Manual

Cryptify Call application for Android

Table of Contents

Scope

This document describes how to install, configure, operate and maintain the Cryptify Call application for Android.

Target audience is end users of Cryptify Call.

Introduction

Cryptify Call voice and messaging encryption for Android is approved by NCSC for HMG communication at level RESTRICTED/OFFICIAL SENSITIVE.

Using Cryptify Call is as simple as making an ordinary phone call or SMS. Cryptify Call have a familiar user interface, and is using the ordinary phone numbers. The solution works in parallel with the ordinary functions of the phone enabling users to choose whether to make a secure or an ordinary call.

Cryptify Call is using *Mobile Data* service in existing mobile networks and complementing Wi-Fi infrastructures. Being able to use Wi-Fi in addition to the Mobile Data services ensures a cost-efficient solution that provides even better availability than regular mobile voice service.

Subject to authorization by the CMS of the respective organization, users can communicate with users belonging to other organizations in an end-to-end encrypted and authenticated manner.

Cryptify Call is built on reliable standards and protocols enabling multi-vendor interoperability. The comprehensive security of the solution is based on well-proven standard algorithms and protocols such as Advanced Encryption Standard (AES), MIKEY-SAKKE, and Secure Real-time Transport Protocol (SRTP).

IMPORTANT! To receive calls and messages the Cryptify Call application must be running. The application is designed to always run, it will not drain the battery and there is normally no reason to turn it off.

Note! Cryptify Call is a Voice over IP (VoIP) solution and requires an Internet connection to work, either Wi-Fi or Cellular Data. In case of travelling abroad, please make sure *Data Roaming* is enabled on the cellular service!

Note! When using Cryptify Call, please find a secluded place to talk. This might be obvious but can easily be forgotten.

Procedures

Installation and configuration

There are two main ways in which Android devices are used in enterprises; administrators may have set up the devices with the Cryptify Call application, and other apps, before delivering them to end users, or end users may be able to install and updates app themselves.

Install Cryptify Call

If users are permitted to install, update or modify the apps on their Android devices, they can install Cryptify Call application on the device by opening the Google Play Store app  , downloading and installing the Cryptify Call application by selecting "Cryptify Call" from the search tab and clicking the install button.

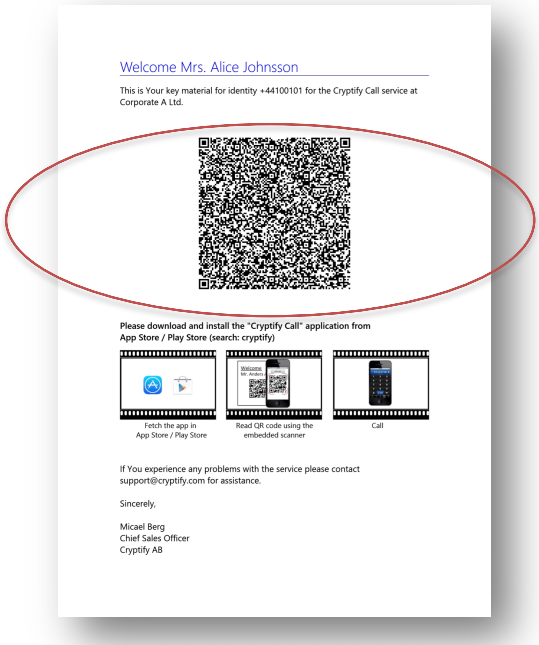
Otherwise, if the Cryptify Call app is not installed, users should ask their administrators to provision it for them.

Provisioning user credentials

Users are enrolled through a controlled onboarding process managed by the CMS Operator or another designated trusted authority. As part of this process, users are issued the Cryptify Call App (CCA) and provided with an initiation letter containing their unique provisioning QR code.

It is essential that users verify the authenticity of the initiation letter and the QR code prior to scanning. The QR code must originate from the CMS Operator or another explicitly trusted and authorized party. Users must not scan QR codes received from unknown, unexpected, or unverified sources. Furthermore, the QR code must be treated as secret and disposed of in a secure manner after it has been scanned.

To provision the app, start the Cryptify Call app and use the embedded scanner to read the QR code provided in the initiation letter.



