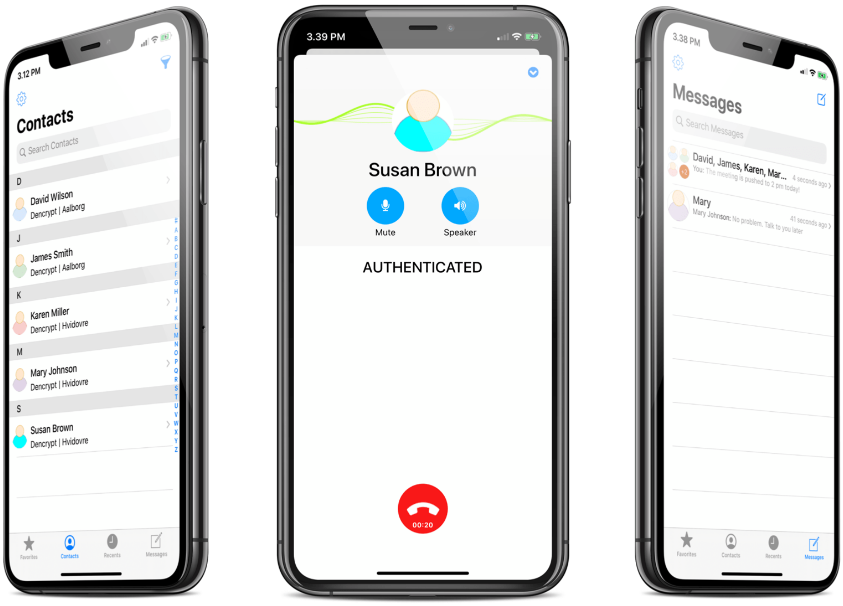
DENCRYPT

Dencrypt Communication Solution

Operational user guide

Dencrypt Connex for iOS

v. 6.5



August 7, 2023

Public

Contents

Version

This guide applies for:

- Dencrypt Connex v. 6.5 for iOS devices.

The version number can be verified from the Settings menu by tapping the ⚙-symbol in the upper-left corner of the screen. See Figure 36.

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:

- iOS devices (iPhone/iPad)

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 and 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 Section 3	Security instructions Getting started	**Essential**
Section 4 Section 5 Section 6 Section 7	Using Dencrypt Connex 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 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 the Apple Appstore. Either as a direct installation from the public Apple Appstore or from the Apple Business Manager via 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. The Dencrypt Connex 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 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 recognization** - 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

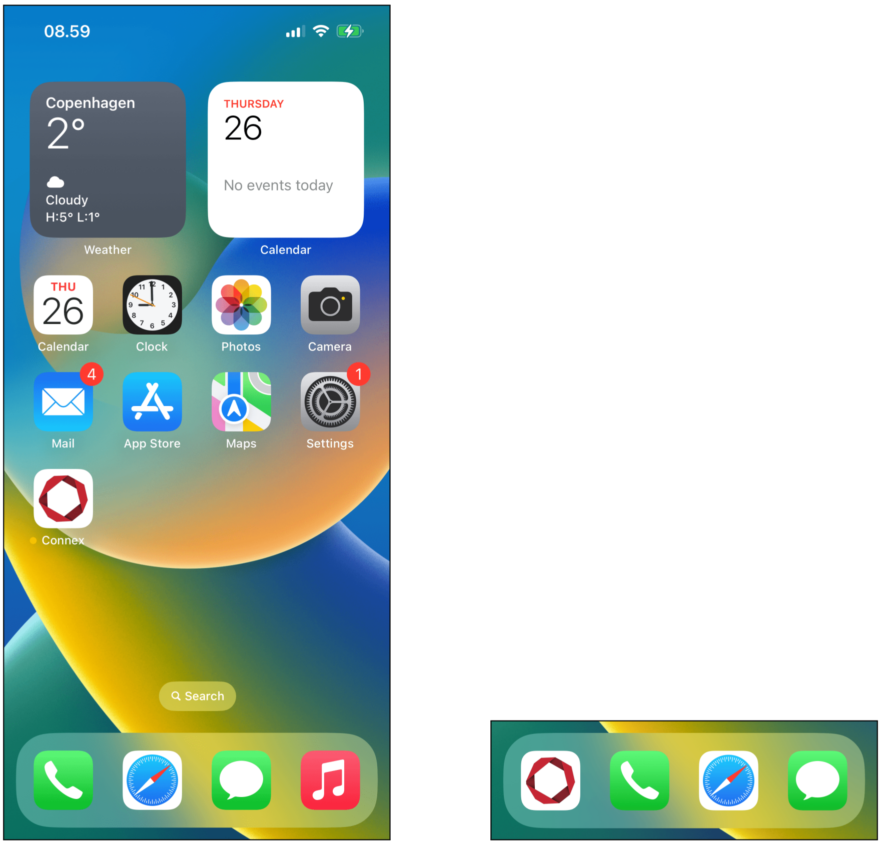
3.1 Installation

Dencrypt Connex is installed via:

- Public Apple App Store for direct installation on end-user devices.
- Apple Business Manager for installation to end-user devices via an MDM.

Links to Dencrypt Connex on the public App stores are available from the Dencrypt webpage: 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.



(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.

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.

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.**

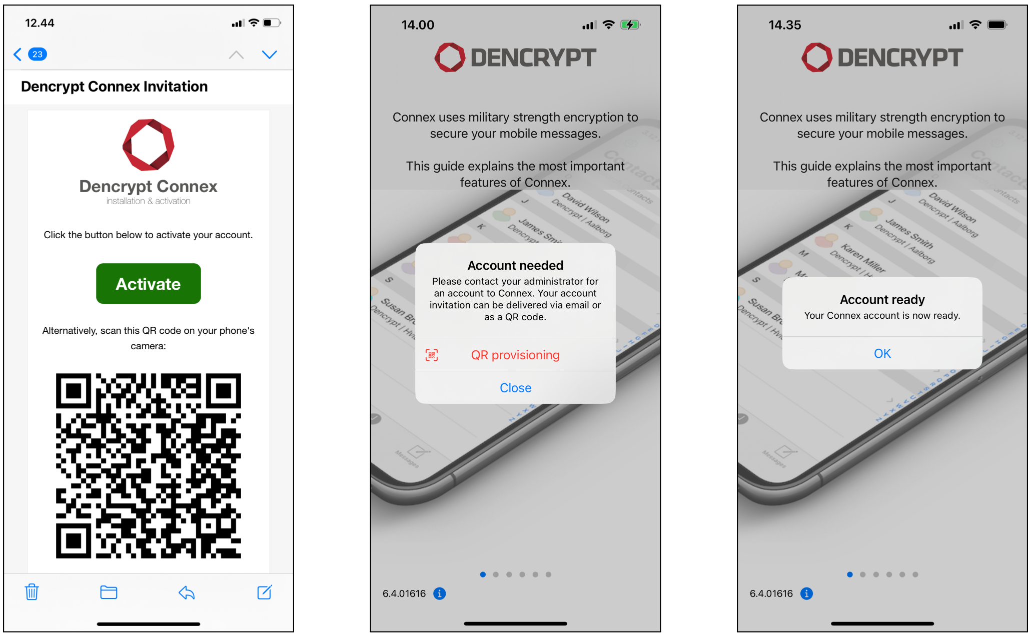
Step 4: Once completed, tap OK to open the app.

Step 5: Scroll through the quick guide and tap close on the last page.

Step 6: The app will request permissions to the device resources for full functionality. Tap Allow for each permission. See [Set permissions 3.3].

Step 7: Dencrypt Connex will connect to the server system to download the phonebook.

Step 8: Dencrypt Connex is now ready for use.



12.44

Dencrypt Connex Invitation

Dencrypt Connex
installation & activation

Click the button below to activate your account.

Activate

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

14.00

DENCRYPT

Connex uses military strength encryption to secure your mobile messages.

This guide explains the most important features of Connex.

Account needed
Please contact your administrator for an account to Connex. Your account invitation can be delivered via email or as a QR code.

QR provisioning

Close

6.4.01616

14.35

DENCRYPT

Connex uses military strength encryption to secure your mobile messages.

This guide explains the most important features of Connex.

Account ready
Your Connex account is now ready.

OK

6.4.01616

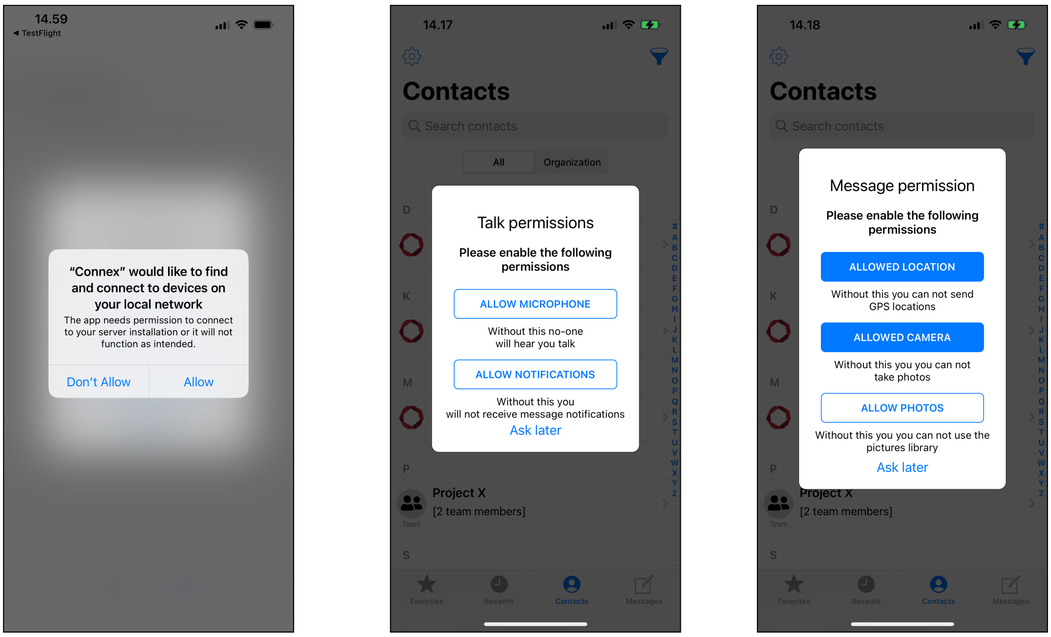
(a) Email invitation (b) QR provisioning. (c) Activation successfully.

Figure 2: Invitations and activation.

3.3 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 if not granted.

During the account setup, Dencrypt Connex will ask for permission for the following resources:



14.59
◂ TestFlight

"Connex" would like to find and connect to devices on your local network
The app needs permission to connect to your server installation or it will not function as intended.

Don't Allow | Allow

14.17

Contacts

Search contacts

All | Organization

Talk permissions

Please enable the following permissions

ALLOW MICROPHONE

Without this no-one will hear you talk

ALLOW NOTIFICATIONS

Without this you will not receive message notifications

Ask later

Project X
[2 team members]

14.18

Contacts

Search contacts

Message permission

Please enable the following permissions

ALLOWED LOCATION

Without this you can not send GPS locations

ALLOWED CAMERA

Without this you you can not take photos

ALLOW PHOTOS

Without this you you can not use the pictures library

Ask later

Project X
[2 team members]

(a) Local network (wifi) permission. (b) Mandatory permissions (c) Optional permissions

Figure 3: Permissions.

Permission	Reason	
Local network	Required to connect through local wifi.	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
Camera	Required to capture images to attach to messages.	Optional
Photo	Required to attach images from the photo album.	Optional

Table 2: Permision usage.

3.4 Revoked application

The system administrator may revoke the Dencrypt Connex access to the server system, which will result in a Security Issue message (Figure 4). 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:

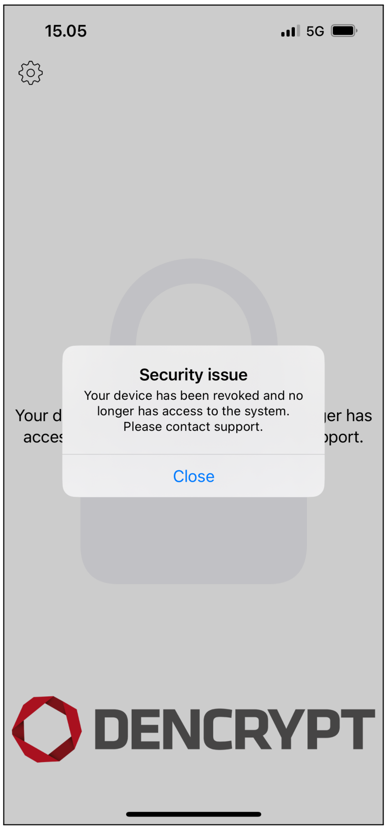
Delete account

Step 1: Tap ⚙-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.



15.05

Security issue

Your device has been revoked and no longer has access to the system. Please contact support.

Figure 4: Revoked access to the server system.

4 Using Dencrypt Connex

Dencrypt Connex offers two main functionalities:

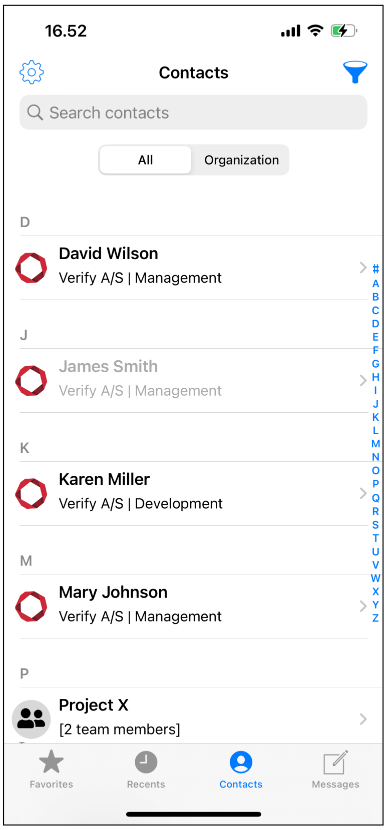
- Secure voice/video communication
- Secure instant messaging of text and content (attachments).

