using handsfree car systems** - The data connection from the device to the handsfree car system is not encrypted. Disable Bluetooth to avoid automatic connection and use wired headsets as an alternative.
- **Avoid using loudspeaker** - Use the Dencrypt ConnexR loudspeaker only with care and in locations, which 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. The Dencrypt ConnexR will show a warning when taking screenshots.
- **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, which 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 recognization** - Avoid using applications, which 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 ConnexR .

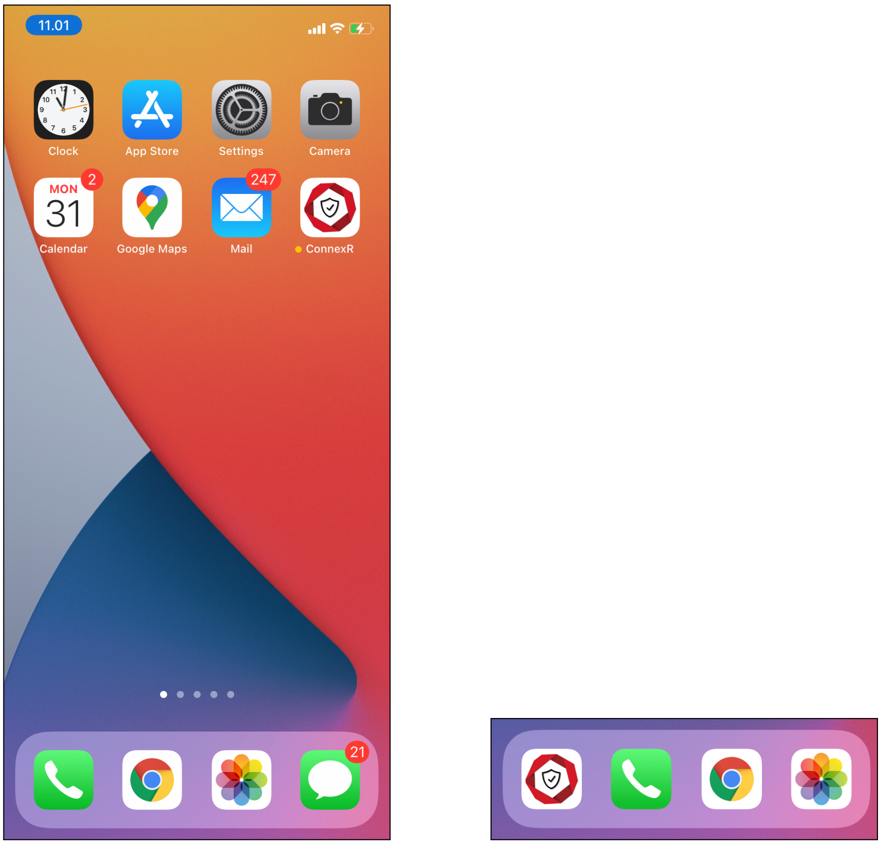
1. Installation
2. Activation
3. Set permissions

3.1 Installation

Dencrypt ConnexR is installed via:

- An Mobile Device Manager (MDM).

Once the app is installed, it is launched by tapping the Dencrypt ConnexR icon. For quick access, the icon can be dragged to the menu bar at the bottom of the screen.



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

Figure 1: Home screen

3.2 Activation

Once installed, the Dencrypt ConnexR 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 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.

Emails shall be encrypted or transmitted using encrypted connections.

Activating the link will start the provisioning process to configure the Dencrypt ConnexR with certificates and credentials to connect to the server system and download the phonebook. Only when the activation process has successfully completed, the Dencrypt ConnexR 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.

Step 2: The user activates the link by tapping the weblink or by scanning the QR-code using Dencrypt ConnexR Figure 2b or the camera application. The user may be prompted to open the link in the Dencrypt ConnexR .

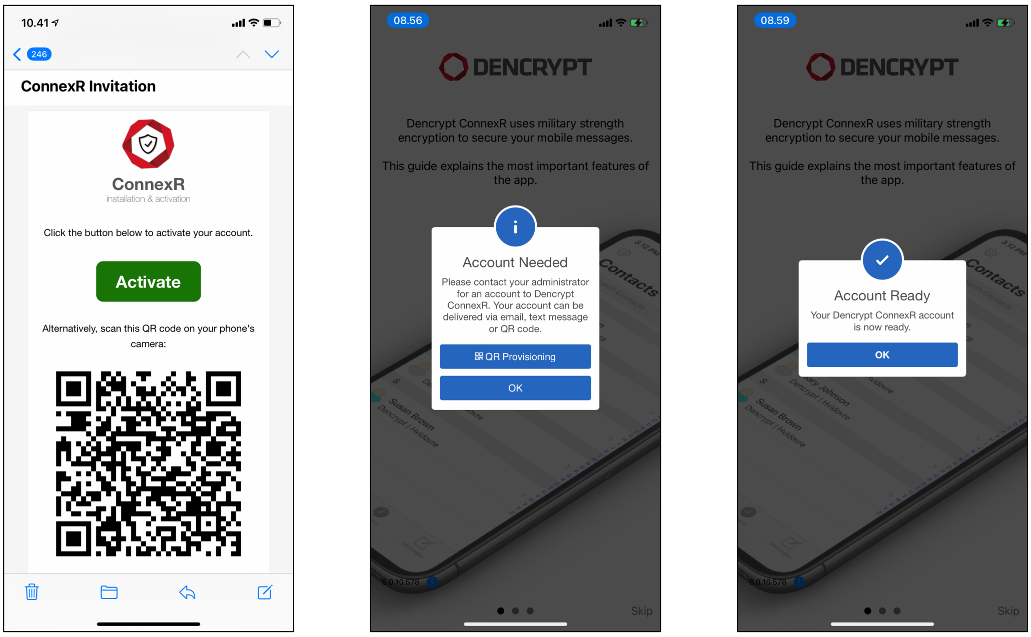
Step 3: The Dencrypt ConnexR opens to configure the account. This may take 1-3 minutes. **Do not close the app during the activation.**

Step 4: Once completed, tap *OK* to open the app.

Step 5: The app will request permissions to the device resources for full functionality. Tap *Allow* for each permission. See [Set permissions 3.4].

Step 6: Dencrypt ConnexR will connect to the server system to download the phonebook.

Step 7: Dencrypt ConnexR is now ready for use.



ConnexR Invitation

Click the button below to activate your account.

Alternatively, scan this QR code on your phone's camera:

Dencrypt ConnexR uses military strength encryption to secure your mobile messages.

This guide explains the most important features of the app.

Account Needed

Please contact your administrator for an account to Dencrypt ConnexR. Your account can be delivered via email, text message or QR code.

Account Ready

Your Dencrypt ConnexR account is now ready.

(a) Email invitation

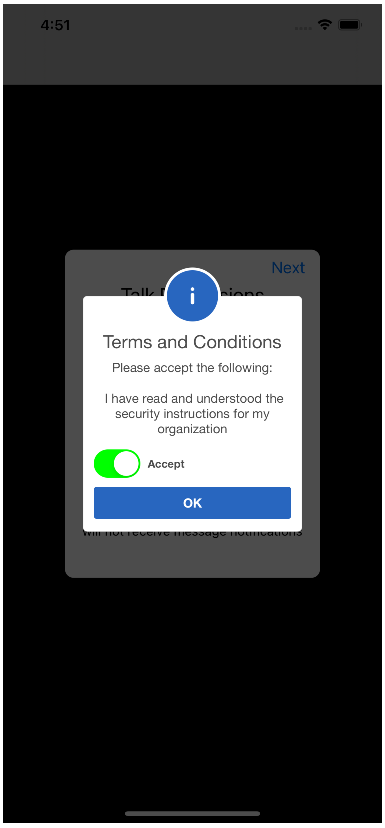
(b) QR provisioning.

(c) Activation successfull.

Figure 2: Invitations and activation.

3.3 Agree on Terms and Conditions

The security policies and instructions for secure usage of Dencrypt ConnexR shall have been received and understood. Before taking the app into use, these terms and conditions of the organizational security policies have to be accepted.



Terms and Conditions

Please accept the following:

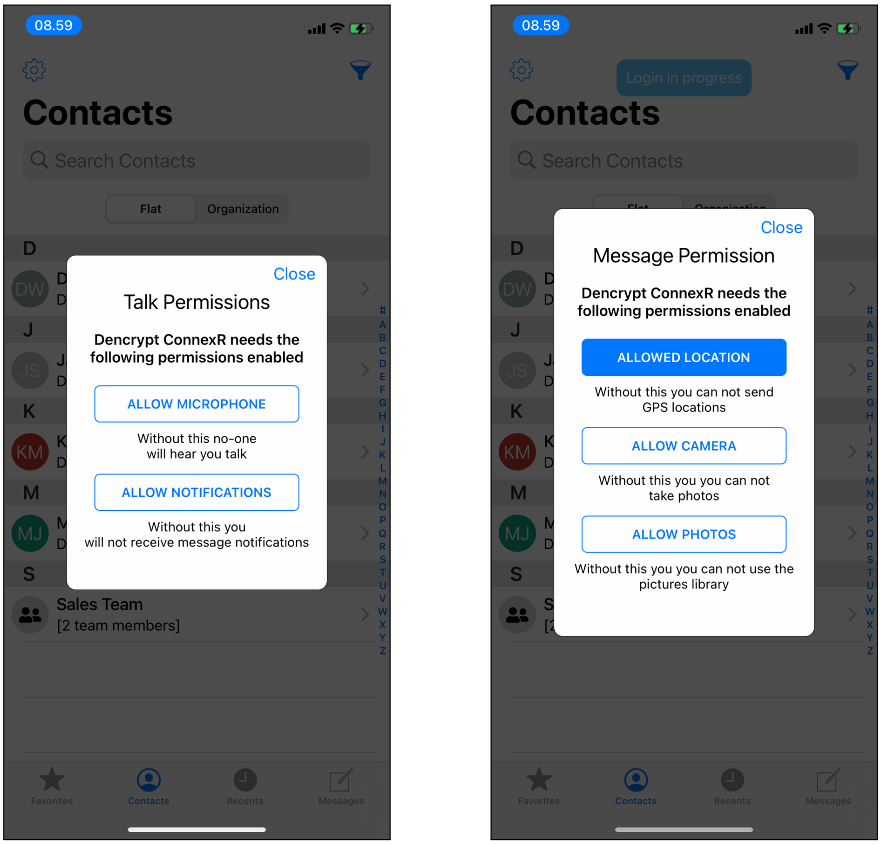
I have read and understood the security instructions for my organization

Figure 3: Terms and conditions acceptance.

3.4 Set permissions

Dencrypt ConnexR 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 if not granted.

During the account setup Dencrypt ConnexR will ask for permission to the following resources:



Sales Team
[2 team members]

Close

Talk Permissions

Dencrypt ConnexR needs the following permissions enabled

ALLOW MICROPHONE

Without this no-one will hear you talk

ALLOW NOTIFICATIONS

Without this you will not receive message notifications

Close

Message Permission

Dencrypt ConnexR needs the following permissions enabled

ALLOWED LOCATION

Without this you can not send GPS locations

ALLOW CAMERA

Without this you you can not take photos

ALLOW PHOTOS

Without this you you can not use the pictures library

(a) Mandatory permissions (b) Optional permissions

Figure 4: Permissions.

Permission	**Reason**
Microphone	Required for voice calls.
Notifications	Required to alert for incoming calls and messages.

(a) Mandatory permissions

Permission	**Reason**
Location	Required to include GPS locations in messages.
Camera	Required to capture images to attach to messages.
Photo	Required to attach images from libary.