Welcome Mrs. Alice Johnsson

This is Your key material for identity +44100101 for the Cryptify Call service at Corporate A Ltd.

Please download and install the "Cryptify Call" application from App Store / Play Store (search: cryptify)

Fetch the app in App Store / Play Store

Read QR code using the embedded scanner

Call

If You experience any problems with the service please contact support@cryptify.com for assistance.

Sincerely,

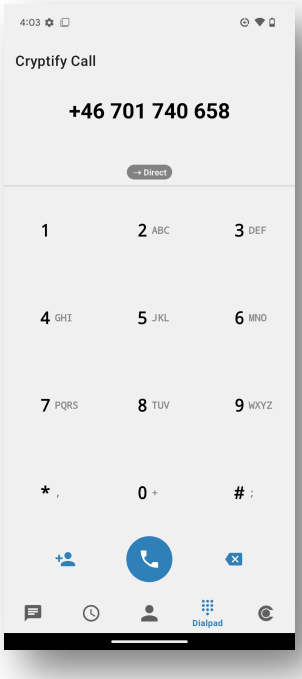
Micael Berg
Chief Sales Officer
Cryptify AB

It is recommended that the initiation letter be destroyed once successfully scanned in order to ensure the credentials don't get into the wrong hands.

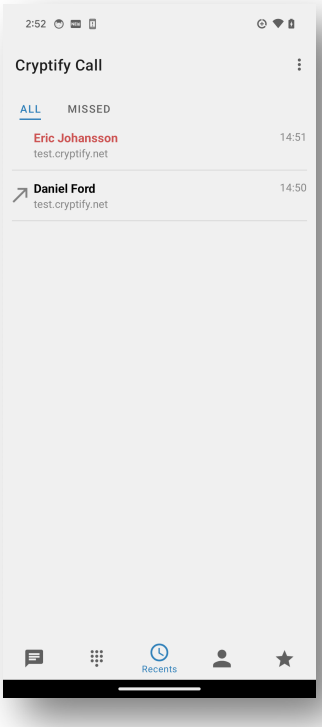
Make a secure call

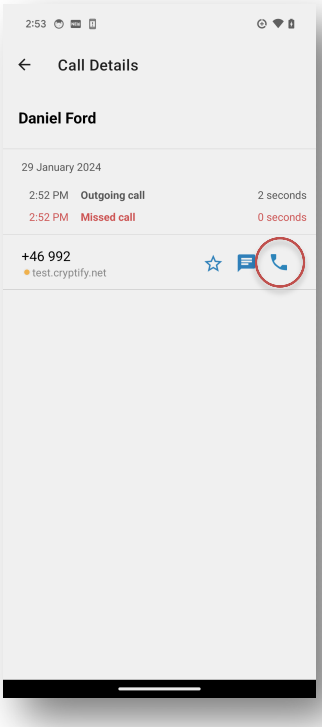
Making a secure call is as easy as dialing the number of the person to call, and normally the number is the same as the mobile number for that person. The only requirement is that both parties use Cryptify Call.

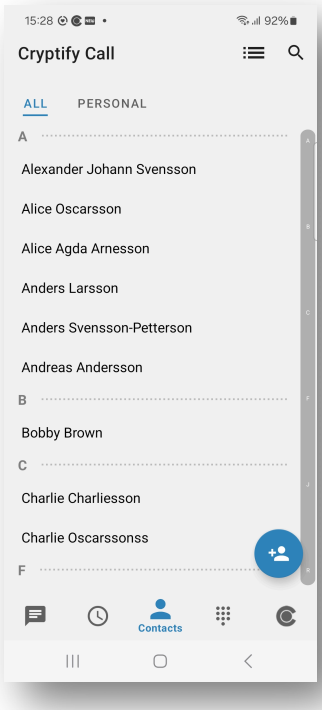
The number can be entered using the dialpad.