The functionalities are accessible from the main screen. The icons in the menu bar at the bottom provide 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 ⚙-icon in the top-left corner.

Dencrypt Connex launches per default with the Contacts screen. The launch screen can be set from: Settings →Account Settings →Launch screen. See also section 7.



D

David Wilson
Verify A/S | Management

J

James Smith
Verify A/S | Management

K

Karen Miller
Verify A/S | Development

M

Mary Johnson
Verify A/S | Management

P

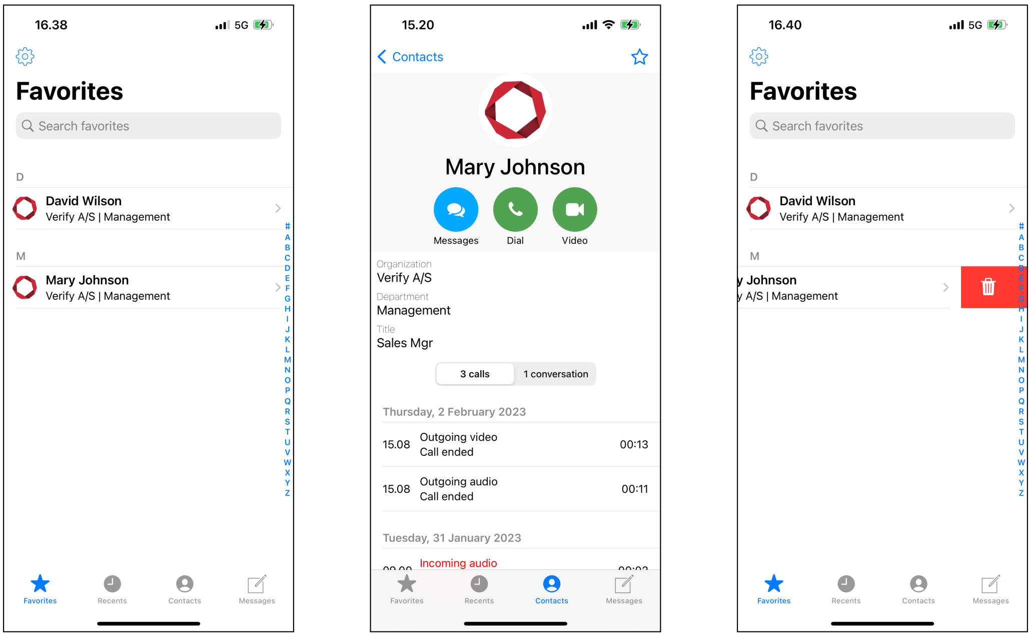
Project X
[2 team members]

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 🗑.



(a) Favourites screen

(b) Add to Favourites

(c) Remove from Favourites.

Figure 6: Favourites.

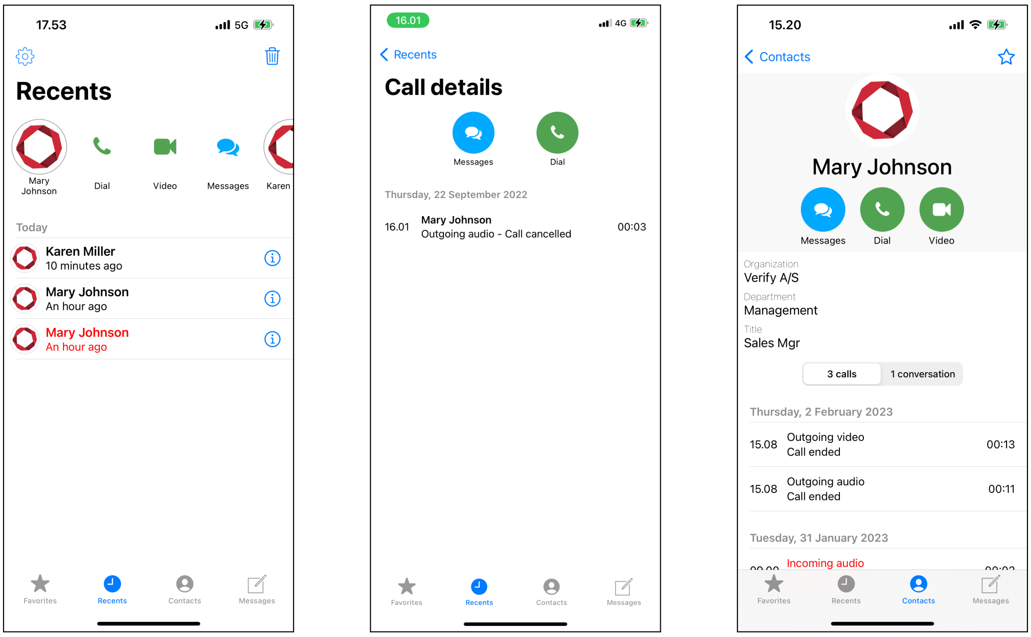
4.2 Recents

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 🗑 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-icon on the right of the screen. This will open the Call Details screen, which contains the call history for the contact.



Today

Karen Miller
10 minutes ago

Mary Johnson
An hour ago

Mary Johnson
An hour ago

Thursday, 22 September 2022

16.01 Mary Johnson
Outgoing audio - Call cancelled 00:03

Organization
Verify A/S

Department
Management

Title
Sales Mgr

Thursday, 2 February 2023

15.08 Outgoing video
Call ended 00:13

15.08 Outgoing audio
Call ended 00:11

Tuesday, 31 January 2023

Incoming audio

(a) Recents screen (b) Recents details screen. (c) Recent call detail from contacts.

Figure 7: Recents.

4.3 Contacts

The Contacts screen shows the entire phone book consisting of individual contacts and team rooms. 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. Change the sorting order from the Settings menu. To locate contacts:

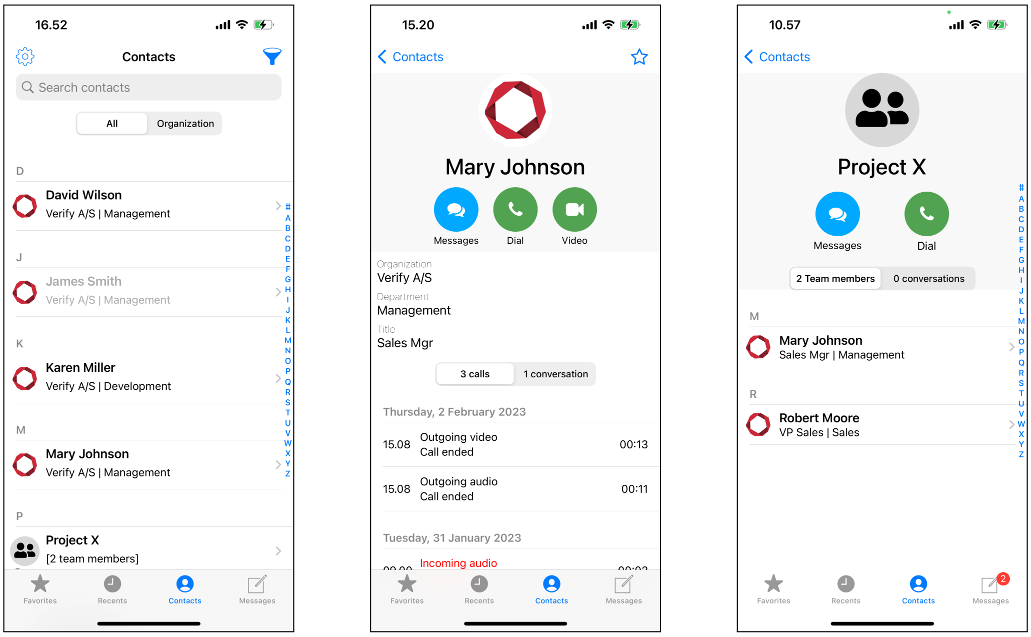
- Skip to a specific letter using the index on the right-hand side of the screen, or
- Search for contacts via the search menu. or
- Use the filter option in the top-right corner [Filtering the phonebook 4.3.2].
- Toggle between an All contact view or Organisation view by tapping the buttons above the 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

Selecting a contact will open the Contact details 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. Tap the buttons above the recent list to toggle between recent calls and recent message conversations.

Selecting a team room will open the Teamroom details to list the members and allow the user to exchange messages with the team or to start a group call with the team.

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



D
David Wilson
Verify A/S | Management

J
James Smith
Verify A/S | Management

K
Karen Miller
Verify A/S | Development

M
Mary Johnson
Verify A/S | Management

P
Project X
[2 team members]

Mary Johnson

Organization
Verify A/S
Department
Management
Title
Sales Mgr

3 calls | 1 conversation

Thursday, 2 February 2023

15.08 Outgoing video
Call ended 00:13

15.08 Outgoing audio
Call ended 00:11

Tuesday, 31 January 2023

Incoming audio

Project X

2 Team members | 0 conversations

M
Mary Johnson
Sales Mgr | Management

R
Robert Moore
VP Sales | Sales

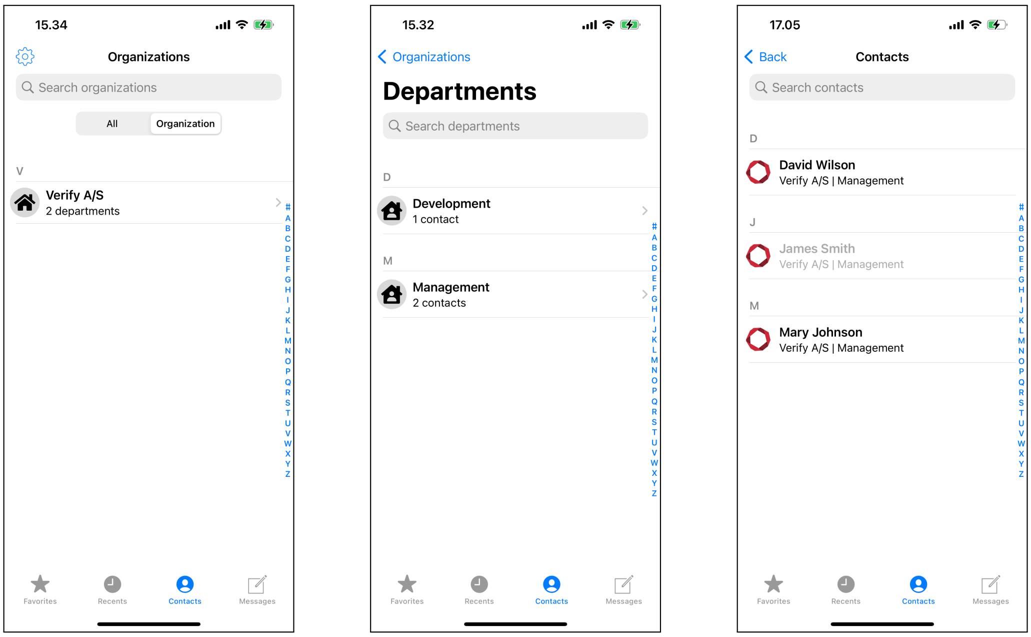
(a) Contacts screen. (b) Contact details. (c) Teamroom details.

Figure 8: Contacts.

4.3.1 Phonebook views

Two phonebook views are available:

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



V
Verify A/S
2 departments

Departments

D
Development
1 contact

M
Management
2 contacts

D
David Wilson
Verify A/S | Management

J
James Smith
Verify A/S | Management

M
Mary Johnson
Verify A/S | Management

(a) First layer: Companies (b) Second layer: Departments (c) Contacts in departments

Figure 9: Contacts in organization view.

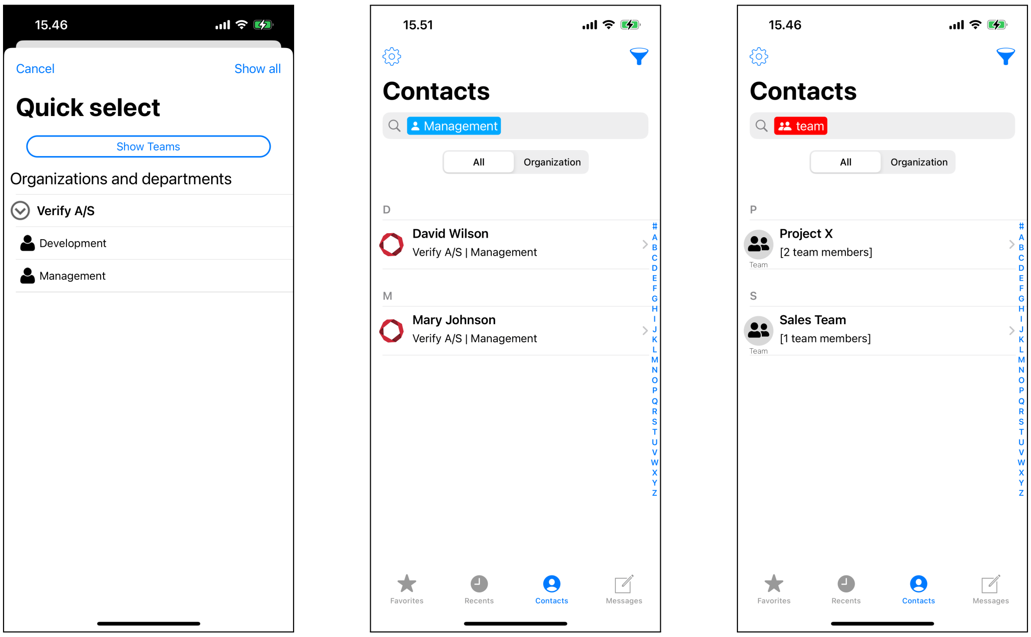
4.3.2 Filtering the phonebook

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 tapping "Show All" or by tapping the search field and deleting the filter.