(b) Optional permissions

Table 2: Permision usage.

4 Using Dencrypt ConnexR

Dencrypt ConnexR offers two main functionalities:

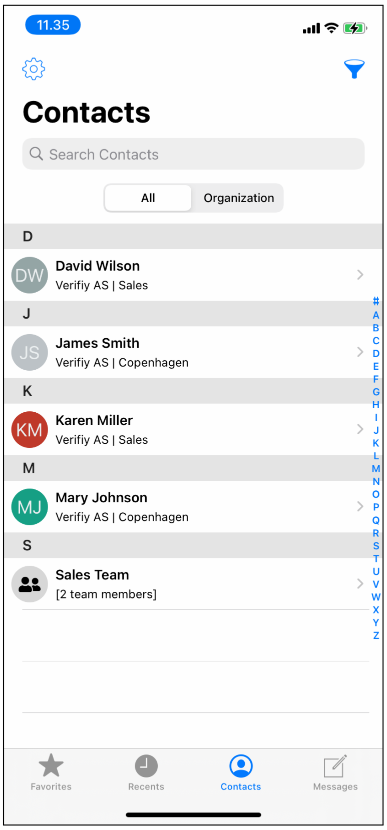
- Secure voice communication
- Secure instant messaging of text and content (attachments).

The functionalities are accessible from the main screen. The icons in the menu bar at the bottom provides a quick access to the following screens.

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

Settings are accessed from the "cogwheel"-icon in top-left corner.

Dencrypt ConnexR launches per default with the *Contacts* screen. The launch screen can be set by the *Launch screen* in the *Account Settings* [Settings 7].



D

DW David Wilson
Verifiy AS | Sales

J

JS James Smith
Verifiy AS | Copenhagen

K

KM Karen Miller
Verifiy AS | Sales

M

MJ Mary Johnson
Verifiy AS | Copenhagen

S

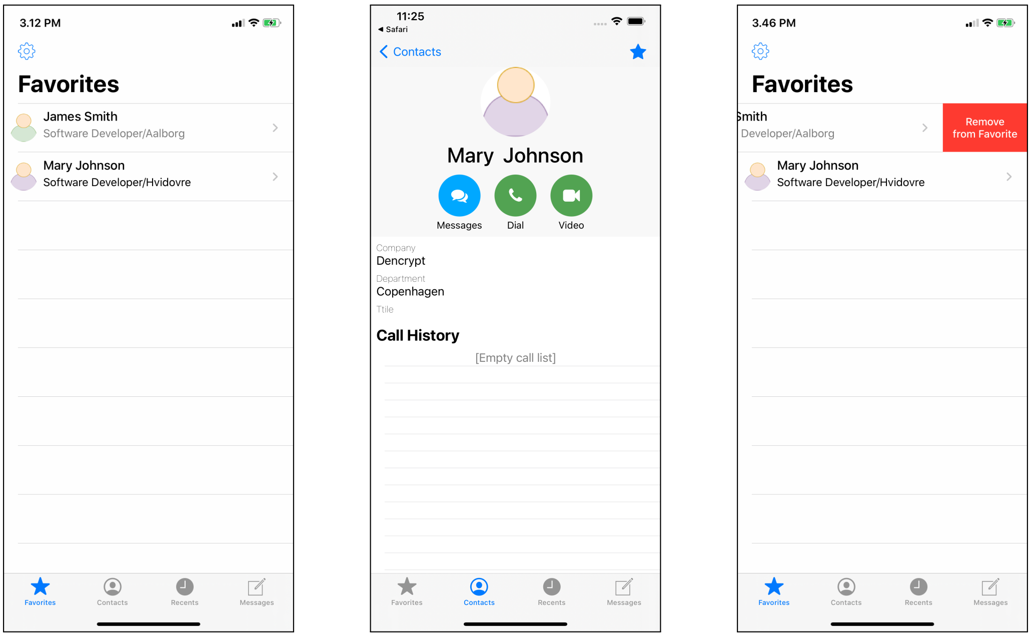
Sales Team
[2 team members]

Figure 5: Contacts screen

4.1 Favourites

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

A contact can be removed from *Favorites* by either tapping the ★-icon again or by swiping left on a favorite and selecting "Remove from Favorites".



3.12 PM

Favorites

James Smith
Software Developer/Aalborg

Mary Johnson
Software Developer/Hvidovre

11:25

Mary Johnson

Company
Dencrypt

Department
Copenhagen

Title

Call History

[Empty call list]

3.46 PM

Favorites

Smith
Developer/Aalborg

Mary Johnson
Software Developer/Hvidovre

(a) *Favourites* screen

(b) Adding favourites

(c) Removing favourites.

Figure 6: Favourites.

4.2 Contacts

The *Contacts* screen shows the entire phone book consisting of individual contacts and teamrooms. 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 firstname per default [1]. To locate contacts:

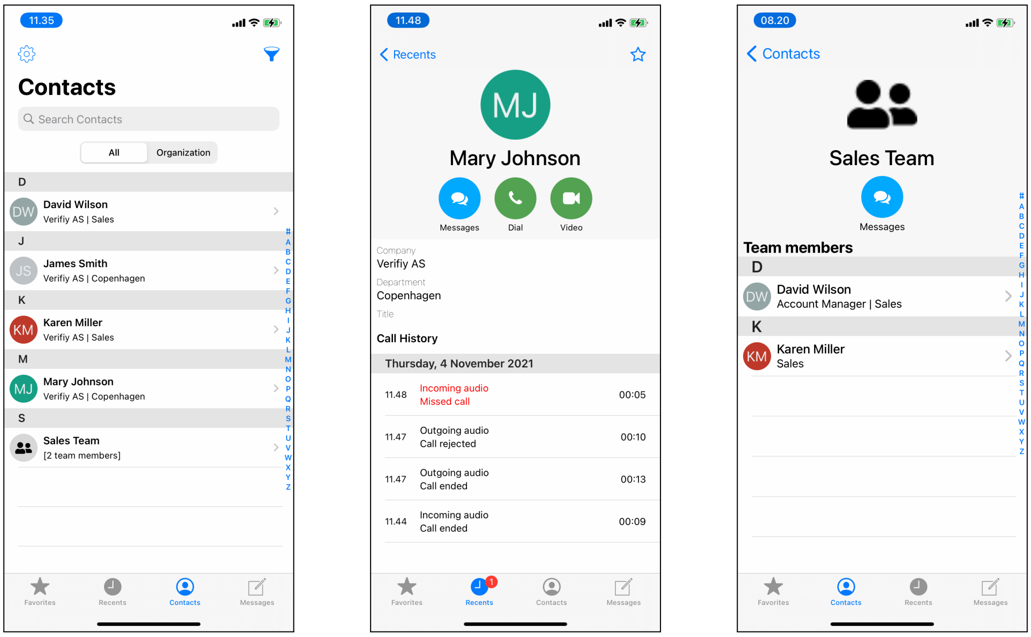
- Skip to a specific letter using the index on the right hand side of the screen, or
- Search for contacts via the search menu, or
- Use the filter option in top-right corner [Filtering the phonebook 4.2.2].
- Structure the contacts by selecting the view option above the list [Phonebook views 4.2.1]

Selecting a contact will open the *Contact details* and allow the user to start a secure 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* to list the members and allow to the exchange messages with the team.

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

[1] Change sorting from the *Settings* menu



11.35

Contacts

Search Contacts

All | Organization

D

David Wilson
Verifiy AS | Sales

J

James Smith
Verifiy AS | Copenhagen

K

Karen Miller
Verifiy AS | Sales

M

Mary Johnson
Verifiy AS | Copenhagen

S

Sales Team
[2 team members]

Favorites | Recents | Contacts | Messages

(a) *Contacts* screen.

11.48

Recents

Mary Johnson

Messages | Dial | Video

Company
Verifiy AS

Department
Copenhagen

Title

Call History

Thursday, 4 November 2021

11.48	Incoming audio Missed call	00:05
11.47	Outgoing audio Call rejected	00:10
11.47	Outgoing audio Call ended	00:13
11.44	Incoming audio Call ended	00:09

Favorites | Recents | Contacts | Messages

(b) Contact details.

08.20

Contacts

Sales Team

Messages

Team members

D

David Wilson
Account Manager | Sales

K

Karen Miller
Sales

Favorites | Contacts | Recents | Messages

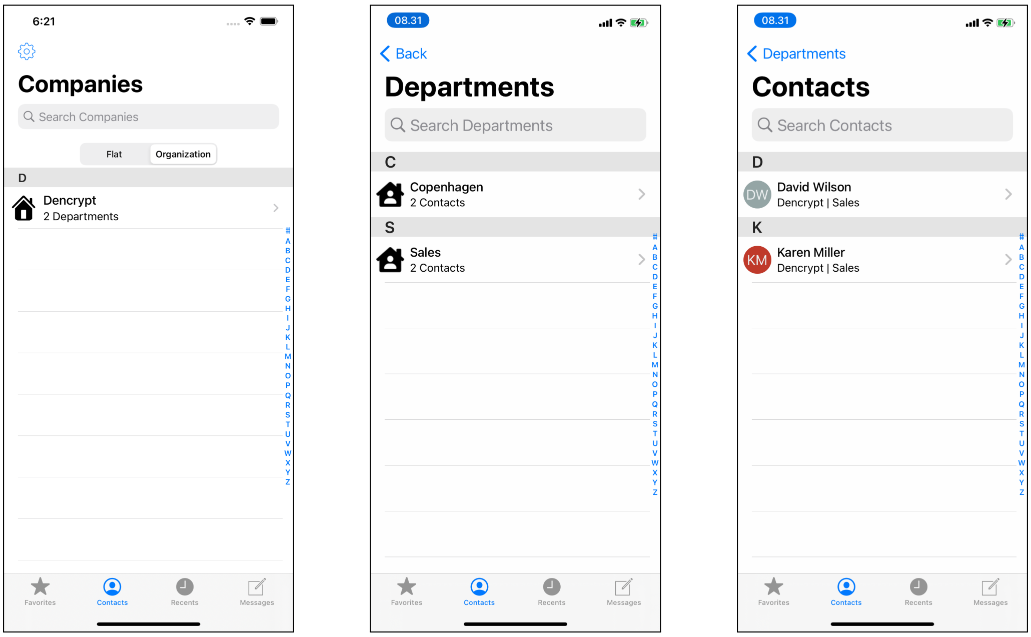
(c) Teamroom details.

Figure 7: Contacts.

4.2.1 Phonebook views

Different views are offered based on the organization the contacts are part of.

The *Organsization* view structures the contacts by two levels: By organization and department. The *All* view shows all contacts in a flat alphabetically ordered list.



6:21

Companies

Search Companies

Flat | Organization

D

Dencrypt
2 Departments

Favorites | Contacts | Recents | Messages

(a) First layer: Companies

08.31

Back

Departments

Search Departments

C

Copenhagen
2 Contacts

S

Sales
2 Contacts

Favorites | Contacts | Recents | Messages

(b) Second layer: Departments

08.31

Departments

Contacts

Search Contacts

D

David Wilson
Dencrypt | Sales

K

Karen Miller
Dencrypt | Sales

Favorites | Contacts | Recents | Messages

(c) Contacts in *departments*

Figure 8: Contacts in *organization* view.