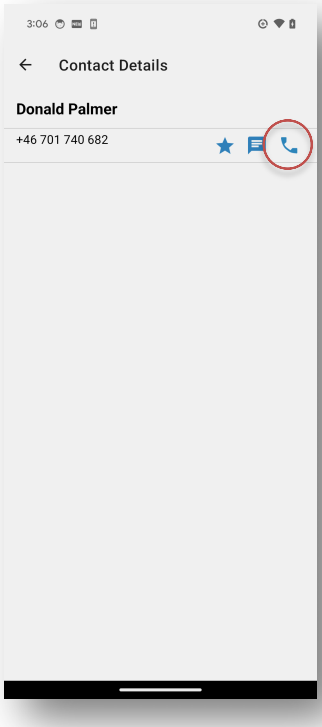


The application also has a *Recents view* where the call log is listed, and a *Contacts view* displaying all contacts available to the app. Contacts are sourced from the contact book stored on the phone, from distributed contact lists as well as from the personal contact list. A secure call can be initiated from the *Details view* of a selected contact.





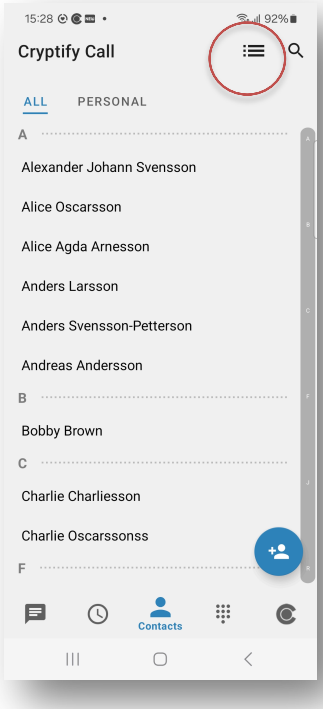


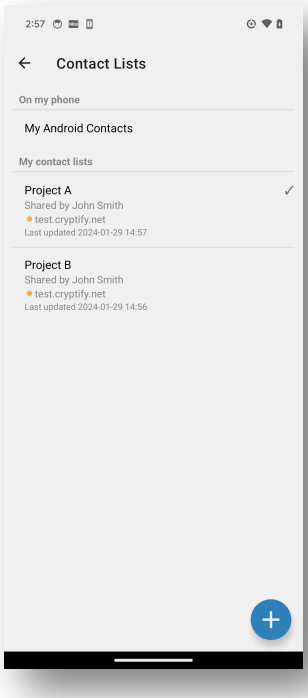


Tapping the lists icon on the Contacts tab shows all available contact lists. Lists that are enabled – that is, are used as a source of contacts – are marked with a checkmark. To enable or disable a list, tap the list and toggle the “Enabled” switch.

Shared contact lists are automatically kept up-to-date, and to unsubscribe from future updates you need to contact the admin of the list. New lists appear in bold face.

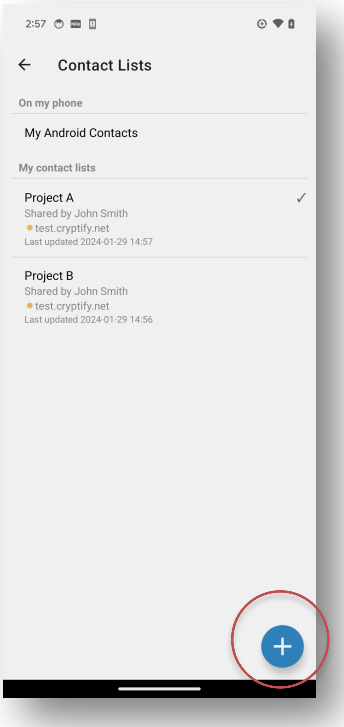
Only enable or import lists from trusted and verified sources. Importing or activating lists from untrusted or unknown sources may compromise the security of the application.