(a) Quick Select

(b) Filtered contacts

(c) Show Teams

Figure 10: Filtering contacts.

4.4 Messages

The Message screen is used for sending and receiving text messages and attachments, such as photos, video, audio clips, file sharing, 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.

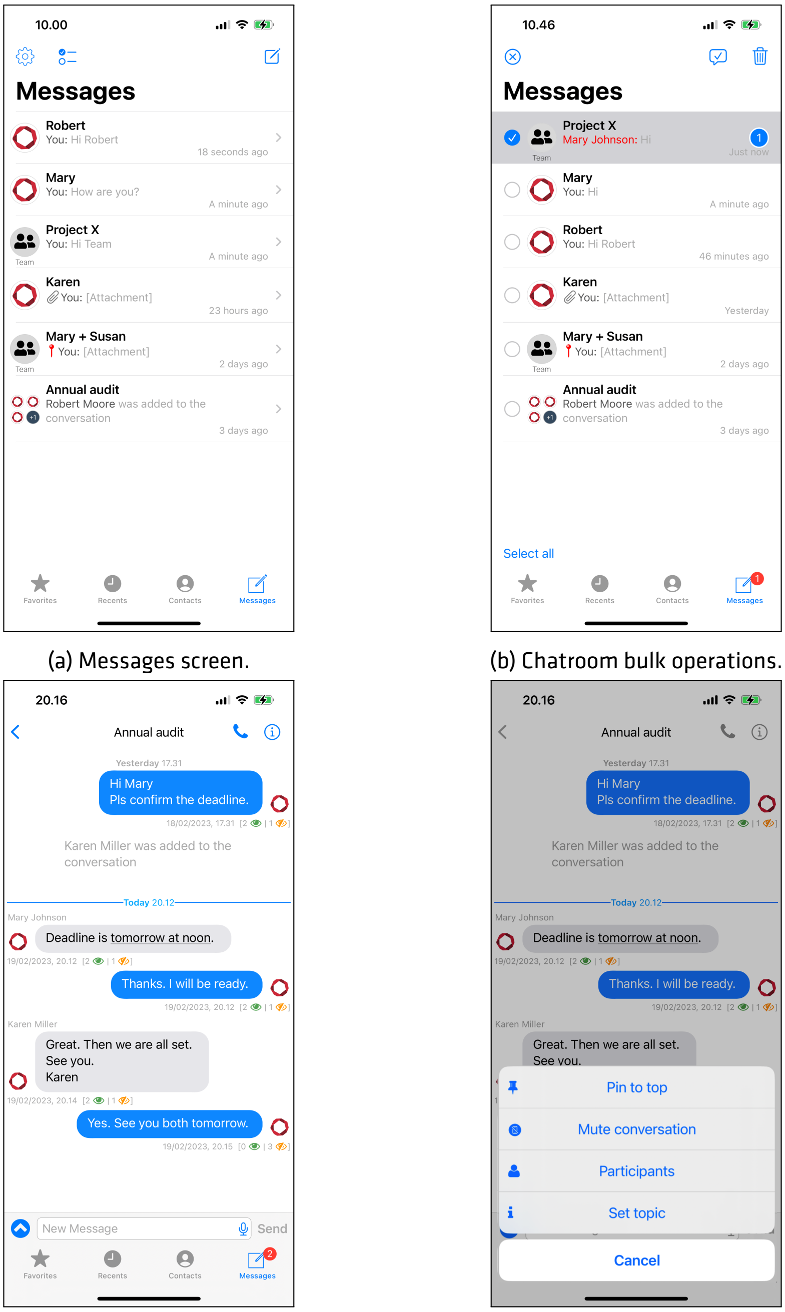
- Teamrooms - persistent chatrooms defined by the system administrator, who also manage the participants. Team rooms are usually created for departments, project teams, o.l. Team rooms are indicated with a TEAM label.

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.

Tap ☰-icon to select bulk delete or mark all messages as read.

Tapping an entry (chatroom) will open up the messages in the conversation. 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.

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



10.00

Messages

Robert
You: Hi Robert
18 seconds ago

Mary
You: How are you?
A minute ago

Project X
You: Hi Team
A minute ago

Karen
You: [Attachment]
23 hours ago

Mary + Susan
You: [Attachment]
2 days ago

Annual audit
Robert Moore was added to the conversation
3 days ago

(a) Messages screen.

10.46

Messages

Project X
Mary Johnson: Hi
Just now

Mary
You: Hi
A minute ago

Robert
You: Hi Robert
46 minutes ago

Karen
You: [Attachment]
Yesterday

Mary + Susan
You: [Attachment]
2 days ago

Annual audit
Robert Moore was added to the conversation
3 days ago

(b) Chatroom bulk operations.

20.16

Annual audit

Yesterday 17.31

Hi Mary
Pls confirm the deadline.
18/02/2023, 17.31

Karen Miller was added to the conversation

Today 20.12

Mary Johnson
Deadline is tomorrow at noon.
19/02/2023, 20.12

Thanks. I will be ready.
19/02/2023, 20.12

Karen Miller
Great. Then we are all set.
See you.
Karen
19/02/2023, 20.14

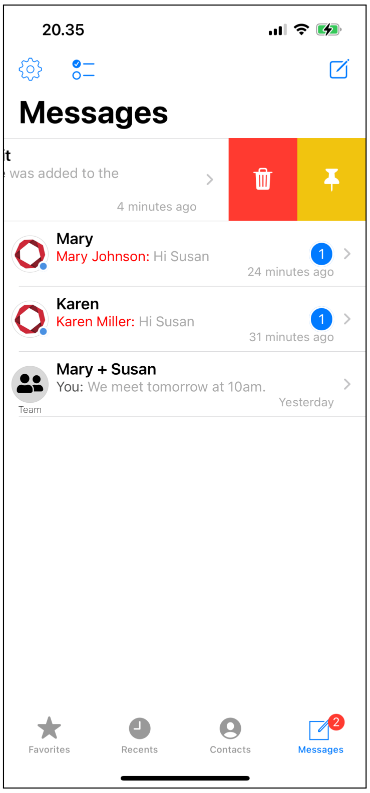
Yes. See you both tomorrow.
19/02/2023, 20.15

(c) Message conversation.

(d) chatroom options.

Figure 11: Messages

Chatrooms can be deleted or marked as favorites (pinned). In the chatroom list: Swipe left 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 conversation will prevent notifications to be displayed for the selected duration. Muted conversations can be identified by a small icon shown in the conversation topic. Conversations can be unmuted from the options menu.



20.35

Messages

t
was added to the
4 minutes ago

Mary
Mary Johnson: Hi Susan
24 minutes ago

Karen
Karen Miller: Hi Susan
31 minutes ago

Mary + Susan
You: We meet tomorrow at 10am.
Team
Yesterday

Figure 12: Deleting or pinning a chatroom.

Participants can be added or removed from a topic chatroom:

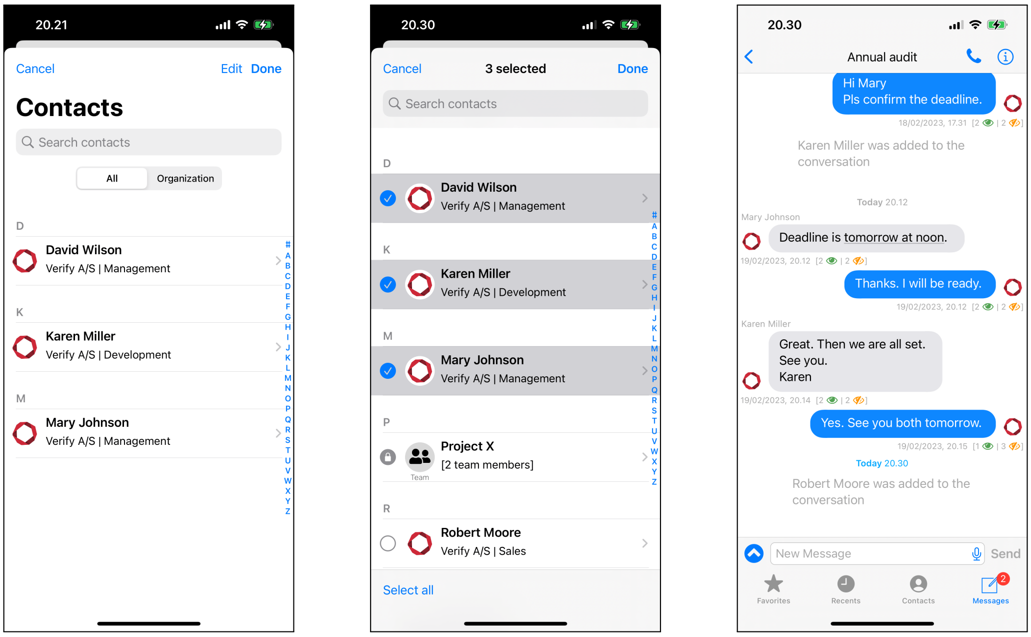
Add/remove participants

Step 1: Open the chatroom and tap ℹ-icon.

Step 2: Tap Participants to diplay a list of chatroom members.

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

Step 4: Tap Done. The participants of the chatroom will be notified about the change.



Contacts

D

David Wilson
Verify A/S | Management

K

Karen Miller
Verify A/S | Development

M

Mary Johnson
Verify A/S | Management

(a) Chatroom members.

3 selected

D

David Wilson
Verify A/S | Management

K

Karen Miller
Verify A/S | Development

M

Mary Johnson
Verify A/S | Management

P

Project X
[2 team members]
Team

R

Robert Moore
Verify A/S | Sales

(b) Select members.

Annual audit

Hi Mary
Pls confirm the deadline.
18/02/2023, 17.31 [2 | 2]

Karen Miller was added to the conversation

Today 20.12

Mary Johnson
Deadline is tomorrow at noon.
19/02/2023, 20.12 [2 | 2]

Thanks. I will be ready.
19/02/2023, 20.12 [2 | 2]

Karen Miller
Great. Then we are all set.
See you.
Karen
19/02/2023, 20.14 [2 | 2]

Yes. See you both tomorrow.
19/02/2023, 20.15 [1 | 3]

Today 20.30

Robert Moore was added to the conversation

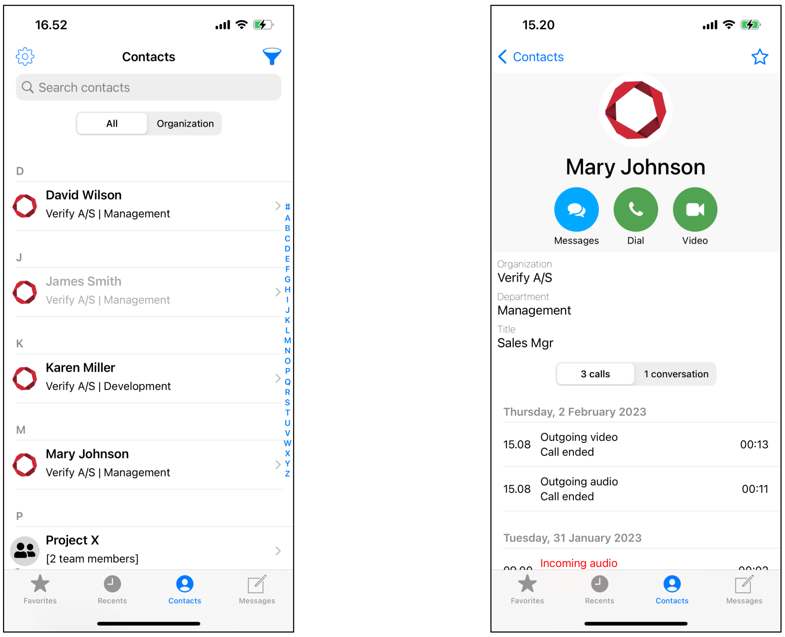
(c) Member added.

Figure 13: 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] 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.



D
David Wilson
Verify A/S | Management

J
James Smith
Verify A/S | Management

K
Karen Miller
Verify A/S | Development

M
Mary Johnson
Verify A/S | Management

P
Project X
[2 team members]

(a) Contacts screen.

Mary Johnson

Organization
Verify A/S

Department
Management

Title
Sales Mgr

Thursday, 2 February 2023

15.08 Outgoing video
Call ended 00:13

15.08 Outgoing audio
Call ended 00:11

Tuesday, 31 January 2023

Incoming audio

(b) Contact details.

Figure 14: Making calls from Contacts

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.