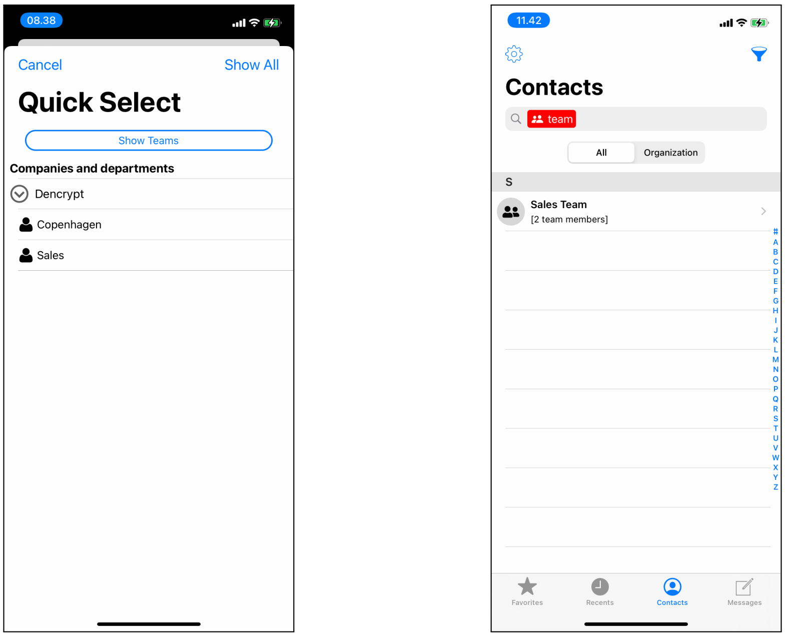
4.2.2 Filtering the phonebook

By default, the entire phonebook is shown. The phonebook can be filtered to show a subset of the contacts by tapping the filter icon. This will open the *Quick Select* screen where contacts can be filtered per company and per department. Tapping *Show Teams* will show team rooms only.

The *Quick Select* screen shows the companies, which can be expanded, to also show departments via the "arrow" on the left of the screen. Tapping on either a company or a department will close the Quick Select screen and filter the phone book accordingly.

The search field in the *Contacts* screen will indicate when a filter is active. Only one filter can be active at a time. A filtered phone book can also be searched via the search field.

A filter can be deleted by opening the Quick Select screen and tap "Show All" or by tapping the search field and delete the filter.



(a) Quick Select

(b) Show Teams

Figure 9: Filtering contacts

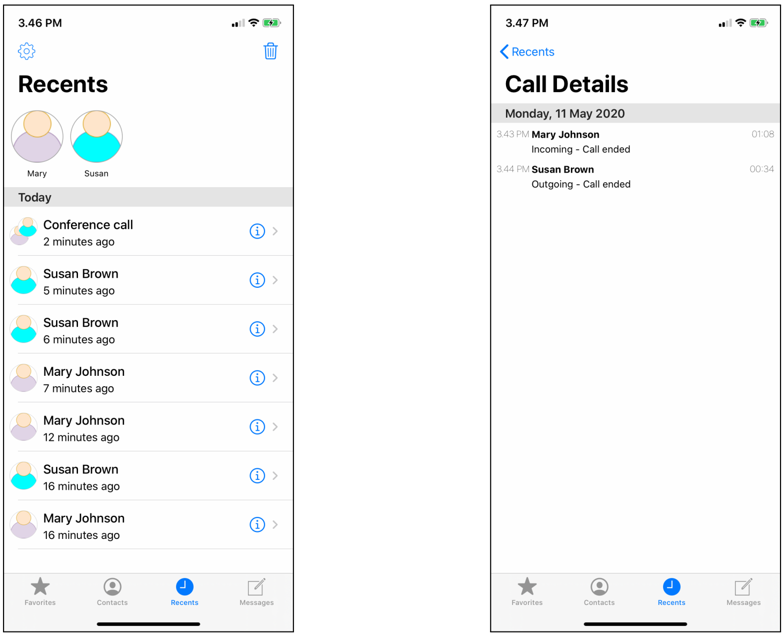
4.3 Recents

The *Recent* screen is divided into two parts. The top row shows the avatar of the most frequently used contacts., while the table below shows the call history in chronological order.

The call history can be deleted by tapping the "trash can" icon in the top-right corner.

The top row contains the most recently used contacts and can be considered an automatically-generated list of favorites. Tapping a contact will slide out a set of buttons allowing the user to start a new call or send a chat message. Tapping the contact again will collapse the buttons.

In the chronological call list, additional call details can be found by tapping the **i**-button on the right of the screen. This will open the *Call Details* screen, which contains the call history for that contact.



3.46 PM

Recents

Mary Susan

Today

Conference call
2 minutes ago

Susan Brown
5 minutes ago

Susan Brown
6 minutes ago

Mary Johnson
7 minutes ago

Mary Johnson
12 minutes ago

Susan Brown
16 minutes ago

Mary Johnson
16 minutes ago

3.47 PM

Recents

Call Details

Monday, 11 May 2020

3:43 PM Mary Johnson 01:08
Incoming - Call ended

3:44 PM Susan Brown 00:34
Outgoing - Call ended

(a) *Recents* screen

(b) Recent call detail

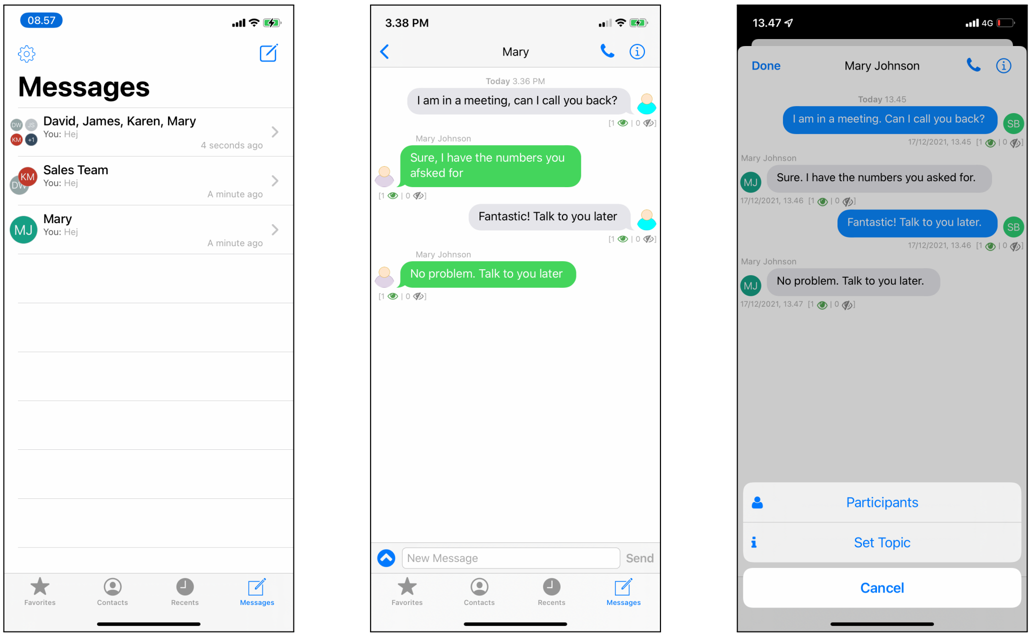
Figure 10: Recents

4.4 Messages

The *Message* screen is used for sending and receiving text messages and attachments (photos, video/audio clips, file sharing and GPS location). It also allows the user to send predefined standard messages.

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

Tapping an entry (chat room) will open up the messages in the conversation. Tapping the ℹ-icon opens a menu for showing a list of participants and for changing the chat room title.



David, James, Karen, Mary
You: Hej
4 seconds ago

Sales Team
You: Hej
A minute ago

Mary
You: Hej
A minute ago

Today 3.36 PM

I am in a meeting, can I call you back?

Mary Johnson

Sure, I have the numbers you afsked for

Fantastic! Talk to you later

Mary Johnson

No problem. Talk to you later

Today 13.45

I am in a meeting. Can I call you back?

17/12/2021, 13.45

Mary Johnson

Sure. I have the numbers you asked for.

17/12/2021, 13.46

Fantastic! Talk to you later.

17/12/2021, 13.46

Mary Johnson

No problem. Talk to you later.

17/12/2021, 13.47

(a) *Messages* screen.

(b) Message conversation.

(c) chat room options.

Figure 11: Messages

Participants can be added or removed from a chat room.

Add/remove participants

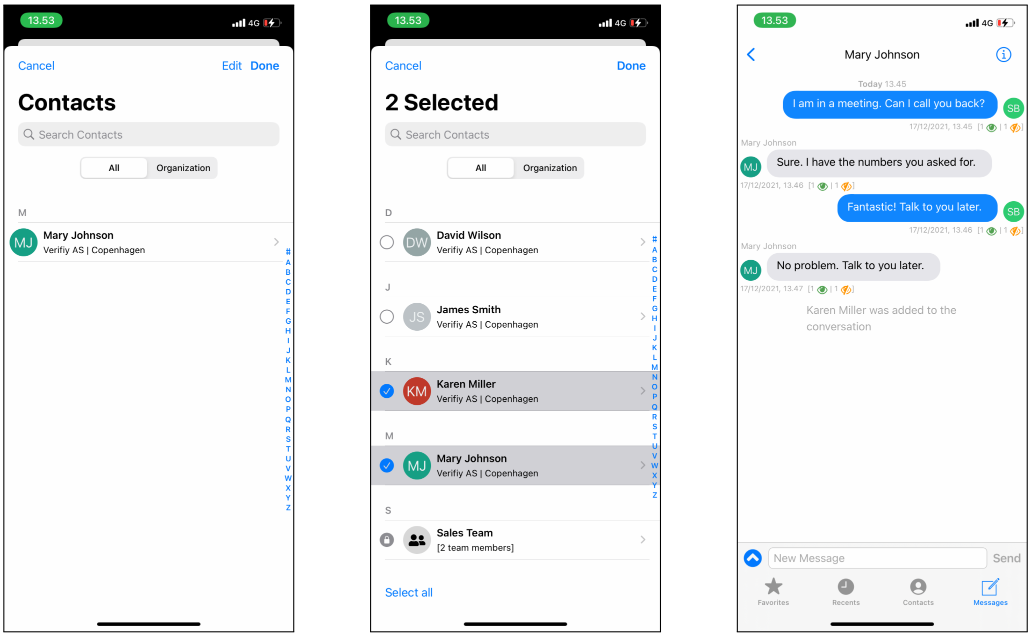
Step 1: Open a chat room and tap ℹ-iconAndroidDevice⁝.

Step 2: Tap *Participants* to diplay a list of chat room members.

Step 3: Tap *Edit* to select or de-select participant.

Step 4: Tap *Done*. The participants of chat room will be notified about the change.

Chatroom can be deleted or marked as favorite. In the chatroom list swipe left on the chat room title to reveal a hidden menu for deleting or mark as favorites. Favorite chatroom are always shown in the top of the list.



Cancel Edit Done

Contacts

Search Contacts

All Organization

M

Mary Johnson
Verifiy AS | Copenhagen

Cancel Done

2 Selected

Search Contacts

All Organization

D

David Wilson
Verifiy AS | Copenhagen

J

James Smith
Verifiy AS | Copenhagen

K

Karen Miller
Verifiy AS | Copenhagen

M

Mary Johnson
Verifiy AS | Copenhagen

S

Sales Team
[2 team members]

Select all

Mary Johnson

Today 13.45

I am in a meeting. Can I call you back?

17/12/2021, 13.45

Mary Johnson

Sure. I have the numbers you asked for.

17/12/2021, 13.46

Fantastic! Talk to you later.

17/12/2021, 13.46

Mary Johnson

No problem. Talk to you later.