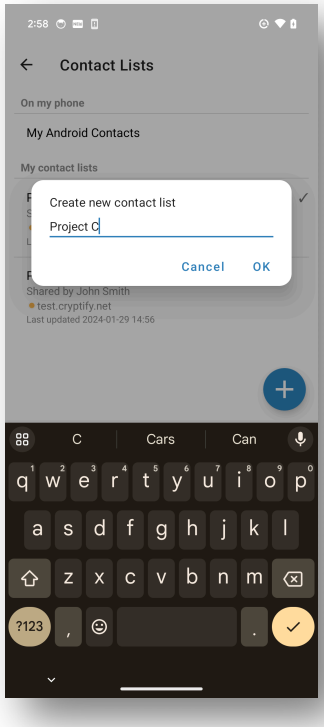




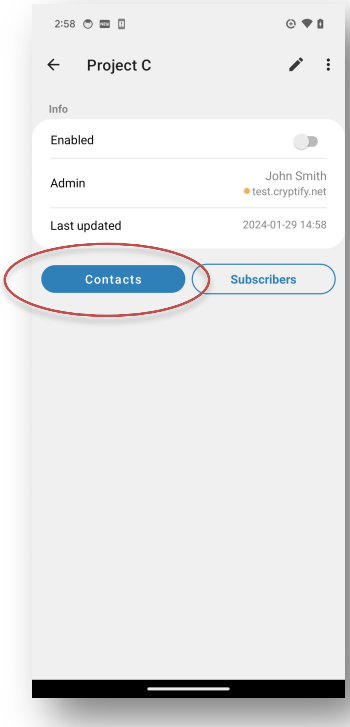
Creating and sharing contact lists

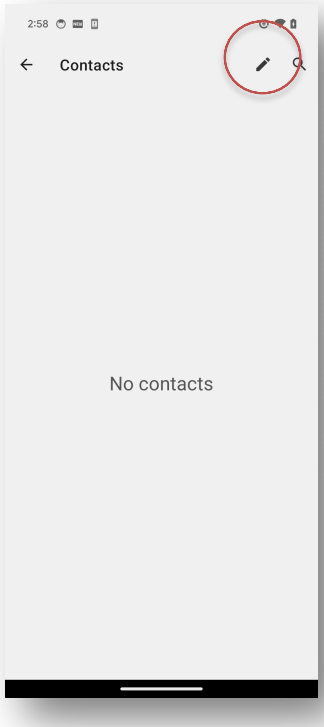
Contact lists can be created within the Cryptify Call app, and optionally shared with other users in a secure manner. To create a new contact list, tap the “+” button and enter a name for the contact list.



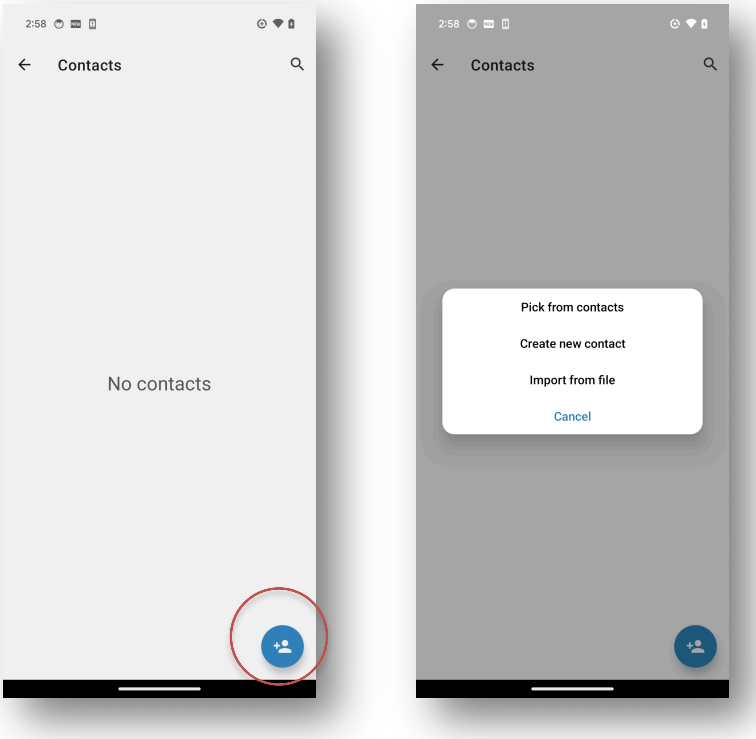


To modify the entries of the contact list, tap “Contacts” and then the edit button.



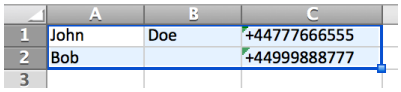


To add a new contact, tap the floating action button and select either “Create new contact”, to manually create a new contact list entry, or “Pick from contacts” to copy existing contacts from other contact sources, including the native phone book.