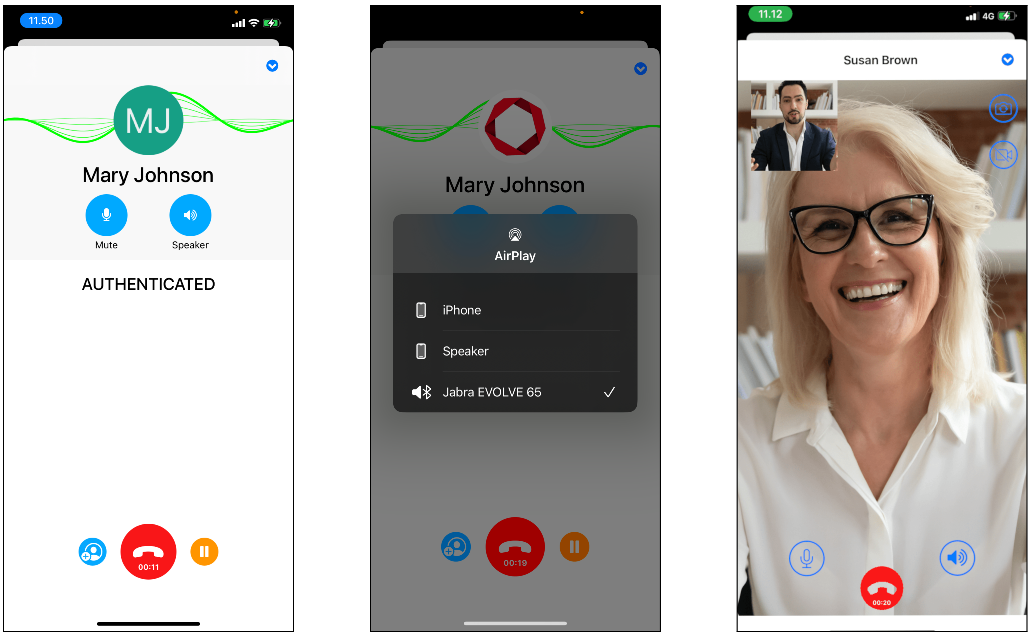
A secure audio call is initiated by tapping the Dial button, which opens the Call screen. A secure video call is started by tapping the Video button.

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 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 the call. During a secure video call, also switching between the front- and the backside camera and disabling the camera is possible. Video autostart can be selected in the Settings menu (figire 37d).

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].



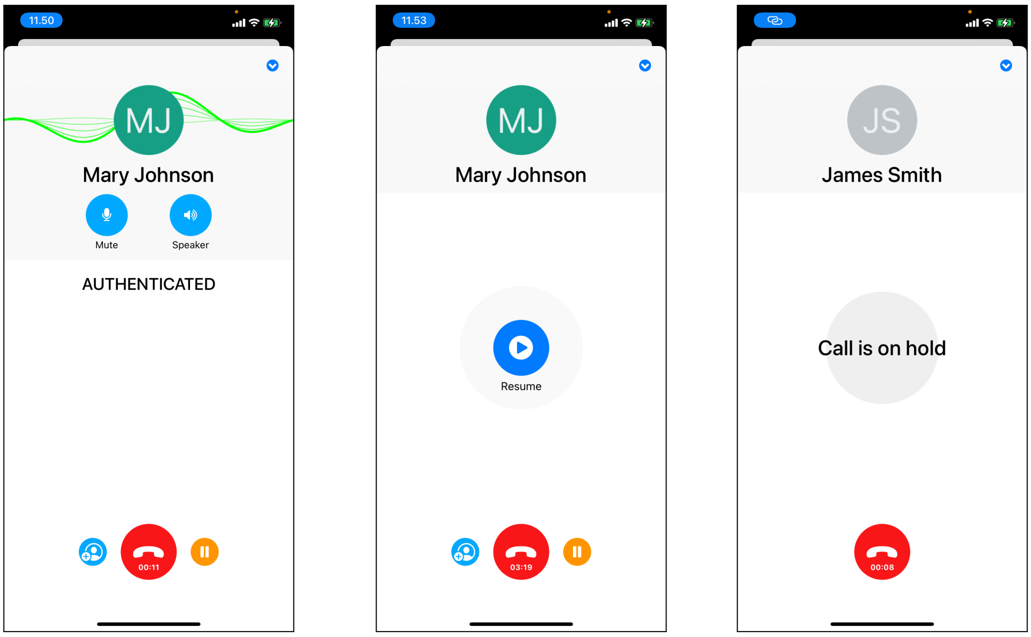
(a) Secured voice call.

(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

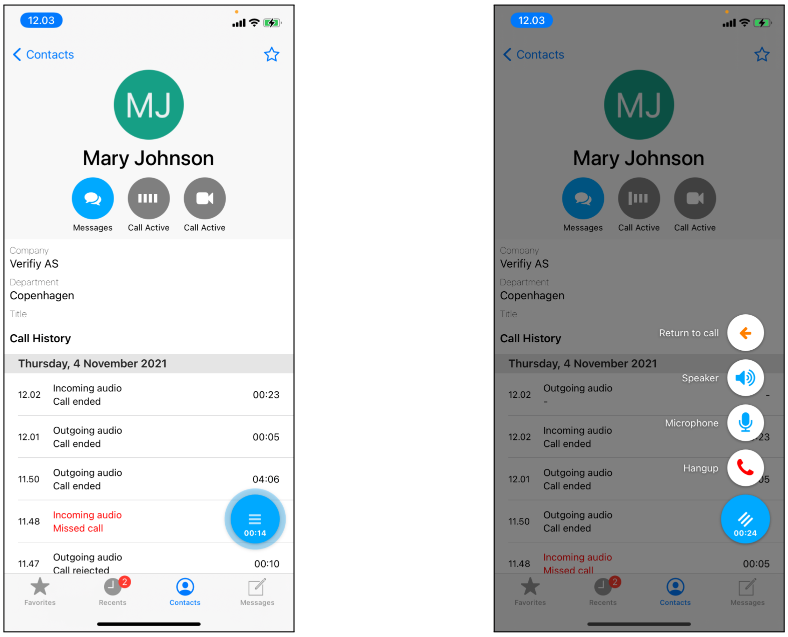
An In-call action menu is displayed when a user navigates away from the Call screen during a call.

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 the call	Opens the in-call screen.
Speaker	Toggles the speaker on/off
Microphone	Toggle the microphone on/off.
Hang up	Terminate the call.

Table 4: in-call actions

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



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

(a) Floating menu.

Company
Verifiy AS
Department
Copenhagen
Title

Call History

Thursday, 4 November 2021

12.02 Outgoing audio -
12.02 Incoming audio Call ended
12.01 Outgoing audio Call ended
11.50 Outgoing audio Call ended
11.48 Incoming audio Missed call 00:05

(b) Actions from the floating menu.

Figure 17: In-call action menu screen

5.3 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 [Making a secure call 5].

Step 2: Tap the blue "+ contact" icon to open the phonebook.

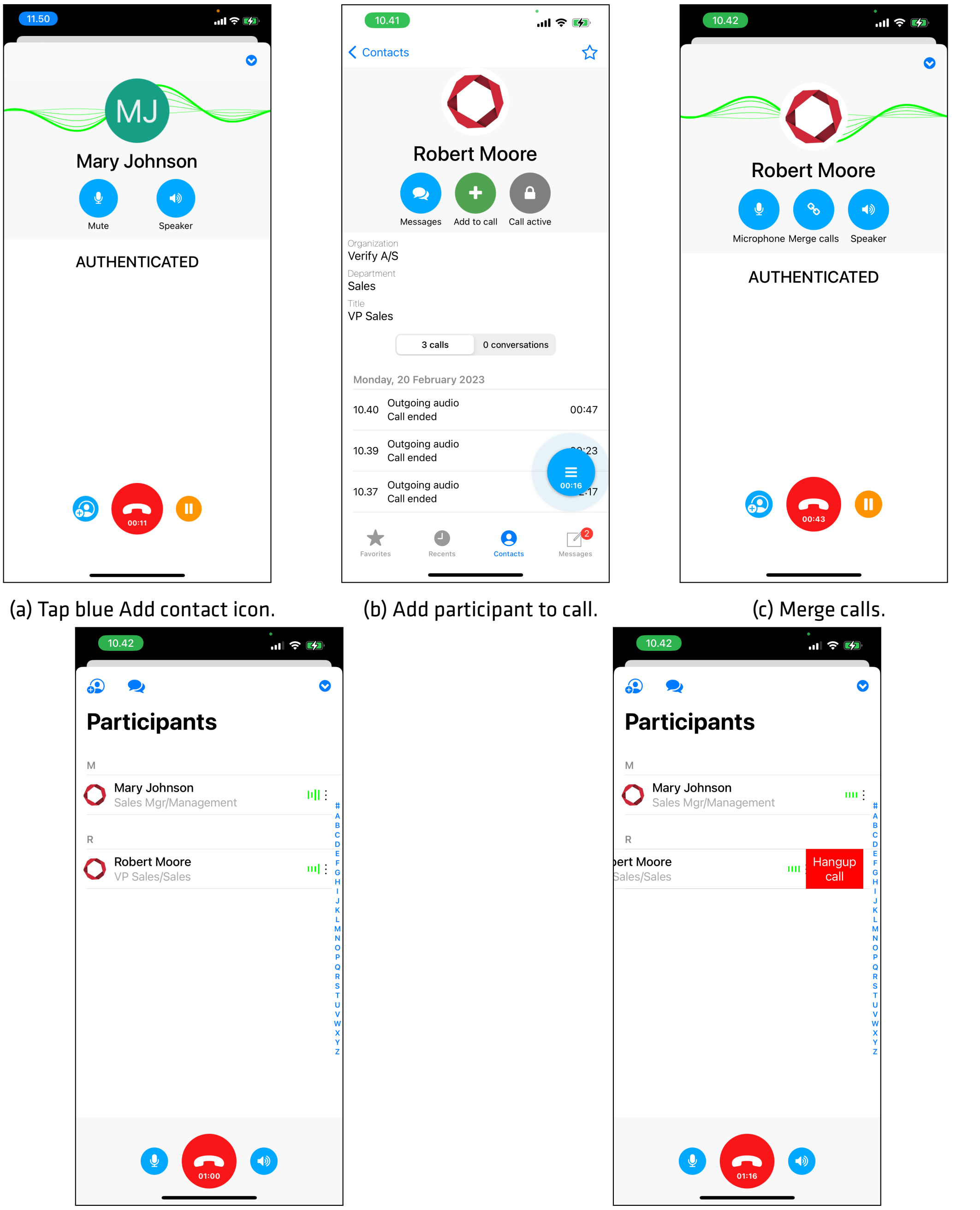
Step 3: Locate a contact in the phonebook and tap Add to call. This will pause the ongoing call and establish a new secure call.

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

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 the participant on hold or hang -up.



Organization
Verify A/S
Department
Sales
Title
VP Sales

Monday, 20 February 2023

10.40	Outgoing audio Call ended	00:47
10.39	Outgoing audio Call ended	00:23
10.37	Outgoing audio Call ended	00:17

(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.

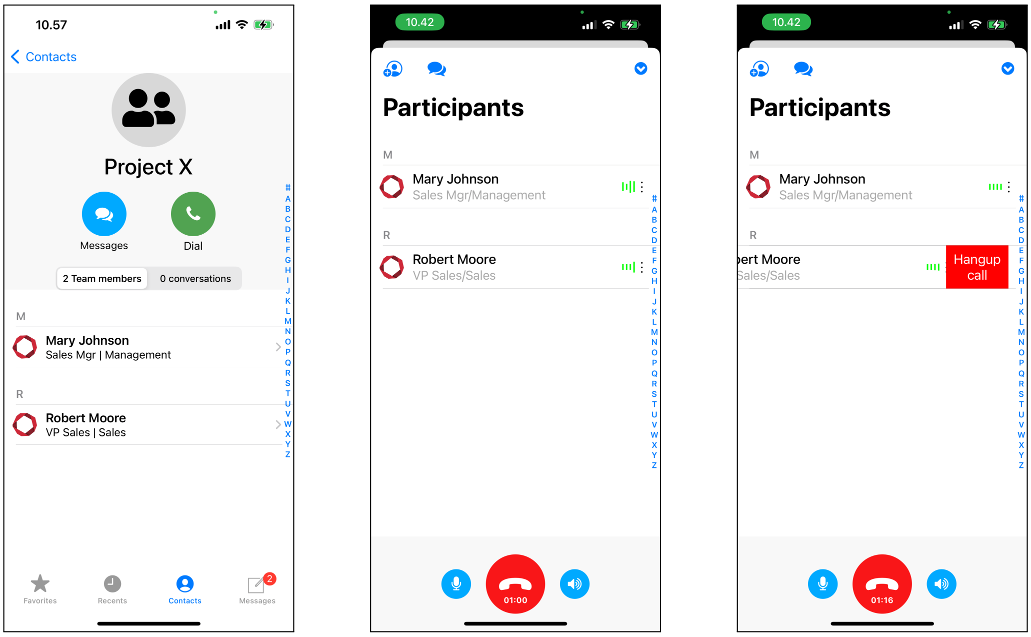
Figure 18: Group calls

Call all participants in a message room

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

Step 2: Tap Call to dial the participants.

Step 3: Swipe left to put the participant on hold or hang up.



(a) Open team-/chatroom. Tap Call. (b) Group call (c) Swipe left to hang up participant.

Figure 19: 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.

5.4 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:

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.