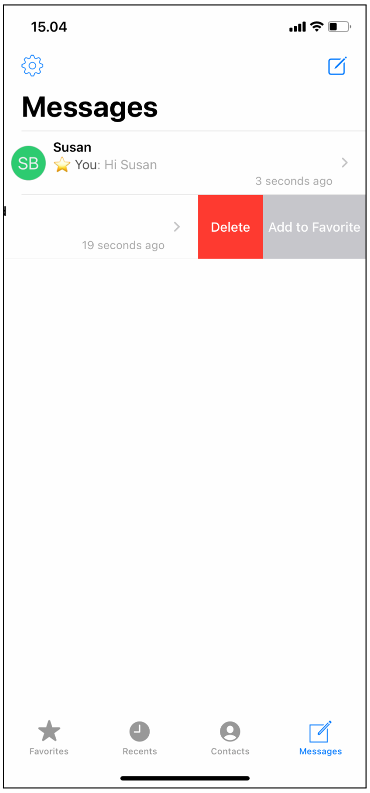
17/12/2021, 13.47

Karen Miller was added to the conversation

New Message Send

(a) chat room members. (b) Select members. (c) Member added.

Figure 12: Add/remove participants.



15.04

Messages

Susan
You: Hi Susan
3 seconds ago

19 seconds ago

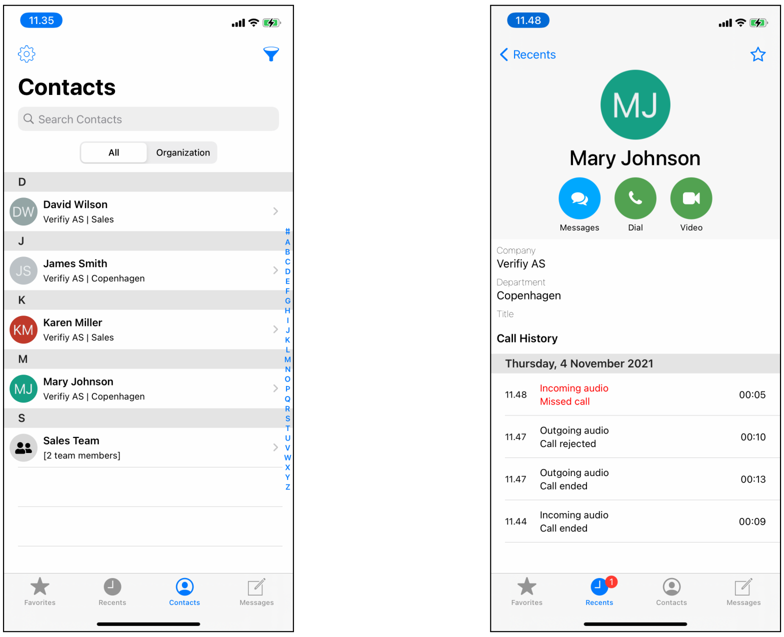
Delete Add to Favorite

Figure 13: Deleting a chatroom.

5 Making a secure call

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

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



11.35

Contacts

Search Contacts

All | Organization

D
David Wilson — Verifiy AS | Sales
J
James Smith — Verifiy AS | Copenhagen
K
Karen Miller — Verifiy AS | Sales
M
Mary Johnson — Verifiy AS | Copenhagen
S
Sales Team — [2 team members]

Favorites · Recents · Contacts · Messages

(a) *Contacts* screen.

11.48

Recents

MJ
Mary Johnson

Messages · Dial · Video

Company
Verifiy AS
Department
Copenhagen
Title

Call History

Thursday, 4 November 2021

11.48	Incoming audio Missed call	00:05
11.47	Outgoing audio Call rejected	00:10
11.47	Outgoing audio Call ended	00:13
11.44	Incoming audio Call ended	00:09

Favorites · Recents · Contacts · Messages

(b) Contact details.

Figure 14: Making calls from *Contacts*

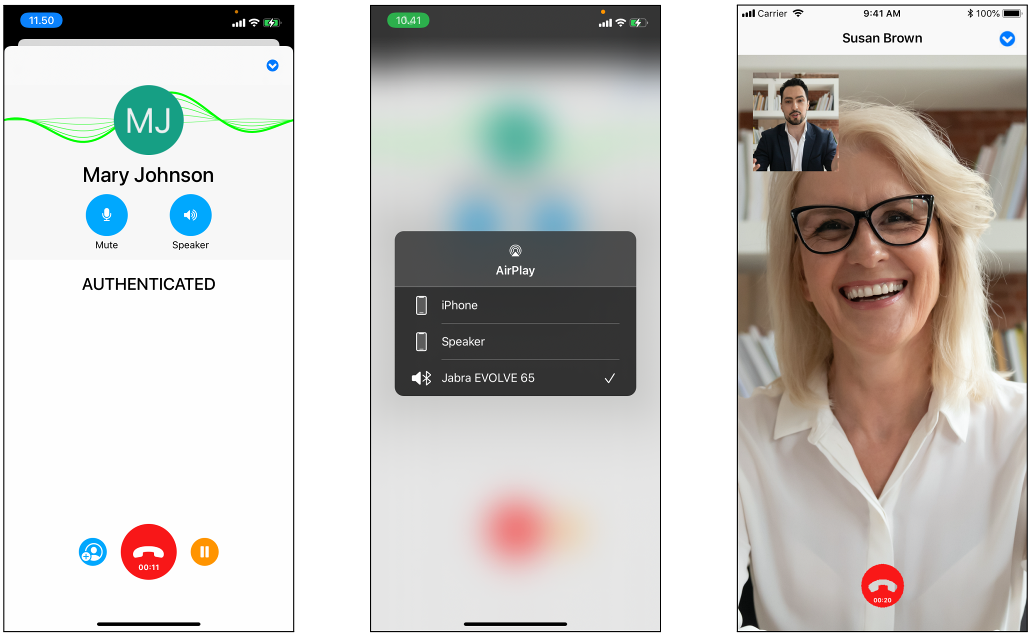
A secure call can only be made when Dencrypt ConnexR has a working internet connection. Secure calls are not possible during flight mode and with a poor data connection. A secure audio call is initiated by tapping the *Dial* button, which opens the *Call* screen. A secure video call is started by tapping 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 ConnexR 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 Figure 15. 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 call. During a secure video call, switching between the front- and the backside camera and disabling the camera is possible.

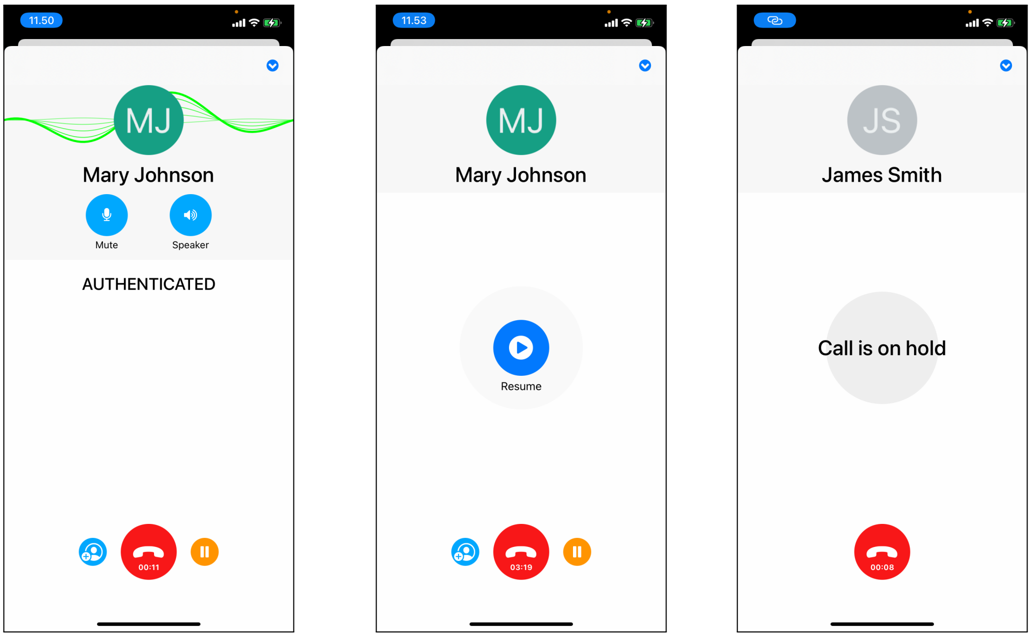
If a Bluetooth device is connected to the device, the speaker button will show a Bluetooth icon. Tapping it will bring up a menu where the audio output can be selected. Be aware of the security risks by applying wireless headsets [Other security recommendations 2.4].



(a) Secured voice call. (b) Bluetooth menu. (c) Secured video call.

Figure 15: In call screens.

A voice call is put on hold by tapping the *Pause* button. The receiving party will hear a pause tone. Tap *Resume* to resume the call.



(a) Tap *Pause* to put a call on hold. (b) Tap *Resume* to resume call. (c) Call on hold. Receiving part.

Figure 16: Call hold

5.1 Voice quality

The top part of the screen displays the call quality. 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**
Green	Good network conditions → Voice quality is high.
Yellow	Some audio artifacts may be heard, but the voice quality should still be understandable.
Orange	Severe audio artifacts and dropouts. Voice quality may be hard to understand.
Red	Data connection is poor → Voice is interrupted.

Table 3: Voice quality indicators

5.2 In-call actions menu

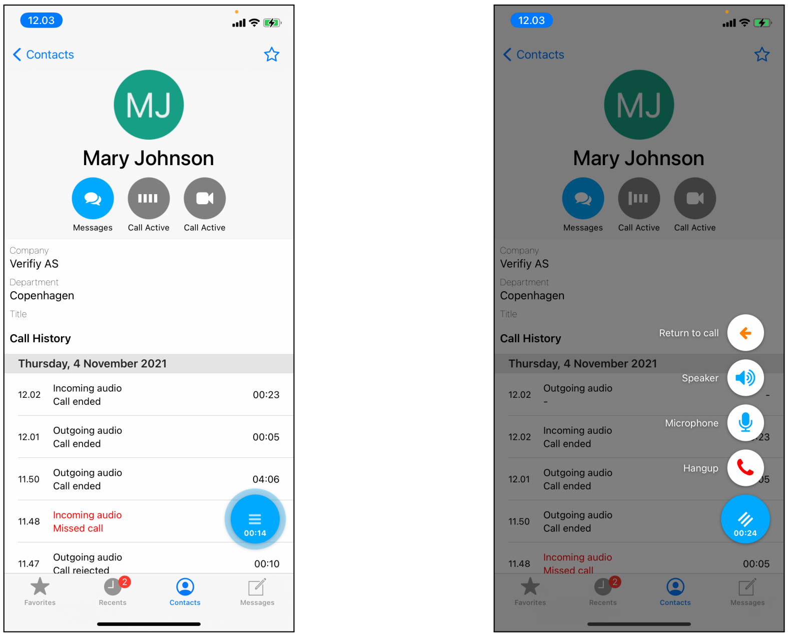
An *In-call action menu* is displayed when a user navigates away from the *Call* screen during a call.

The blue *In-call action menu* button will be shown on the screen while the call is active. Tapping the *In-call action menu* will bring up a menu showing the additional functionality available during the call.

Menu	**Action**
Return to call	Opens the in-call screen.
Speaker	Toggles the speaker on/off
Microphone	Toggle the microphone on/off.
Hangup	Terminates the call.

Table 4: in-call actions

Tapping anywhere outside the in-call actions will close the *In-call action menu*.