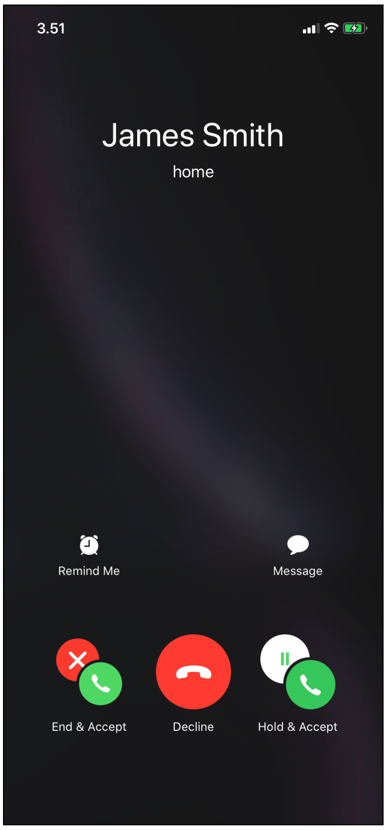


Figure 20: Incoming call during a secure call

5.5 Incoming secure calls

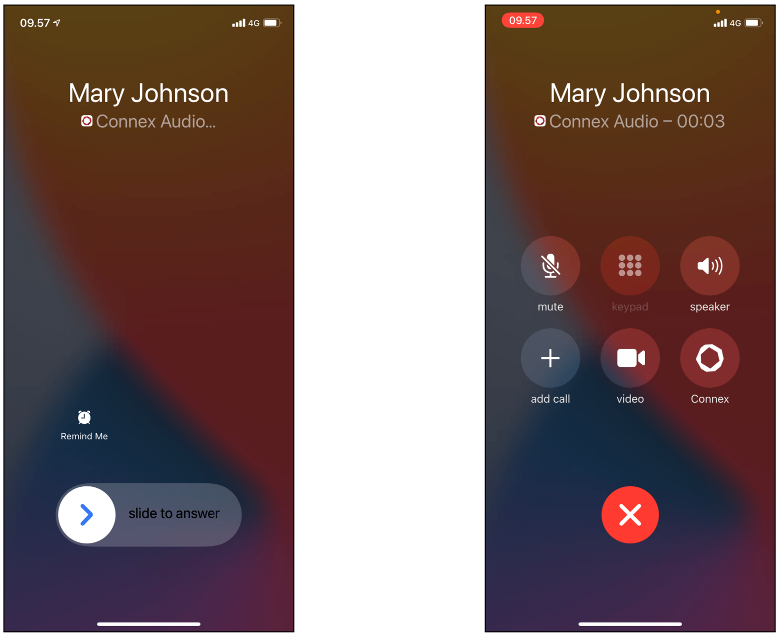
Incoming secure voice calls are alerted using VoIP push notifications, which launch the native iOS call screen. When receiving a secure call, the incoming call screen is displayed, where the caller's name is shown in large letters followed by Connex Audio indicating a secure voice call or by Connex Video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

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.

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

Menu	**Action**
Mute	microphone on/off.
Speaker	Toggles the speaker on/off.
Dencrypt Connex	Opens Dencrypt Connex 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 21: 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.

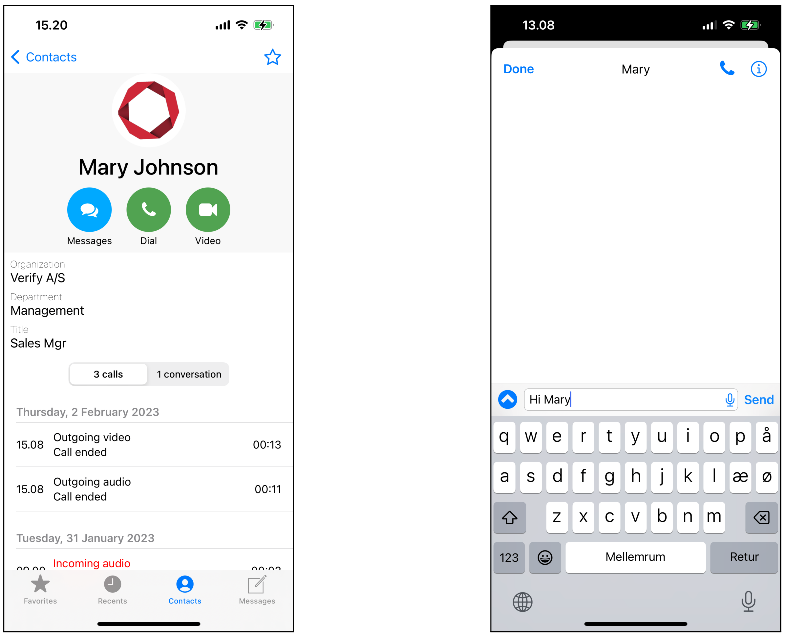
6.1 Create a *direct chat room*

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.

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



Mary Johnson

Organization
Verify A/S

Department
Management

Title
Sales Mgr

Thursday, 2 February 2023

15.08 Outgoing video Call ended 00:13

15.08 Outgoing audio Call ended 00:11

Tuesday, 31 January 2023

Incoming audio

Hi Mary

(a) Select Message.

(b) Start typing the first message.

Figure 22: 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 new *topic conversation* or group conversation

Step 1: Goto the the Message tap.

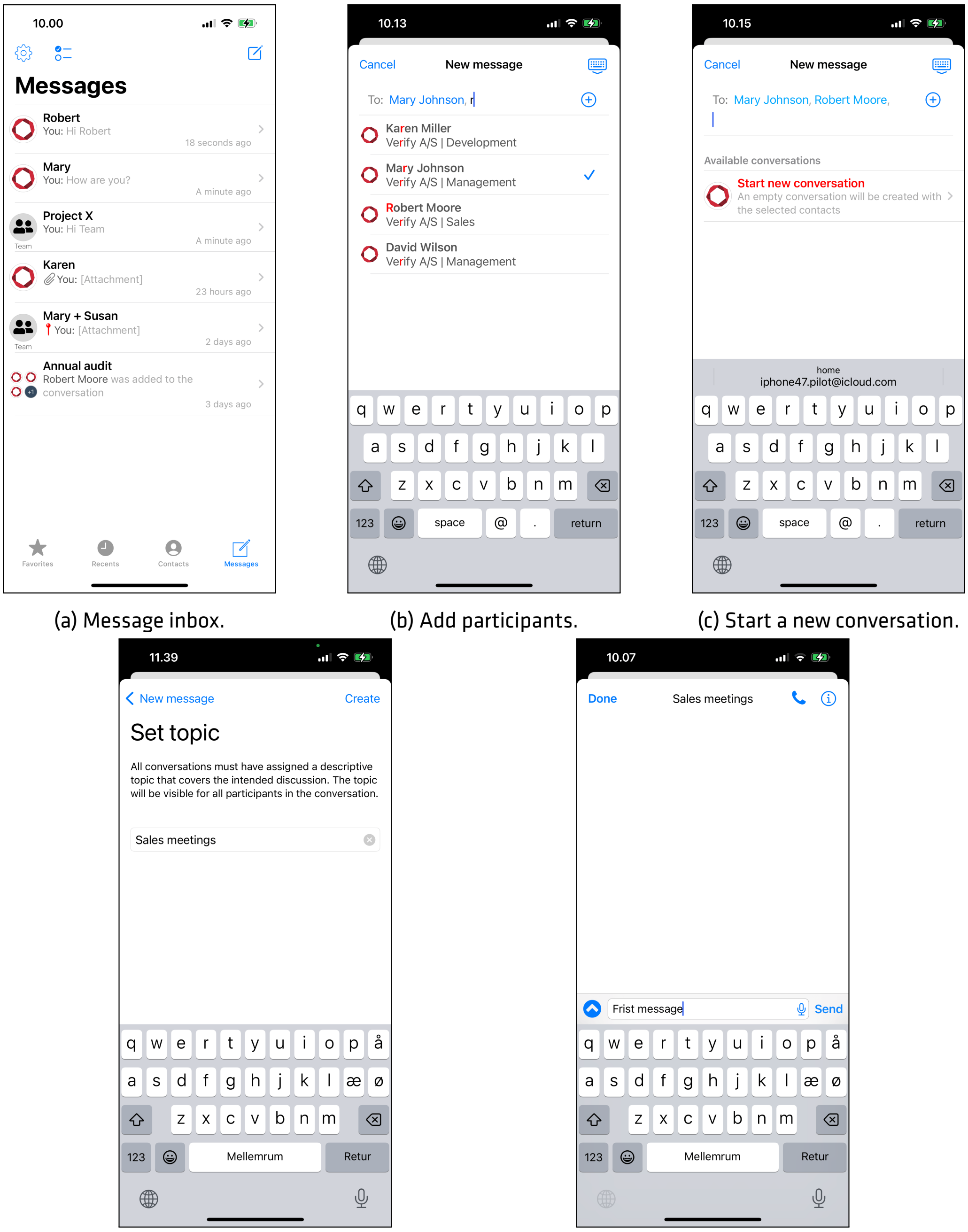
Step 2: Tap the ✎-icon in the top-right corner, which opens the New Message screen.

Step 3: Add recipients by typing their names (matches are shown while typing) or select + to select from the phonebook.

Step 4: Select an existing chatroom or select Start new conversation.

Step 5: If a new conversation is started: Set a title for the chat room and tap Create.

Step 6: Start writing the first message.



Robert
You: Hi Robert
18 seconds ago

Mary
You: How are you?
A minute ago

Project X
You: Hi Team
A minute ago

Karen
You: [Attachment]
23 hours ago

Mary + Susan
You: [Attachment]
2 days ago

Annual audit
Robert Moore was added to the conversation
3 days ago

(a) Message inbox.

To: Mary Johnson, r

Karen Miller
Verify A/S | Development

Mary Johnson ✓
Verify A/S | Management

Robert Moore
Verify A/S | Sales

David Wilson
Verify A/S | Management

(b) Add participants.

To: Mary Johnson, Robert Moore,

Available conversations

Start new conversation
An empty conversation will be created with the selected contacts

(c) Start a new conversation.

Set topic

All conversations must have assigned a descriptive topic that covers the intended discussion. The topic will be visible for all participants in the conversation.

Sales meetings

(d) Set title.

Frist message

(e) Write the first message.

Figure 23: 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.

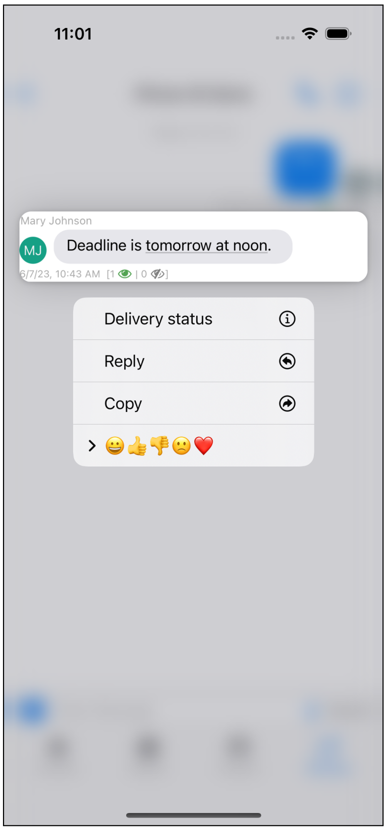
The message is encrypted and transmitted immediately when an active data connection exists. A successful transmission is indicated by a ✓-icon.

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.

6.4 Message context menu

Long pressing on any message will bring up a context menu which will present the following options.



Mary Johnson

MJ Deadline is tomorrow at noon.

6/7/23, 10:43 AM [1 👁 | 0 ⊘]

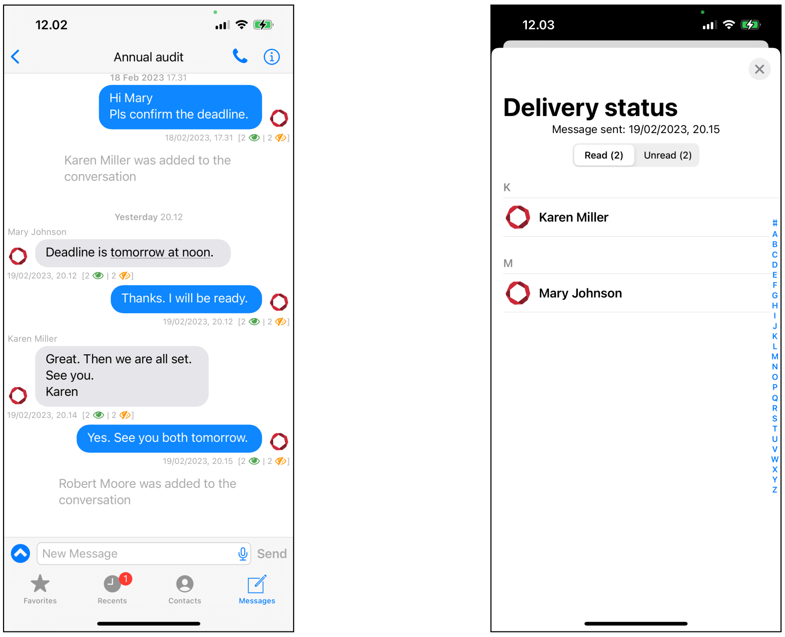
Figure 24: Long pressing on a message

6.4.1 Message delivery status

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

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

Figure 25 gives a conversation example with all color codes. Detailed delivery status is available when long pressing on a message.



12.02

Annual audit

18 Feb 2023 17.31

Hi Mary
Pls confirm the deadline.

18/02/2023, 17.31

Karen Miller was added to the conversation

Yesterday 20.12

Mary Johnson

Deadline is tomorrow at noon.

19/02/2023, 20.12

Thanks. I will be ready.

19/02/2023, 20.12

Karen Miller

Great. Then we are all set.
See you.
Karen

19/02/2023, 20.14

Yes. See you both tomorrow.

19/02/2023, 20.15

Robert Moore was added to the conversation

(a) Conversation screen.