12.03
Contacts
MJ
Mary Johnson
Messages
Call Active
Call Active
Company
Verifiy AS
Department
Copenhagen
Title
Call History
Thursday, 4 November 2021
12.02 Incoming audio Call ended 00:23
12.01 Outgoing audio Call ended 00:05
11.50 Outgoing audio Call ended 04:06
11.48 Incoming audio Missed call
11.47 Outgoing audio Call rejected 00:10
00:14
Favorites
Recents
Contacts
Messages
Return to call
Speaker
Microphone
Hangup
00:24

(a) Floating menu.

(b) Actions from floating menu.

Figure 17: *In-call action menu* screen

5.3 Group calls

Once a secure call has been established, additional contacts can be added to the conversation.

Add participants to a secure call.

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

Step 2: Tap the blue ”+ *contact”* icon open the phonebook.

Step 3: Locate a contact in the phonebook and tap *Add to call* . This will pause the ongoing call and establish a new secure call.

Step 4: Combine the two conversations by tapping *Merge*. The first call is resumed and merged with second.

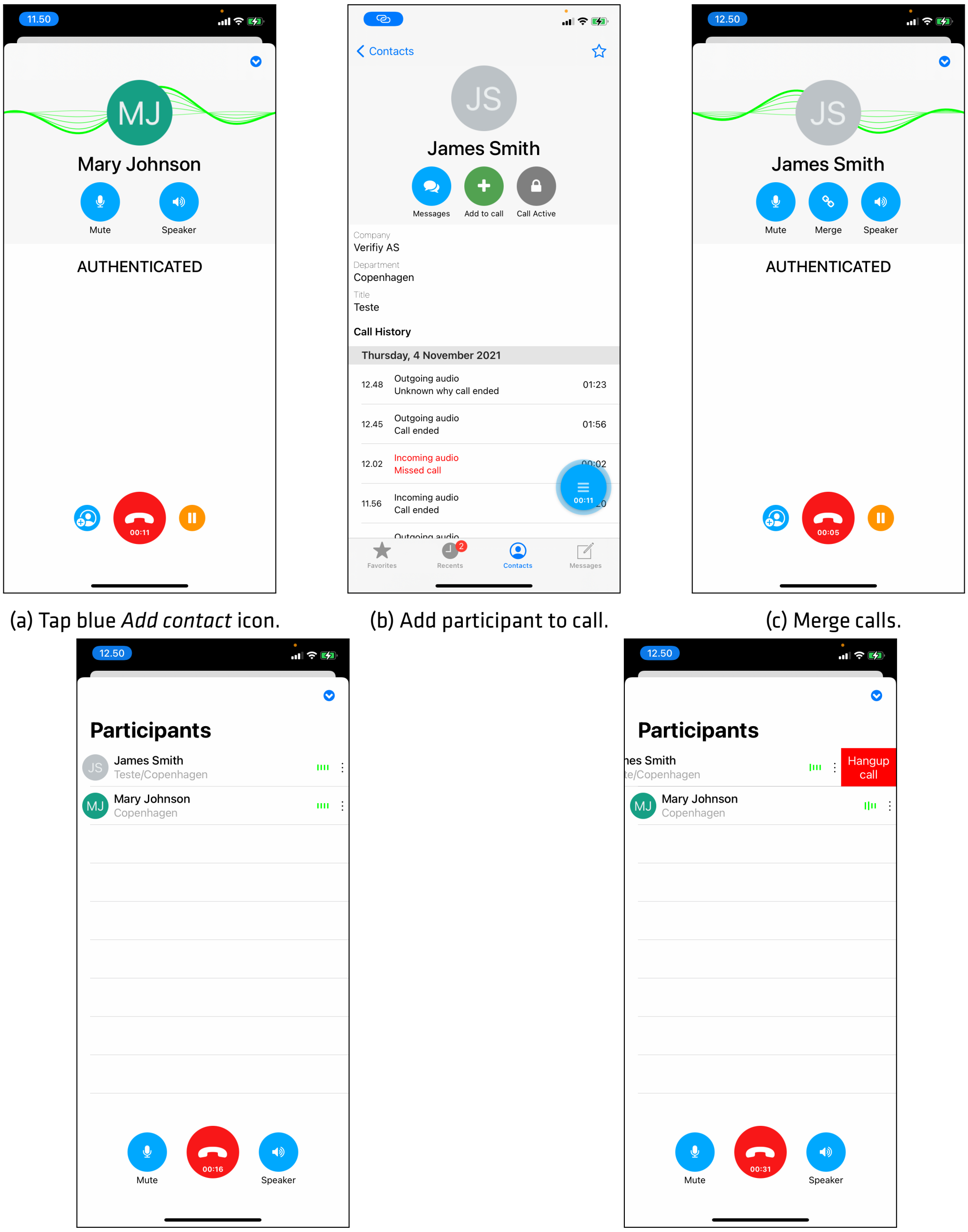
Step 5: The *In-call screen* displays a list of participants.

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

Step 7: Swipe left to put participant on hold or hang-up.

The practical number of participants in a group call is limited by the available bandwidth. 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.



Company
Verifiy AS
Department
Copenhagen
Title
Teste

Call History

Thursday, 4 November 2021

12.48 Outgoing audio
Unknown why call ended 01:23

12.45 Outgoing audio
Call ended 01:56

12.02 Incoming audio
Missed call 00:02

11.56 Incoming audio
Call ended

Outgoing audio

James Smith
Teste/Copenhagen

Mary Johnson
Copenhagen

nes Smith
e/Copenhagen

Mary Johnson
Copenhagen

(a) Tap blue *Add contact* icon. (b) Add participant to call. (c) Merge calls.

(d) Group call established. (e) Swipe left to put participant on hold or hang-up.

Figure 18: Group calls

5.4 Incoming normal 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:

Menu	Action
End and Accept	Terminate the current secure call and accept the incoming call.
Decline	Reject the incoming call.
Hold and Accept	Pause the active secure call. The secure call is resumed by tapping the *Pause* button. (Require *Call waiting* is enabled for the device.)

Table 5: Actions for incoming calls during a secure call.

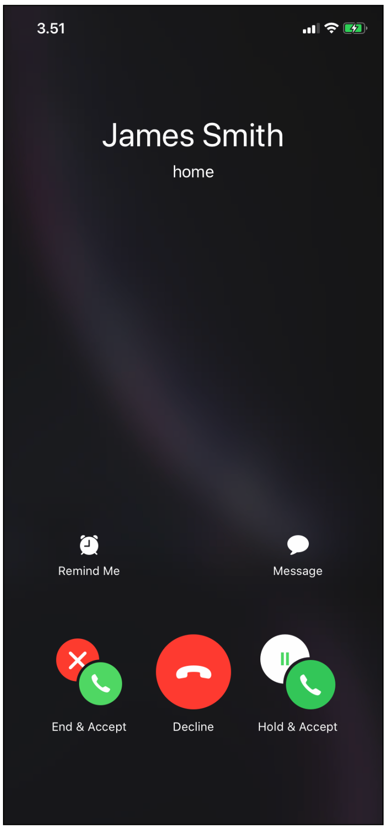


Figure 19: Incoming call during a secure call

5.5 Incoming secure calls

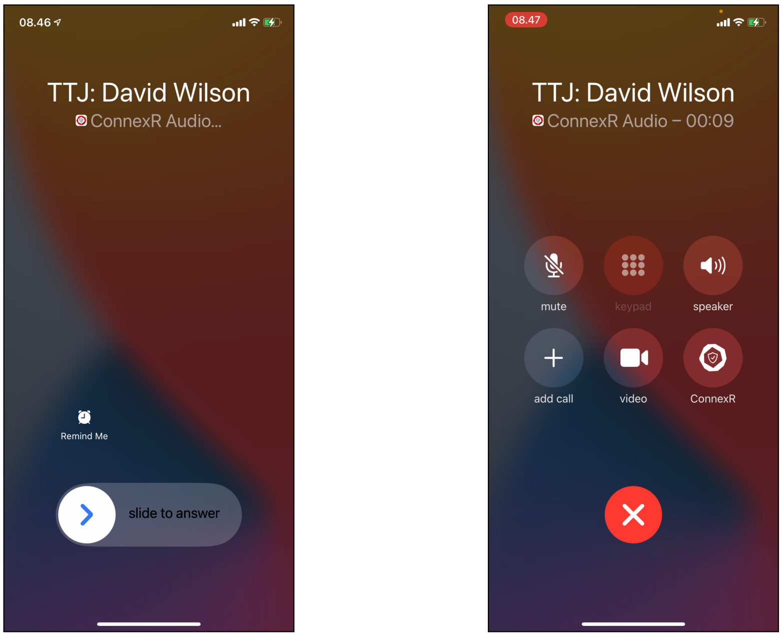
Incoming secure voice calls are alerted using VoIP push notifications, which launch the native iOS call screen. When receiving a secure call, the incoming call screen is displayed, where the name of the caller is shown in large letters followed by *Connex Audio* indicating a secure call.

When answering the call, the Dencrypt ConnexR 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.

From the native call screen, the usual call actions are available.

Menu	Action
Mute	microphone on/off.
Speaker	Toggles the speaker on/off.
Dencrypt ConnexR	Opens Dencrypt ConnexR application.
Add call	Functionality is not available.
Facetime	Functionality is not available.

Table 6: in-call actions from native call screen



(a) Incoming secure call.

(b) Ongoing secure call.

Figure 20: Incoming secure call.

6 Sending a secure message

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

Creating a conversation

Step 1: Tap the ✎-icon in the top-right corner. This opens the *New Message* screen.

Step 2: Add recipients by typing their names (suggestions are shown while typing) or select + to select from the phonebook. Tap a contact name or team room to add them to a conversation.

Sending a secure message

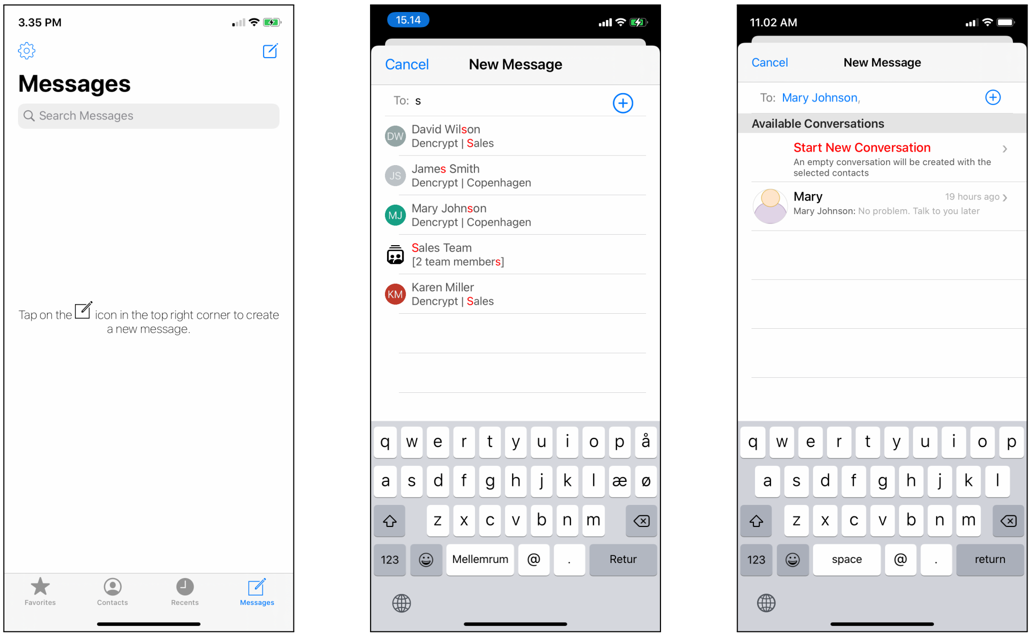
Step 1: Select an existing *Conversation* or tap *Compose* icon to create a new.