12.03

Delivery status

Message sent: 19/02/2023, 20.15

Read (2) Unread (2)

K

Karen Miller

M

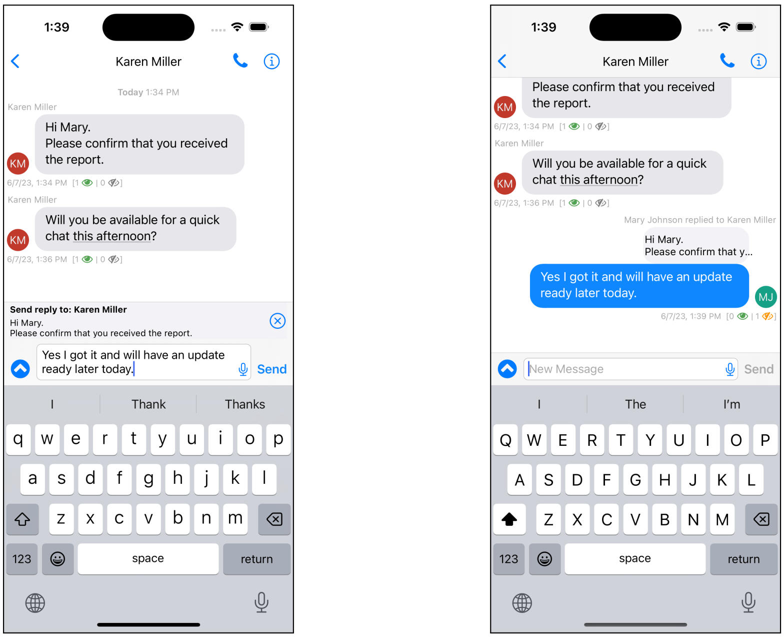
Mary Johnson

(b) Delivery status details.

Figure 25: 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 Close button will cancel the reply feature, tapping Send will send the reply. Both the sender and receiver will show the original message and the reply message. Tapping the original message will scroll the conversation so the original message is shown.



1:39

Karen Miller

Today 1:34 PM

Karen Miller

Hi Mary.
Please confirm that you received the report.

6/7/23, 1:34 PM

Karen Miller

Will you be available for a quick chat this afternoon?

6/7/23, 1:36 PM

Send reply to: Karen Miller
Hi Mary.
Please confirm that you received the report.

Yes I got it and will have an update ready later today.

(a) Writing a reply.

1:39

Karen Miller

Please confirm that you received the report.

6/7/23, 1:34 PM

Karen Miller

Will you be available for a quick chat this afternoon?

6/7/23, 1:36 PM

Mary Johnson replied to Karen Miller

Hi Mary.
Please confirm that y...

Yes I got it and will have an update ready later today.

6/7/23, 1:39 PM

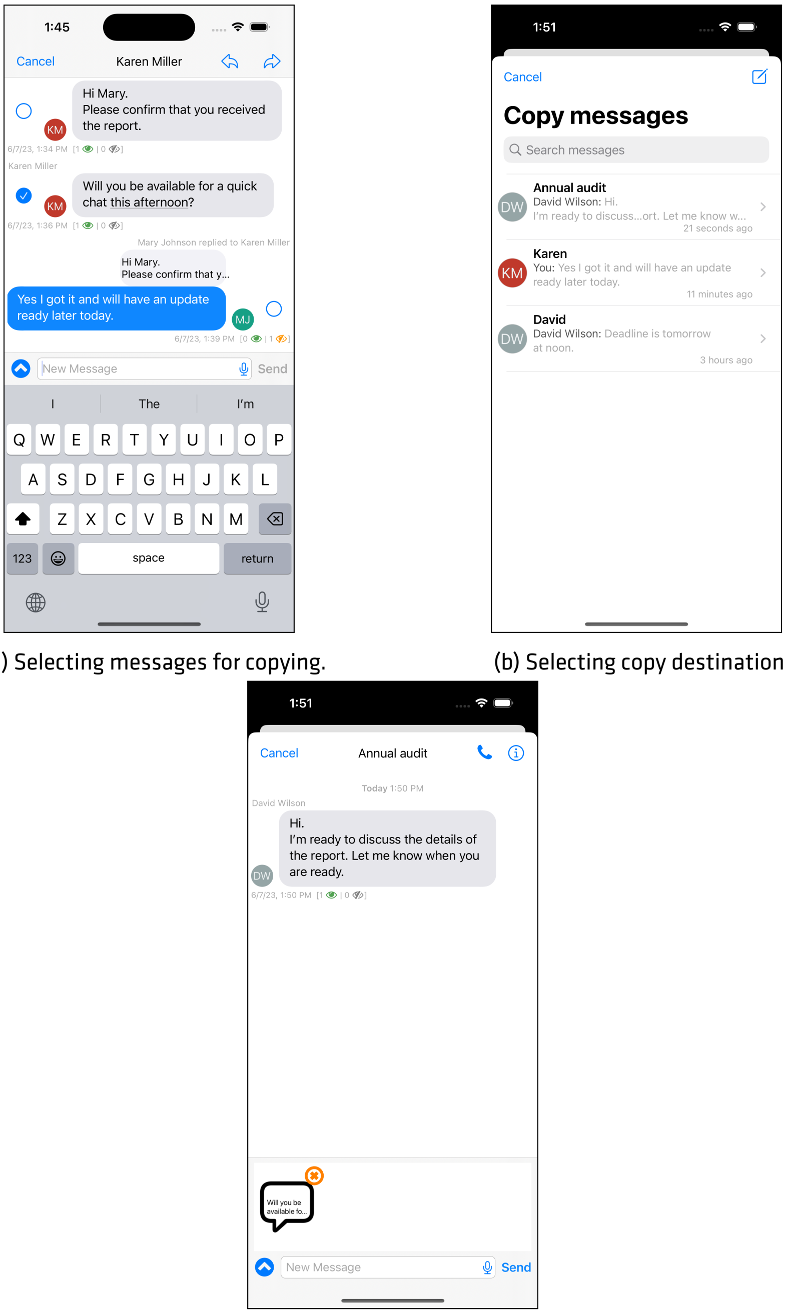
(b) Reply sent.

Figure 26: Message with a reply.

6.4.3 Copy messages

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

Selecting Copy from the context menu will allow the user to select one or more elements to be selected. Selected elements are shown with a tickmark. From the top menu two icons will appear, one for Reply and one for Copy. Please note that Reply will only be available if a single element is selected. Tap the Copy icon to initiate the Copy. Finish the Coping by selecting a destination conversation and send the message.



1:45
Cancel Karen Miller

Hi Mary.
Please confirm that you received the report.
6/7/23, 1:34 PM

Karen Miller
Will you be available for a quick chat this afternoon?
6/7/23, 1:36 PM

Mary Johnson replied to Karen Miller
Hi Mary.
Please confirm that y...
Yes I got it and will have an update ready later today.
6/7/23, 1:39 PM

New Message Send

1:51
Cancel

Copy messages

Search messages

Annual audit
David Wilson: Hi.
I'm ready to discuss...ort. Let me know w...
21 seconds ago

Karen
You: Yes I got it and will have an update ready later today.
11 minutes ago

David
David Wilson: Deadline is tomorrow at noon.
3 hours ago

1:51
Cancel Annual audit

Today 1:50 PM
David Wilson
Hi.
I'm ready to discuss the details of the report. Let me know when you are ready.
6/7/23, 1:50 PM

Will you be available fo...

New Message Send

(a) Selecting messages for copying.

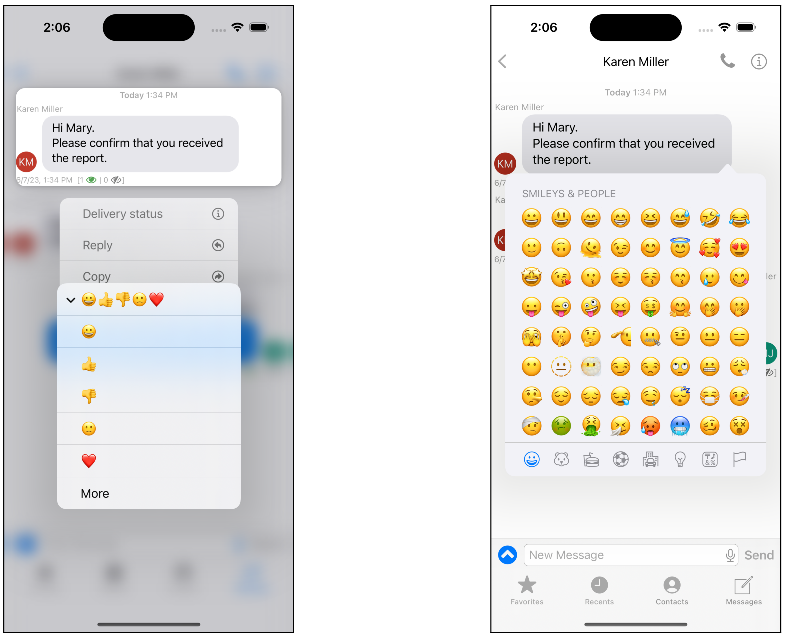
(b) Selecting copy destination.

(c) Copied messages ready to sent.

Figure 27: Copying messages.

6.4.4 Emoji reaction

Emojis can assigned to messages from the context menu.



Karen Miller

Today 1:34 PM

Hi Mary.
Please confirm that you received the report.

(a) Recent emojis

(b) More emojis

Figure 28: Emojis

6.5 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.

Options are:

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 attachment.

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 Connex will not be stored outside the app and will not appear in photo libraries.

iCloud files Opens the iOS file browser to select any file stored locally on the device or from iCloud if the user is signed in.

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

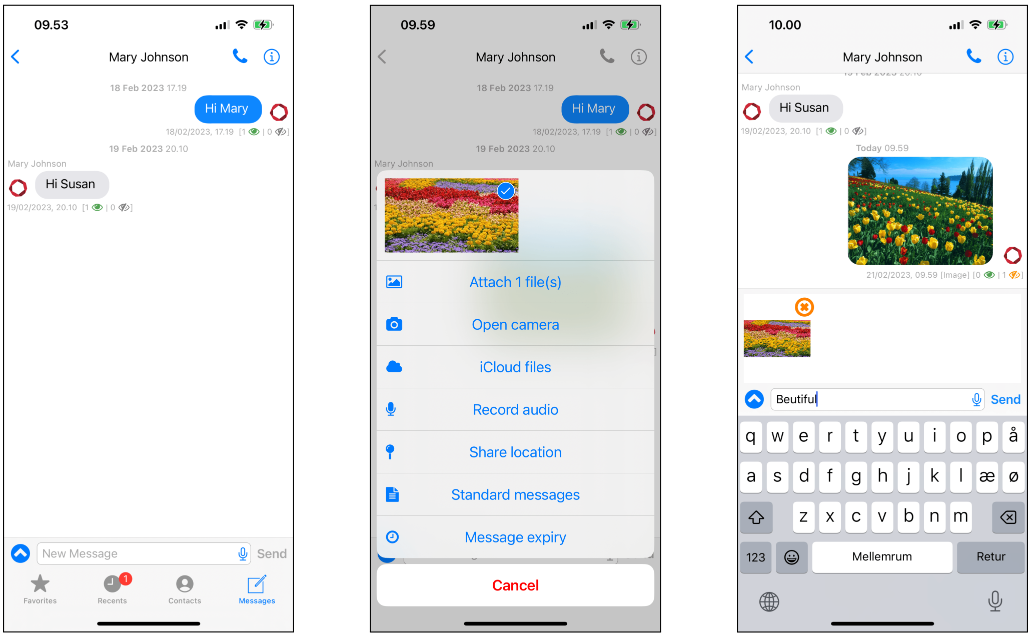
Share Location Opens a map showing the current location. The initial pin location is the current position. The pin can be placed at a new location by dragging it or by a "long-press" anywhere on the map.

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

Message Expiry Use Message expiry to 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. Photos, videos, audio clips, and shared locations generated from within Dencrypt Connex will permanently disappear and cannot be recovered once removed.



(a) Open attachment menu (⌃). (b) Select attachment type. (c) Attachment selected.

Figure 29: Sending attachments.

6.6 Push-to-Talk

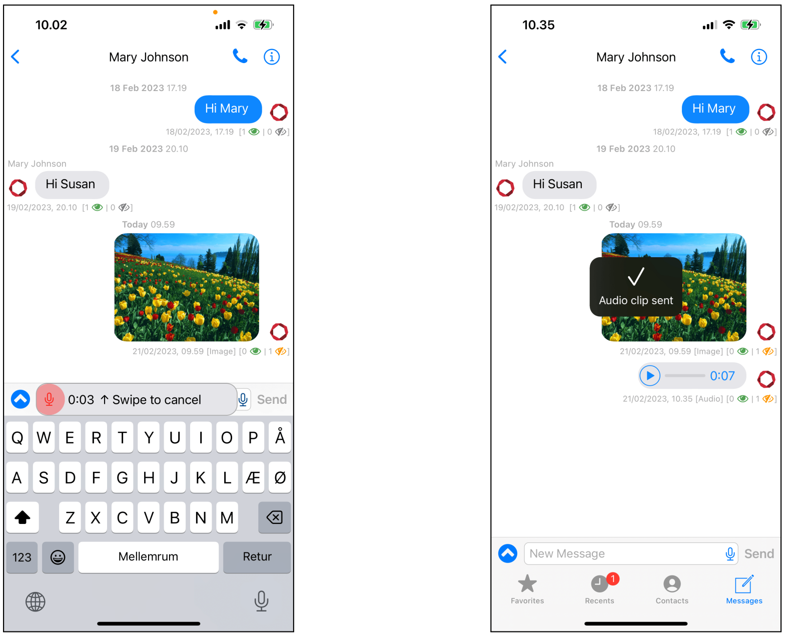
Push-to-Talk functionality is available through the 🎤-icon in the compose field.

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.



10.02

Mary Johnson

18 Feb 2023 17.19

Hi Mary

18/02/2023, 17.19 [1 | 0]

19 Feb 2023 20.10

Mary Johnson

Hi Susan

19/02/2023, 20.10 [1 | 0]

Today 09.59

21/02/2023, 09.59 [Image] [0 | 1]

0:03 ↑ Swipe to cancel

10.35

Mary Johnson

18 Feb 2023 17.19

Hi Mary

18/02/2023, 17.19 [1 | 0]

19 Feb 2023 20.10

Mary Johnson

Hi Susan

19/02/2023, 20.10 [1 | 0]

Today 09.59

Audio clip sent

21/02/2023, 09.59 [Image] [0 | 1]

0:07

21/02/2023, 10.35 [Audio] [0 | 1]

(a) Record audio message.

(b) Send audio clip.

Figure 30: Push-to-Talk messaging

6.7 Location sharing

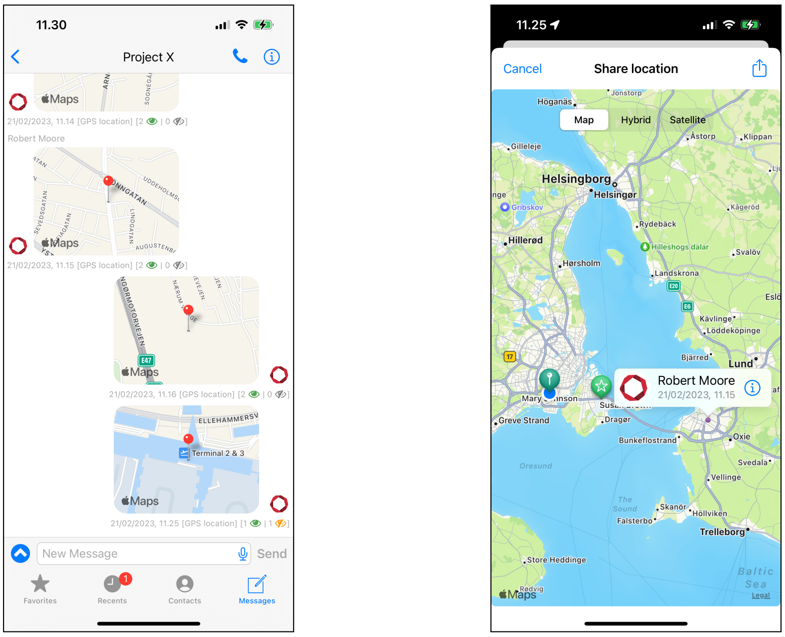
Participants in a chat room can share their location as an attachment. The last known location of the participants, who have shared a location, is displayed on a single map.

View last known locations

Step 1: Open the chatroom and tap any of the shared locations.

Step 2: The map opens with a pin and name for each of the participants.

Step 3: Tap a pin to see a timestamp for the location sharing.



(a) Shared locations.

(b) Map view.

Figure 31: Location sharing

6.8 Standard messages

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

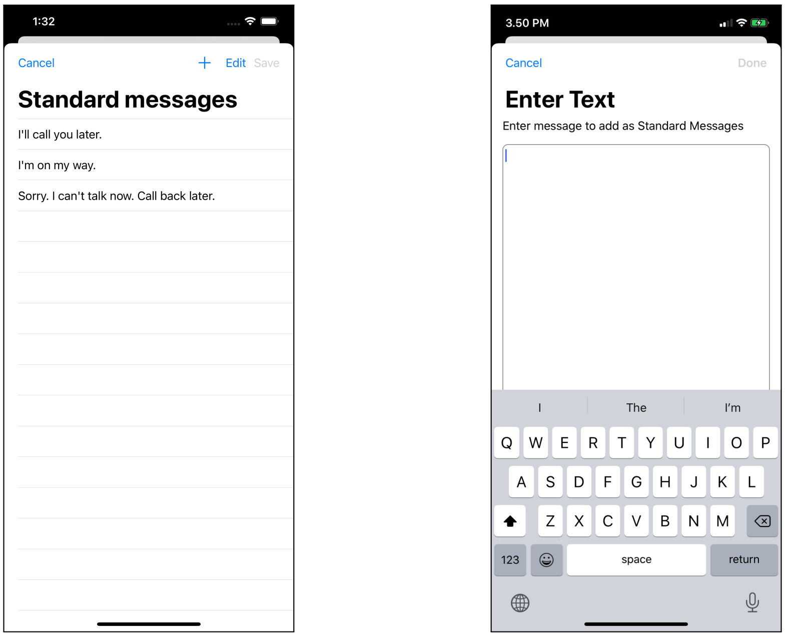
Insert a standard message

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 32: Standard messages

6.9 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.

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 three separate lines:

(a) Not Before date.

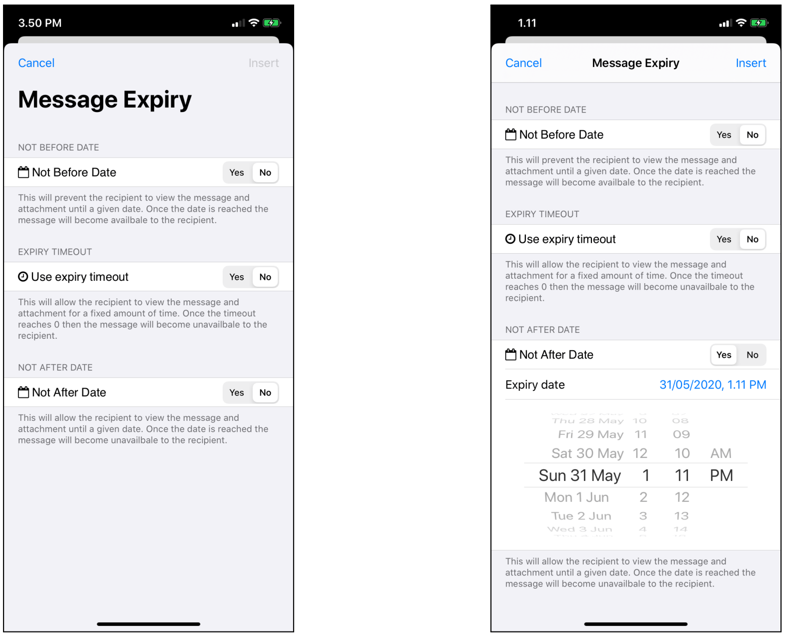
(b) Expiry time.

(c) Not After date.

Not before date The message will not be available for the recipients before this date/time. The receiver will get a notification when the message becomes available.

Expiry timeout The message will only be available for the receivers for a limited duration. A timer will start a 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/time.



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 availbale 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

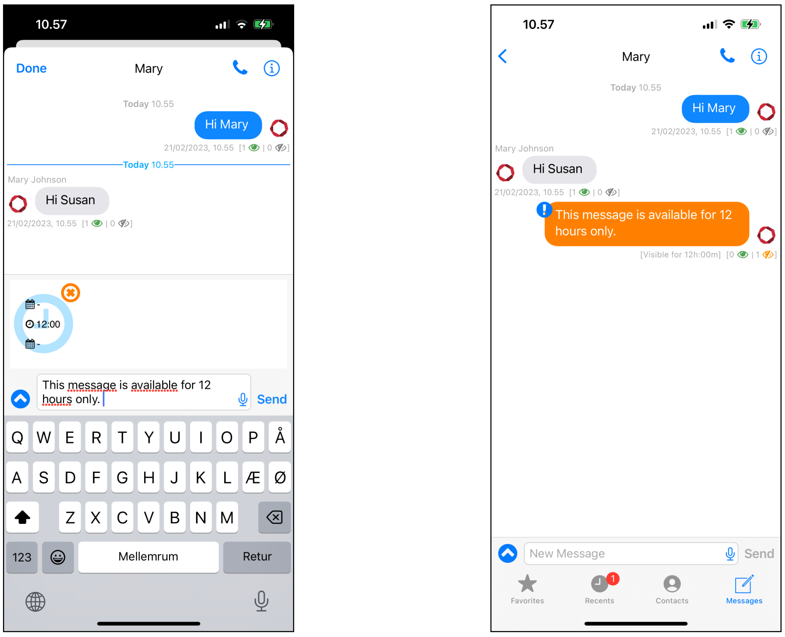
Not After Date Yes No

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 availbale to the recipient.

(b) Message with time constraints.

Figure 33: Set message expiry.



10.57

Done Mary

Today 10.55

Hi Mary

21/02/2023, 10.55 [1 | 0]

Today 10.55

Mary Johnson

Hi Susan

21/02/2023, 10.55 [1 | 0]

12:00

This message is available for 12 hours only.

Send

(a) Typing message.

10.57

Mary

Today 10.55

Hi Mary

21/02/2023, 10.55 [1 | 0]

Mary Johnson

Hi Susan

21/02/2023, 10.55 [1 | 0]

This message is available for 12 hours only.

[Visible for 12h:00m] [0 | 1]

New Message Send

(b) Time limited message.

Figure 34: Message expiry

6.10 Emergency message

An Emergency message is a fast way to share the current location with another device. The system administrator must configure an emergency contact for the feature to be available.

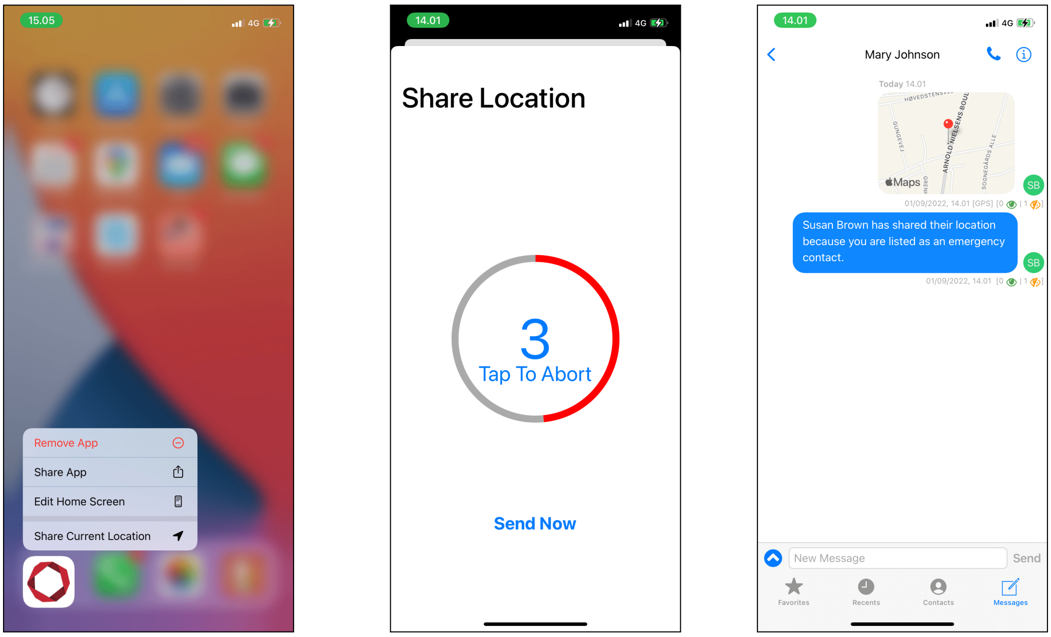
Send an emergency message

Step 1: Long press Dencrypt Connex -icon to open the app menu.

Step 2: Select Share current location

Step 3: Location is sent after 5 seconds or when tapping Share Now.

Step 4: The message can be seen in the Message-tab.



01/09/2022, 14.01 [GPS] [0 | 1]

Susan Brown has shared their location because you are listed as an emergency contact.

01/09/2022, 14.01 [0 | 1]

(a) Long press the app icon. (b) Select Share current location (c) Location message

Figure 35: Sending an emergency message.

7 Settings

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

The settings menu is opened by tapping the "cogwheel"-icon in the top left corner of the screen. The Settings menu gives access to the following options and information:

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 Connex .

Status Server connection status.

App version Dencrypt Connex version number.

Phonebook Settings From the phonebook settings, the user can change the default settings for:

- Default phonebook view [All/Organisation/Last used].
- Phonebook sorting [Firstname/Lastname].
- Phonebook display [Firstname Lastname/Lastname, Firstname].
- Contact logo [Organisation logo/Initials/Do not show].
- Show unregistered users [Default/Show/Hide].
- Organisation details in organization view [Show/Hide].
- Color messages. Display incoming messages with the same color or use a new color per contact [Default/Individual].

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

- Ringing tone [iOS default/office phone/Mystic call].
- Screen off - toggle if screen shall be off during calls or controlled by proximity sensor.
- Video autostart: Select if video shall automatically be enabled when receiving a video call [Default-/On/Off].
- Toggle Tunnel mode. Used in VoIP blocking regions (Default: Off) [Default/Auto/Enable/Disable].