Step 2: Enter text and tap *Send*. See Figure 21.

The message is encrypted and transmitted immediately, when an active data connection exist. A successful transmission is indicated by displaying the avatar/logo next to the message.

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 re-send the message.

Notice that sending large attachments will take longer to encrypt and transmit.



3.35 PM

Messages

Search Messages

Tap on the ☐ icon in the top right corner to create a new message.

15.14

Cancel New Message

To: s

DW David Wilson
Dencrypt | Sales

JS James Smith
Dencrypt | Copenhagen

MJ Mary Johnson
Dencrypt | Copenhagen

Sales Team
[2 team members]

KM Karen Miller
Dencrypt | Sales

11.02 AM

Cancel New Message

To: Mary Johnson,

Available Conversations

Start New Conversation
An empty conversation will be created with the selected contacts

Mary 19 hours ago
Mary Johnson: No problem. Talk to you later

(a) Empty inbox. (b) Add participants. (c) Start new conversation.

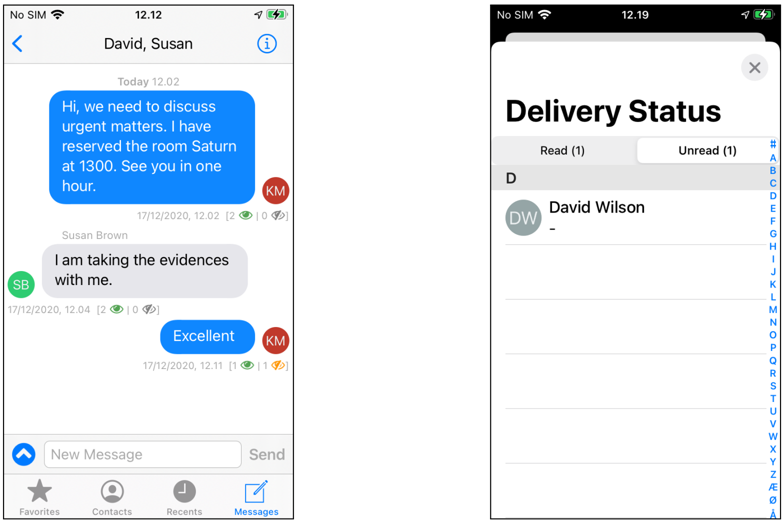
Figure 21: Sending a secure message.

6.1 Message delivery status

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

- The green 👁-icon indicates the number of participants who have opened the message.
- The 👁-icon show the number of participants who have not yet opened the message.

Figure 22 gives a conversation example with all color codes. Detailed delivery status is shown when tapping the delivery status.



Today 12.02

Hi, we need to discuss urgent matters. I have reserved the room Saturn at 1300. See you in one hour.

KM

17/12/2020, 12.02 [2 | 0]

Susan Brown

SB

I am taking the evidences with me.

17/12/2020, 12.04 [2 | 0]

Excellent

KM

17/12/2020, 12.11 [1 | 1]

David Wilson
-

(a) Conversation screen.

(b) Delivery status details.

Figure 22: Message delivery status

6.2 Sending attachments

Sending attachments

Step 1: Open the *Attachment menu* by tapping the ^-icon the lower-left corner.

Step 2: Select the source for attachments.

The available options may differ as the supported attachment are defined by the system administrator.

Camera roll Display the latest pictures and videos from the camera roll for quick selection. Multiple attachments can be selected. Once an attachment has been selected, the "Open Library" menu changes to "Attach X file(s). Tapping this will insert the selected attachments

Open Library Open the photo albums. Multiple attachments can be selected and attached to a message.

Open Camera Open the camera capturing images or videos. Photos and videos taken from the Dencrypt ConnexR will not be stored outside the app and will not appear in photo libraries.

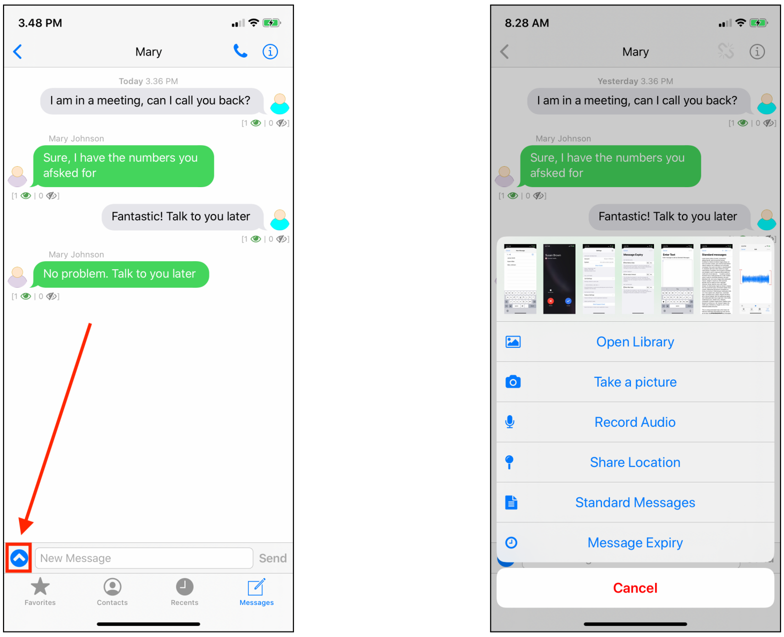
Record Audio Opens the audio recorder. Audio clips will not be stored outside the app and will not appear in any libraries.

Share Location Opens a map showing the current location. The initial pin location is the current position. The pin can be placed at a new location either by dragging it or by "long-press" anywhere on the map.

Standard Messages This will opens a list of pre-defined messages.

Message Expiry Use *Message expiry* to set time constraints on a message availability.

Attachments will be added to the *Attachment browser* located above the compose text field. Attachments can be removed from the message by tapping the ☒-icon on the top-right corner of each attachment. Photos, videos, audio clips, and shared locations generated from within Dencrypt ConnexR will permanently disappear and cannot be recovered when removed from the attachment browser.



I am in a meeting, can I call you back?

Sure, I have the numbers you afsked for

Fantastic! Talk to you later

No problem. Talk to you later

(a) Open attachment menu.

(b) Select attachment type.

Figure 23: Sending attachments.

6.3 Standard messages

Standard messages are a list of pre-defined messages defined by the system administrator or locally by the user.

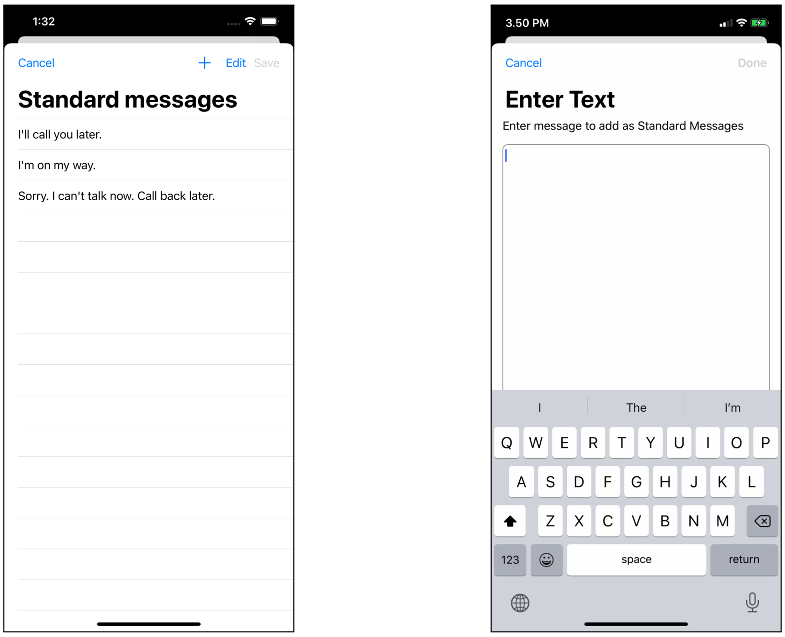
Insert a standard message

Step 1: Tap *Standard Message* to open a list of pre-defined messages.

Step 2: Tap a message to insert the content.

Step 3: Rearrange message by tapping *Edit* and drag messages.

Step 4: Create new standard messages by tapping the ”+” icon. Enter text and tap *Done*.



Standard messages

I'll call you later.

I'm on my way.

Sorry. I can't talk now. Call back later.

Enter Text

Enter message to add as Standard Messages

(a) Standard message.

(b) New standard message

Figure 24: Standard messages

6.4 Message expiry timer

Message expiry is used to set time constraints on a message making it available in defined time periods only.

Set time constraints on messages

Step 1: Tap *Message Expiry* to open the configuration screen.

Step 2: Toggle "Yes/No" on the time constraint options.

Step 3: Enter date or duration.

Step 4: Tap *Insert*

Step 5: The attachment icon will show the selected values on 3 separate lines:

(a) Not Before date.

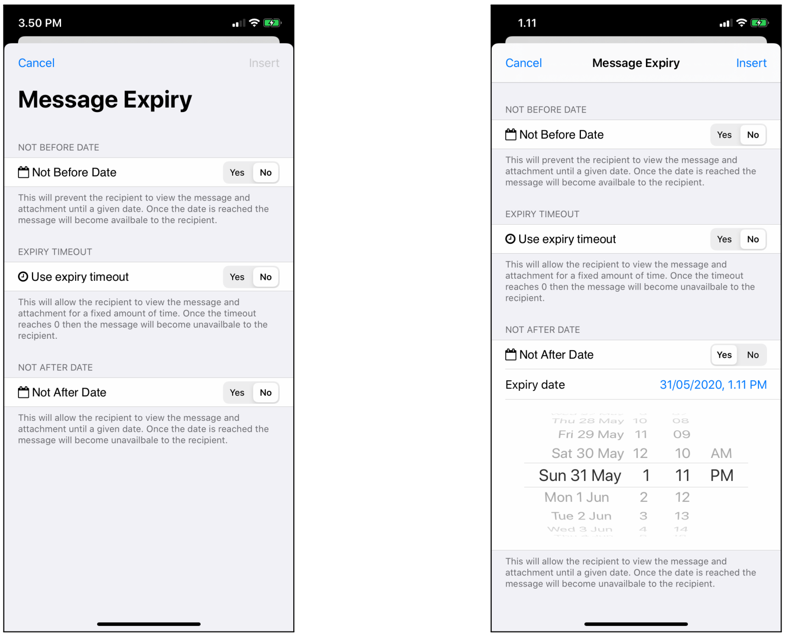
(b) Expiry time.

(c) Not After date.

Not Before The message will not be available for the recipients before this date. The receiver will get a notification when the message becomes available. The message will appear in the chat timeline at the Not Before date and not when it was originally sent.

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

Not After The message will not be available for the recipients after this date.


3.50 PM

Cancel Insert

Message Expiry

NOT BEFORE DATE

Not Before Date Yes No

This will prevent the recipient to view the message and attachment until a given date. Once the date is reached the message will become availbale to the recipient.

EXPIRY TIMEOUT

Use expiry timeout Yes No

This will allow the recipient to view the message and attachment for a fixed amount of time. Once the timeout reaches 0 then the message will become unavailbale to the recipient.

NOT AFTER DATE

Not After Date Yes No

This will allow the recipient to view the message and attachment until a given date. Once the date is reached the message will become unavailbale to the recipient.

(a) Message expiry options.

1.11

Cancel Message Expiry Insert

NOT BEFORE DATE

Not Before Date Yes No

This will prevent the recipient to view the message and attachment until a given date. Once the date is reached the message will become availbale to the recipient.

EXPIRY TIMEOUT

Use expiry timeout Yes No

This will allow the recipient to view the message and attachment for a fixed amount of time. Once the timeout reaches 0 then the message will become unavailbale to the recipient.

NOT AFTER DATE

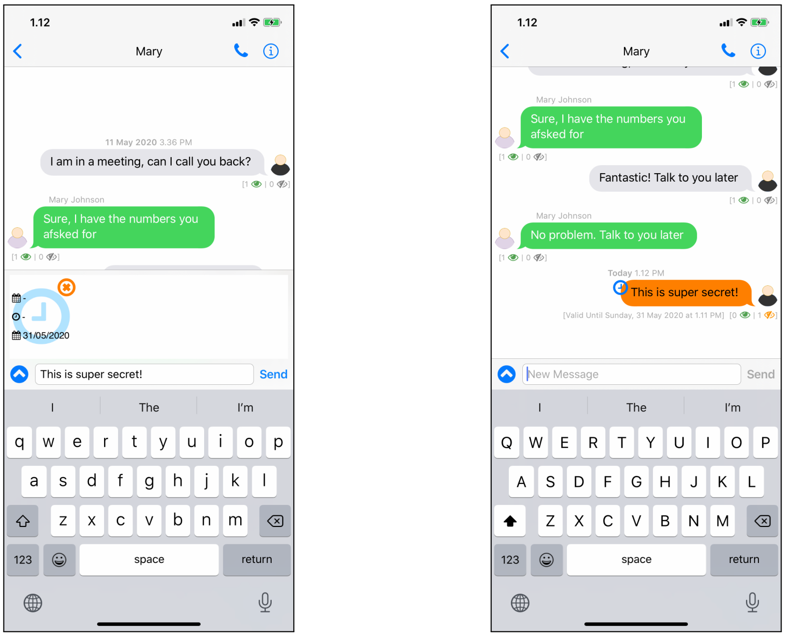
Not After Date Yes No

Expiry date 31/05/2020, 1.11 PM

This will allow the recipient to view the message and attachment until a given date. Once the date is reached the message will become unavailbale to the recipient.

(b) Message with time constraints.

Figure 25: Message expiry


1.12

Mary

11 May 2020 3.36 PM

I am in a meeting, can I call you back?

[1 | 0]

Mary Johnson

Sure, I have the numbers you afsked for

[1 | 0]

-

-

31/05/2020

This is super secret! Send

(a) When typing.

1.12

Mary

[1 | 0]

Mary Johnson

Sure, I have the numbers you afsked for

[1 | 0]

Fantastic! Talk to you later

[1 | 0]

Mary Johnson

No problem. Talk to you later

[1 | 0]

Today 1.12 PM

This is super secret!

[Valid Until Sunday, 31 May 2020 at 1.11 PM] [0 | 1]

New Message Send

(b) Constrained message in chat.

Figure 26: Message expiry

7 Settings

Dencrypt ConnexR settings are opened by tapping the ”cogwheel”-icon in the top left corner of the screen. Most of the configuration of Dencrypt ConnexR is performed centrally by the system administrator. The *Settings* menu provides the following information/options:

Account Displays the user's name.

Show System Info Displays the following information in a new window. For error investigation, this information can be exported.

- The account name, account id and system name.
- The app name, app version. SDK version and client ID.
- The root cert version.
- The client certificate expiry date.
- The common name (CN) of the MDM pushed provisioning client (if applicable).
- App bundle id
- OS version, Device name and Device type.
- A timestamp for information.

Show Guide Opens a quick guide to Dencrypt ConnexR .

Status Server connection status.

App version Dencrypt ConnexR version number

App version Version number of Dencrypt ConnexR .

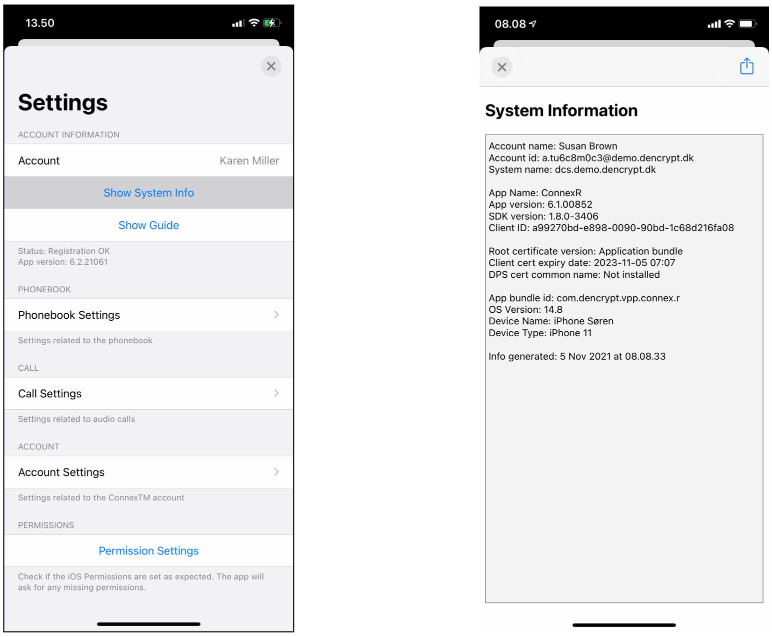
Phonebook Settings From the phonebook settings, the user can change the default settings for launch page, phonebook sorting and display.

Call Settings From the call settings menu, the user can change the default settings for:

- Customize ringing tone
- Toggle if screen shall be off during calls or controlled by proximity sensor.
- Toggle Tunnel mode. Used in VoIP blocking regions (Default: Off).

Account Settings From the account settings menu, the user can change default settings for the badge icon, the launch screen, and delete the account.

Permission Settings Checks app permissions.



13.50

Settings

ACCOUNT INFORMATION

Account Karen Miller

Show System Info

Show Guide

Status: Registration OK
App version: 6.2.21061

PHONEBOOK

Phonebook Settings

Settings related to the phonebook

CALL

Call Settings

Settings related to audio calls

ACCOUNT

Account Settings

Settings related to the ConnexTM account

PERMISSIONS

Permission Settings

Check if the iOS Permissions are set as expected. The app will ask for any missing permissions.

(a) Settings menu.

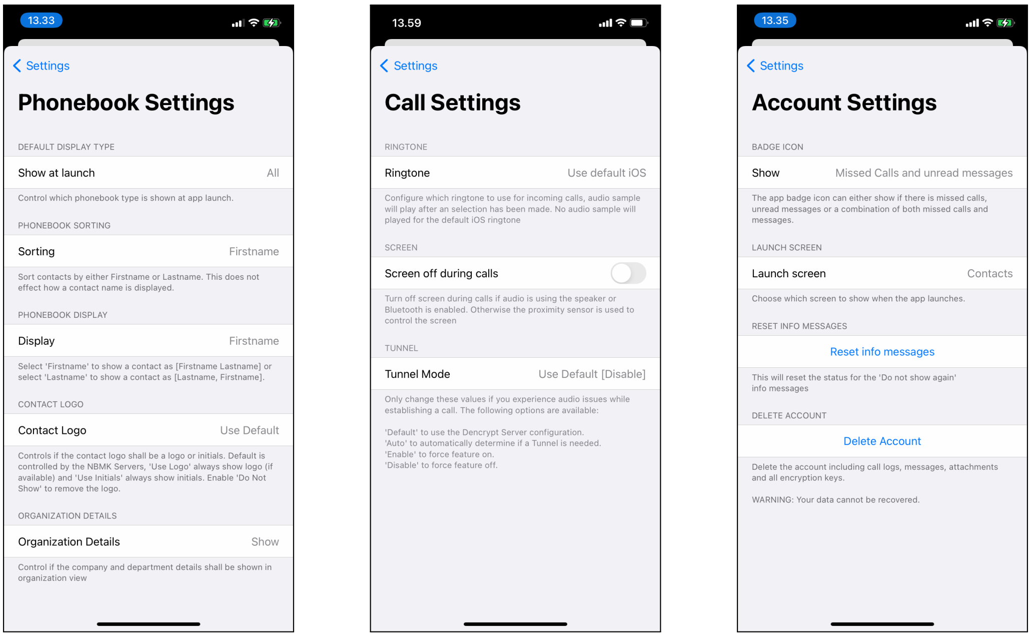
08.08

System Information

```
Account name: Susan Brown
Account id: a.tu6c8m0c3@demo.dencrypt.dk
System name: dcs.demo.dencrypt.dk

App Name: ConnexR
App version: 6.1.00852
SDK version: 1.8.0-3406
Client ID: a99270bd-e898-0090-90bd-1c68d216fa08

Root certificate version: Application bundle
Client cert expiry date: 2023-11-05 07:07
DPS cert common name: Not installed

App bundle id: com.dencrypt.vpp.connex.r
OS Version: 14.8
Device Name: iPhone Søren
Device Type: iPhone 11

Info generated: 5 Nov 2021 at 08.08.33
```

(b) App Information.

Figure 27: Settings and app information.



Phonebook Settings

DEFAULT DISPLAY TYPE

Show at launch	All

Control which phonebook type is shown at app launch.

PHONEBOOK SORTING

Sorting	Firstname

Sort contacts by either Firstname or Lastname. This does not effect how a contact name is displayed.

PHONEBOOK DISPLAY

Display	Firstname

Select 'Firstname' to show a contact as [Firstname Lastname] or select 'Lastname' to show a contact as [Lastname, Firstname].

CONTACT LOGO

Contact Logo	Use Default

Controls if the contact logo shall be a logo or initials. Default is controlled by the NBMK Servers, 'Use Logo' always show logo (if available) and 'Use Initials' always show initials. Enable 'Do Not Show' to remove the logo.

ORGANIZATION DETAILS

Organization Details	Show

Control if the company and department details shall be shown in organization view

Call Settings

RINGTONE

Ringtone	Use default iOS

Configure which ringtone to use for incoming calls, audio sample will play after an selection has been made. No audio sample will played for the default iOS ringtone

SCREEN

Screen off during calls	○

Turn off screen during calls if audio is using the speaker or Bluetooth is enabled. Otherwise the proximity sensor is used to control the screen

TUNNEL

Tunnel Mode	Use Default [Disable]

Only change these values if you experience audio issues while establishing a call. The following options are available:

'Default' to use the Dencrypt Server configuration.
'Auto' to automatically determine if a Tunnel is needed.
'Enable' to force feature on.
'Disable' to force feature off.

Account Settings

BADGE ICON

Show	Missed Calls and unread messages

The app badge icon can either show if there is missed calls, unread messages or a combination of both missed calls and messages.

LAUNCH SCREEN

Launch screen	Contacts

Choose which screen to show when the app launches.

RESET INFO MESSAGES

Reset info messages

This will reset the status for the 'Do not show again' info messages

DELETE ACCOUNT

Delete Account

Delete the account including call logs, messages, attachments and all encryption keys.

WARNING: Your data cannot be recovered.

(a) Phonebook settings.

(b) Call settings.

(c) Account settings.

Figure 28: Phonebook, call and account settings.

Appendices

A Dencrypt Communication Solution

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

The solution consists of Dencrypt ConnexR , a smartphone application (app) installed to the end-users smartphone, and a Dencrypt Server System as illustrated in Figure 29. The Dencrypt Server System is responsible for setting up the encrypted calls , for routing messages, 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 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 ConnexR application is installed by a Mobile-Device-Management (MDM) system. The Dencrypt Server System is managed by a system administrator.