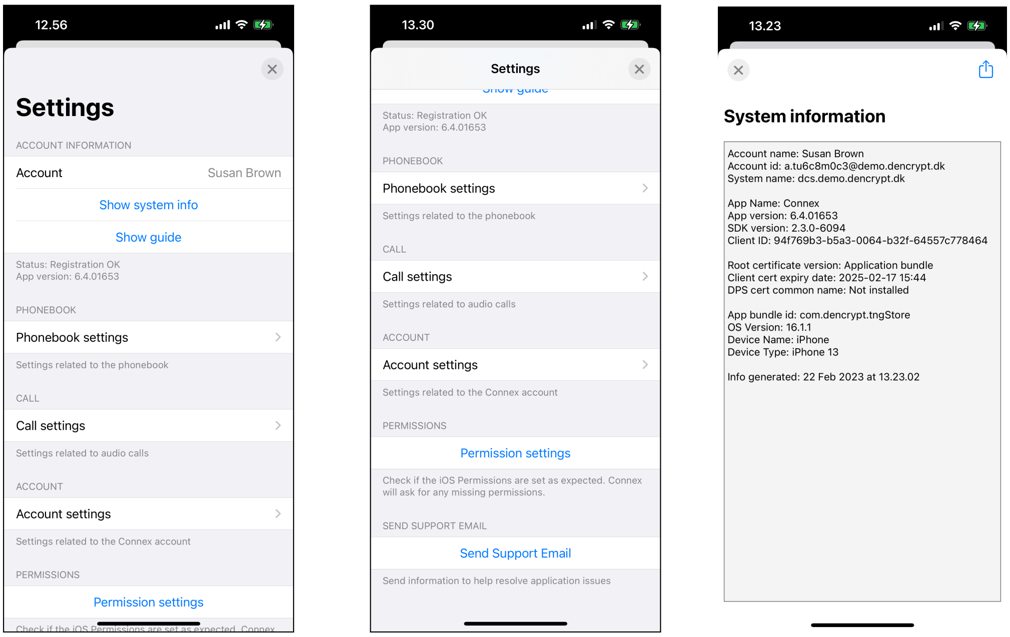
Account Settings From the account settings menu, the user can change default settings for:

- Badge icon: Set what the badge icon shall show [Missed calls/Unread messages/Missed calls and unread messages].
- Launch screen [Favorites/Contacts/Recents/Messages/Last used].
- Block rotation: Toggle to lock screen in portrait mode during calls.
- Show pending messages: Toggle to receive notification for messages not sent.
- Reset info messages. Reset display of info messages.

- Delete account. Warning: Permanently delete all messages and data.

Permission Settings Checks app permissions.

Send Support Mail Toshare logs with Dencrypt Developers. Used for troubleshooting.



12.56

Settings

ACCOUNT INFORMATION

Account Susan Brown

Show system info

Show guide

Status: Registration OK
App version: 6.4.01653

PHONEBOOK

Phonebook settings

Settings related to the phonebook

CALL

Call settings

Settings related to audio calls

ACCOUNT

Account settings

Settings related to the Connex account

PERMISSIONS

Permission settings

Check if the iOS Permissions are set as expected. Connex

(a) Settings menu - Part 1.

13.30

Settings

Show guide

Status: Registration OK
App version: 6.4.01653

PHONEBOOK

Phonebook settings

Settings related to the phonebook

CALL

Call settings

Settings related to audio calls

ACCOUNT

Account settings

Settings related to the Connex account

PERMISSIONS

Permission settings

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

SEND SUPPORT EMAIL

Send Support Email

Send information to help resolve application issues

(b) Settings menu - Part 2.

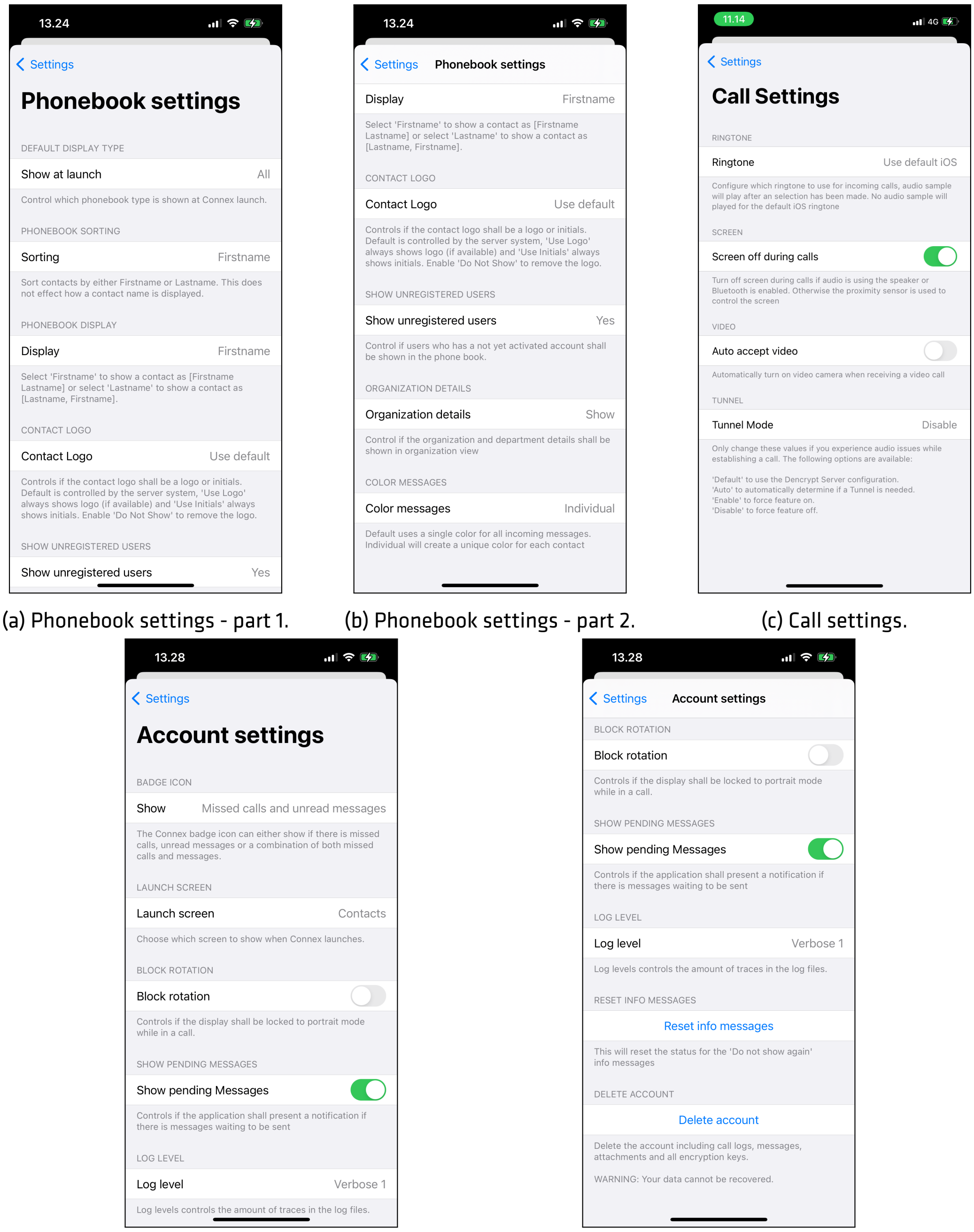
13.23

System information

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

App Name: Connex
App version: 6.4.01653
SDK version: 2.3.0-6094
Client ID: 94f769b3-b5a3-0064-b32f-64557c778464

Root certificate version: Application bundle
Client cert expiry date: 2025-02-17 15:44
DPS cert common name: Not installed

App bundle id: com.dencrypt.tngStore
OS Version: 16.1.1
Device Name: iPhone
Device Type: iPhone 13

Info generated: 22 Feb 2023 at 13.23.02
```

(c) System information

Figure 36: Settings and system information.



13.24

‹ Settings

Phonebook settings

DEFAULT DISPLAY TYPE	
Show at launch	All
Control which phonebook type is shown at Connex 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 server system, 'Use Logo' always shows logo (if available) and 'Use Initials' always shows initials. Enable 'Do Not Show' to remove the logo.	
SHOW UNREGISTERED USERS	
Show unregistered users	Yes

(a) Phonebook settings - part 1.

13.24

‹ Settings Phonebook settings

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 server system, 'Use Logo' always shows logo (if available) and 'Use Initials' always shows initials. Enable 'Do Not Show' to remove the logo.	
SHOW UNREGISTERED USERS	
Show unregistered users	Yes
Control if users who has a not yet activated account shall be shown in the phone book.	
ORGANIZATION DETAILS	
Organization details	Show
Control if the organization and department details shall be shown in organization view	
COLOR MESSAGES	
Color messages	Individual
Default uses a single color for all incoming messages. Individual will create a unique color for each contact	

(b) Phonebook settings - part 2.

11.14 4G

‹ Settings

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	
VIDEO	
Auto accept video	☐
Automatically turn on video camera when receiving a video call	
TUNNEL	
Tunnel Mode	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.	

(c) Call settings.

13.28

‹ Settings

Account settings

BADGE ICON	
Show	Missed calls and unread messages
The Connex 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 Connex launches.	
BLOCK ROTATION	
Block rotation	☐
Controls if the display shall be locked to portrait mode while in a call.	
SHOW PENDING MESSAGES	
Show pending Messages	☑
Controls if the application shall present a notification if there is messages waiting to be sent	
LOG LEVEL	
Log level	Verbose 1
Log levels controls the amount of traces in the log files.	

(d) Account settings - part 1.

13.28

‹ Settings Account settings

BLOCK ROTATION	
Block rotation	☐
Controls if the display shall be locked to portrait mode while in a call.	
SHOW PENDING MESSAGES	
Show pending Messages	☑
Controls if the application shall present a notification if there is messages waiting to be sent	
LOG LEVEL	
Log level	Verbose 1
Log levels controls the amount of traces in the log files.	
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.	

(e) Account settings - part 2.

Figure 37: Phonebook-, call-, and account 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 38. 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 Apple Appstore or pushed by a Mobile-Device-Management (MDM) system. The Dencrypt Server System is managed by a system administrator.

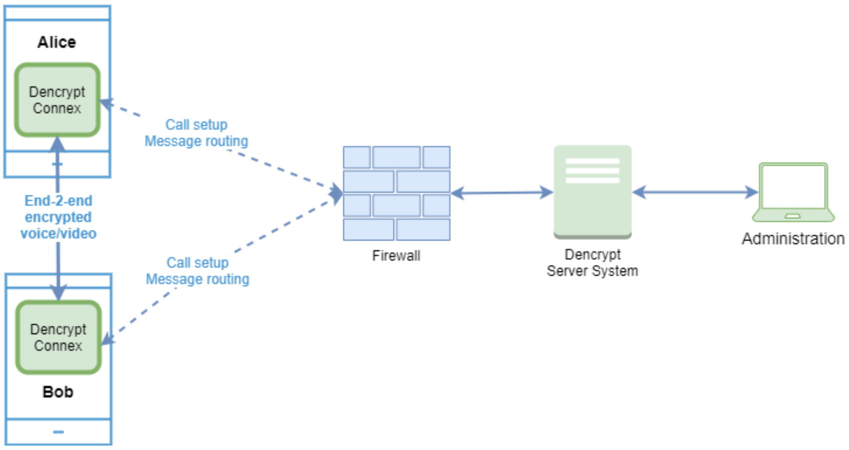


Figure 38: Dencrypt Communication Solution.

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 39

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.

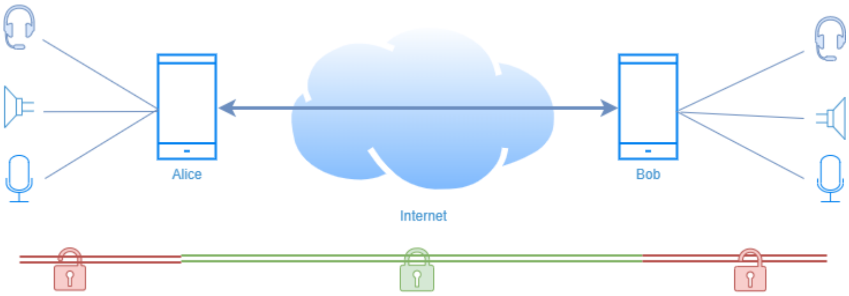


Figure 39: Area of protection for voice/video calls.

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 40.

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.

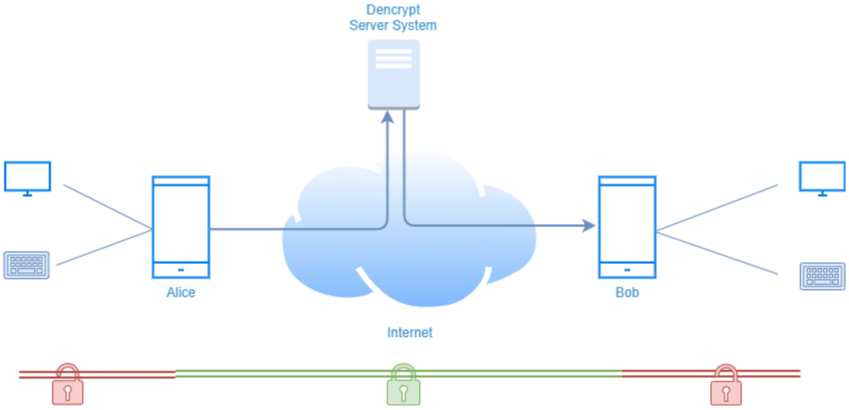


Figure 40: Area of protection for instant messaging

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.

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 Apple are used for alerting on incoming secure calls and messages. The push messages are sent 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:** INFO
- **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:** ERROR
- **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 Connex . 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 Connex did not have a valid account, please contact your administrator to get a Dencrypt Connex 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 Connex 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 Connex 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 Connex 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:**