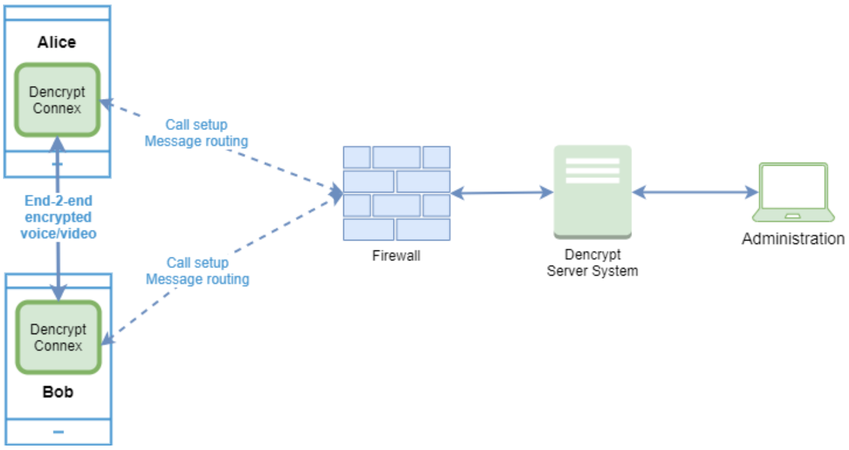


Figure 29: Dencrypt Communication Solution.

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 30

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.

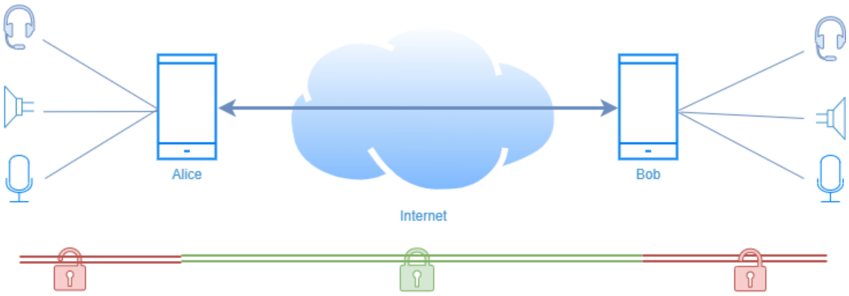


Figure 30: Area of protection for voice/video calls.

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 31.

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.

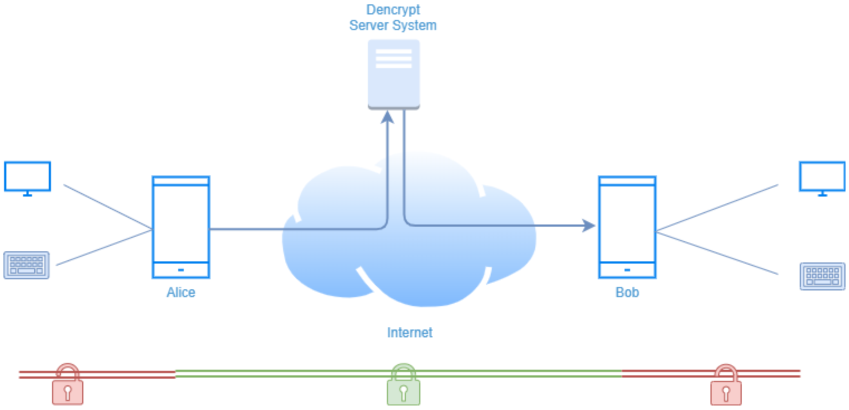


Figure 31: Area of protection for instant messaging

A.3 Authenticated connections

All communication between the Dencrypt ConnexR 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 both 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.

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.

A.6 Push notifications

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

B Errors messages

Terms and Conditions - Please accept the following: I have read and understood the security instructions for my organization

- **Type:**
- **Description:** The user needs to indicate that the security instructions have been read
- **Actions:**

Please Restart App - A push token is not received from Apple, it's not possible to receive VoIP calls without it. Please restart app.

- **Type:**
- **Description:** The application did not receive a push token from Apple. The token is needed to receive calls and messages.
- **Actions:**

Token Error - Your token is invalid, please restart the application.If this issue persists then please contact support.

- **Type:** ERROR

- **Description:** The push token received from Apple was in an unknown format. Without a valid push token then the user will not be able to receive calls.
- **Actions:** Restart the application. If the issue persists then Dencrypt Support shall be contacted.

Please Restart - Your push token has been invalidated, please restart the application.If the this issue persists then please contact support.

- **Type:** ERROR
- **Description:** Apple has invalidated the push token. Without a valid push token then the user will not be able to receive calls.
- **Actions:** Restart the application. If the issue persists then Dencrypt Support shall be contacted.

Application Starting - Please wait while application is starting

- **Type:** INFO
- **Description:** The application is starting
- **Actions:**

Screenshot Detected - A screenshot was taken.

- **Type:** INFO
- **Description:** The user took a screenshot of the application
- **Actions:**

Recording Detected - Screen recording active.

- **Type:** INFO
- **Description:** The user has screen recording active
- **Actions:**

Live Chat Received - A Live Chat fromswas received. This feature is not supported, please inform the sender.

- **Type:** INFO
- **Description:** The user has received an unsupported live chat from Talk
- **Actions:**

A unrecoverable error has been detected. Please contact the system administrator. -

- **Type:** ERROR
- **Description:** A fatal error has been detected
- **Actions:**

A security incident was detected and your call has been terminated. Please contact your system administrator. -

- **Type:** INFO
- **Description:** A security issue was detected
- **Actions:**

Your device has been revoked and no longer has access. Please contact your system administrator. -

- **Type:** INFO
- **Description:** A security issue was detected
- **Actions:**

Network Issue - Server connection refused

- **Type:** ERROR
- **Description:** The was an issue connecting to the internet
- **Actions:**

Call is authenticated, a secure channel is established. -

- **Type:** INFO
- **Description:** Shown when a secure channel is established when receiving a call while the application is running in the background
- **Actions:**

Account Needed - Please contact your administrator for an account to Dencrypt ConnexR . Your account can be delivered via email, text message or QR code.

- **Type:** INFO
- **Description:** The application has no account
- **Actions:** An account invitation shall be generated by the company administrator. The invitation can either be received via sms, email or a QR code. The user cannot make call nor send messages without an account.

App Information - The app information has been copied to the clipboard

- **Type:** INFO
- **Description:** App information has been copied to the clipboard
- **Actions:** Information can be shared

App information - The application is locked until the user is authenticated

- **Type:** INFO
- **Description:** The application is locked until the user is authenticated.
- **Actions:**

Database Locked - Please wait while the database is decrypting

- **Type:** INFO
- **Description:** The application database is encrypted and locked until the decryption key has been downloaded from the Dencrypt Servers.
- **Actions:**

System Maintenance - Please wait while the system is in maintenance

- **Type:** INFO
- **Description:** The Dencrypt servers are in maintenance.
- **Actions:**

Remove contact - Do you want to be removed from this conversation?

- **Type:** INFO
- **Description:** Shown when the user wants to remove a contact from a conversation
- **Actions:**

- An account already exists, provisioning stopped.

- **Type:** INFO
- **Description:** The user used an invitation on an application which already have an account.
- **Actions:**

- There was an issue with the invitation, please contact your administrator.

- **Type:** INFO
- **Description:** There was en error with the invitation.
- **Actions:**

- The Dencrypt servers could not be contacted, please verify that the internet connection is working and try again.

- **Type:** INFO
- **Description:** There was not connection to the server.
- **Actions:**

- Dencrypt ConnexR did not have a valid account, please contact your administrator to get a Dencrypt ConnexR account.

- **Type:** INFO
- **Description:** The migration failed because Talk did not have an account
- **Actions:**

- The application will be updated to the latest version, this will take a few seconds.

- **Type:** INFO
- **Description:** The application is being updated to a new version
- **Actions:**

Please wait - Your account is being configured.This may take a few minutes.Do not close the app.

- **Type:** INFO
- **Description:** An account is being setup
- **Actions:**

Account Ready - Your Dencrypt ConnexR account is now ready.

- **Type:** INFO
- **Description:** The account is ready
- **Actions:**

User busy - The contact was busy

- **Type:** INFO
- **Description:** The contact was busy and rejected the call
- **Actions:**

Missed call -

- **Type:** INFO
- **Description:** The user received a call but did not answer it before the caller ended the call
- **Actions:**

Call rejected - Tap to send a message to @

- **Type:** INFO
- **Description:** The user rejected an incoming call. Tapping the notification will open the predefined standard messages and allow the user to send a message to the caller.
- **Actions:**

Unsent Messages - There are messages waiting to be sent, please open Dencrypt ConnexR to send them.

- **Type:** INFO
- **Description:** There are pending messages that didn't get sent while the application was running. This might be due to bad network conditions or large attachments.
- **Actions:** Restart the application to send the pending messages.

Not Found - The attachment download is pending, please try again later.

- **Type:** INFO
- **Description:** The selected attachment is not downloaded from the Dencrypt Servers yet.
- **Actions:**

Attachment found - Attachment is inserted at new message start.

- **Type:** INFO
- **Description:** An attachment was shared from a 3rd party application. It's placed on an internal clipboard and will be added once the user start to compose a message.
- **Actions:**

Permission Check - Permission check completed

- **Type:** INFO
- **Description:** The user started an iOS permission check which is now completed
- **Actions:**

Clear Recent - Are you sure that the Recent list shall be cleared?

- **Type:** INFO
- **Description:** Confirmation dialog asking if the user wants to clear the recent call list
- **Actions:**

Message Ready - A Message was scheduled to become available now

- **Type:** INFO
- **Description:** A message which had a not-before date is now ready to the read
- **Actions:**

App update available - There is a new version of Dencrypt ConnexR available, please update your app

- **Type:** INFO
- **Description:** There is a new version of the application available on the Apple App Store.
- **Actions:**

Subject Changed - Participant Changed

- **Type:** INFO
- **Description:** The user changed the subject
- **Actions:**

New message received -

- **Type:** INFO
- **Description:** A new message was received
- **Actions:**

Message Expired - [This message is no longer available]

- **Type:** INFO
- **Description:** The user tapped a message or attachment which no longer is available.
- **Actions:**

Loading Attachment - Please wait while decrypting attachment.

- **Type:** INFO
- **Description:** The attachment is being decrypted.
- **Actions:**

Attachment To Large - The attachment is to large and cannot be attached to this message. Max supported size is s

- **Type:** ERROR
- **Description:** The selected attachment is too large to be sent
- **Actions:**

Offline Messages - There are messages waiting to be delivered, they will automatically be transmitted once connection to the server is established.

- **Type:** INFO
- **Description:** There is messages waiting to be send once a connection to the Dencrypt Servers has been established
- **Actions:**

Video Limit - Video recordings can maximum be d seconds. Recoding will automatically stop once this limit is reached.

- **Type:** INFO
- **Description:** There is a maximum time limit on video recordings. After the specified time the recording will automatically stop
- **Actions:**

Attachment detected - The attachment will be inserted when composing a message text starts

- **Type:** INFO
- **Description:** The user has selected an attachment which is now ready to be attached to a message
- **Actions:**

Contacts removed - The following contacts were removed since they are no longer in the phonebook:@

- **Type:** INFO
- **Description:** The user start to compose a new message when a selected contact was removed from the phonebook. The removed contact is removed from the message.
- **Actions:**

Location Disabled - Please enable location sharing in iOS Settings.

- **Type:** INFO
- **Description:** Locations cannot be shared with the application having permissions from iOS
- **Actions:**

Cannot Send Location - There is no contacts set for instant location sharing, please contact your administrator.Location has not been sent.

- **Type:** INFO
- **Description:** The user used instant location share but no contacts was configured on the Dencrypt Servers
- **Actions:**