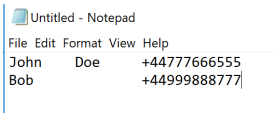
It is also possible to import contacts from a TSV (tab separated values) file by clicking the import button and selecting “Import from file”.

The file should have UTF-8 (or ASCII) encoding with three columns per line, specifying the first name, the last name and the phone number. It is easy to create such a file using Excel and Notepad (or TextEdit on macOS).

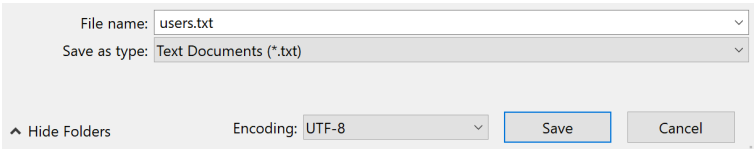


	A	B	C
1	John	Doe	+44777666555
2	Bob		+44999888777
3			

Step 1: Select a range of cells containing three columns and choose copy the cells using Edit > Copy (or control-C).

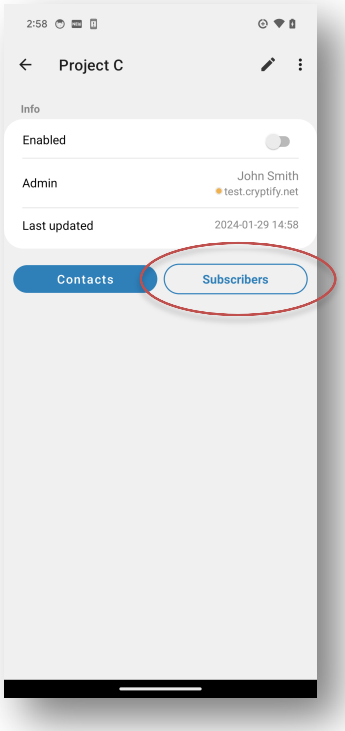


Step 2: Paste the result into a new document in Notepad. (If using TextEdit on macOS, select Format > Make Plain Text before pasting the data.)



Step 3: Save the document, and make sure to select UTF-8 encoding.

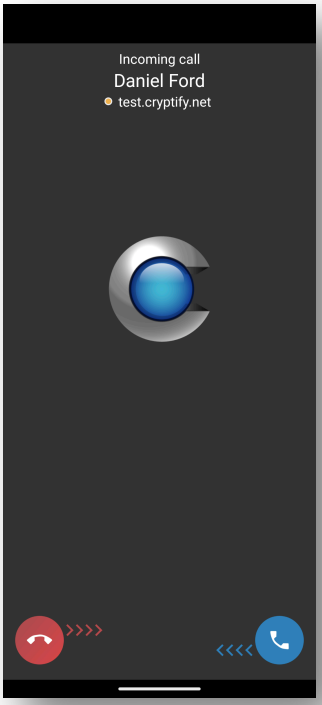
Similarly, the list of subscribers – that is, those who will receive the contact list – is edited by tapping “Subscribers”. As before, only a contact list that is marked as “Enabled” is used as a contact list source, but even disabled lists are distributed to subscribers.

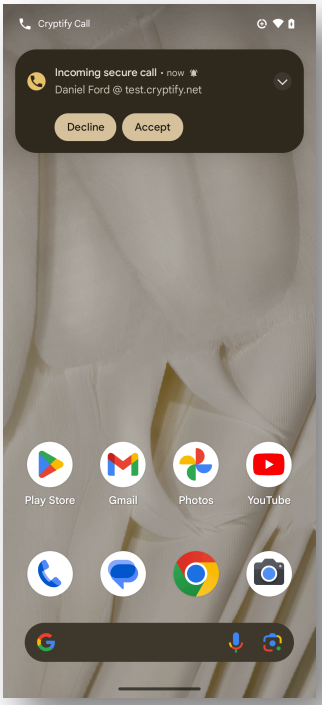


Answer an incoming secure call

An incoming secure call will be displayed together with the number of the person who is calling and the Security Domain that person belongs to. If there is a contact available in the device for that number, the contact name is displayed instead of the number.

The incoming call is notified either in full screen or as a notification:

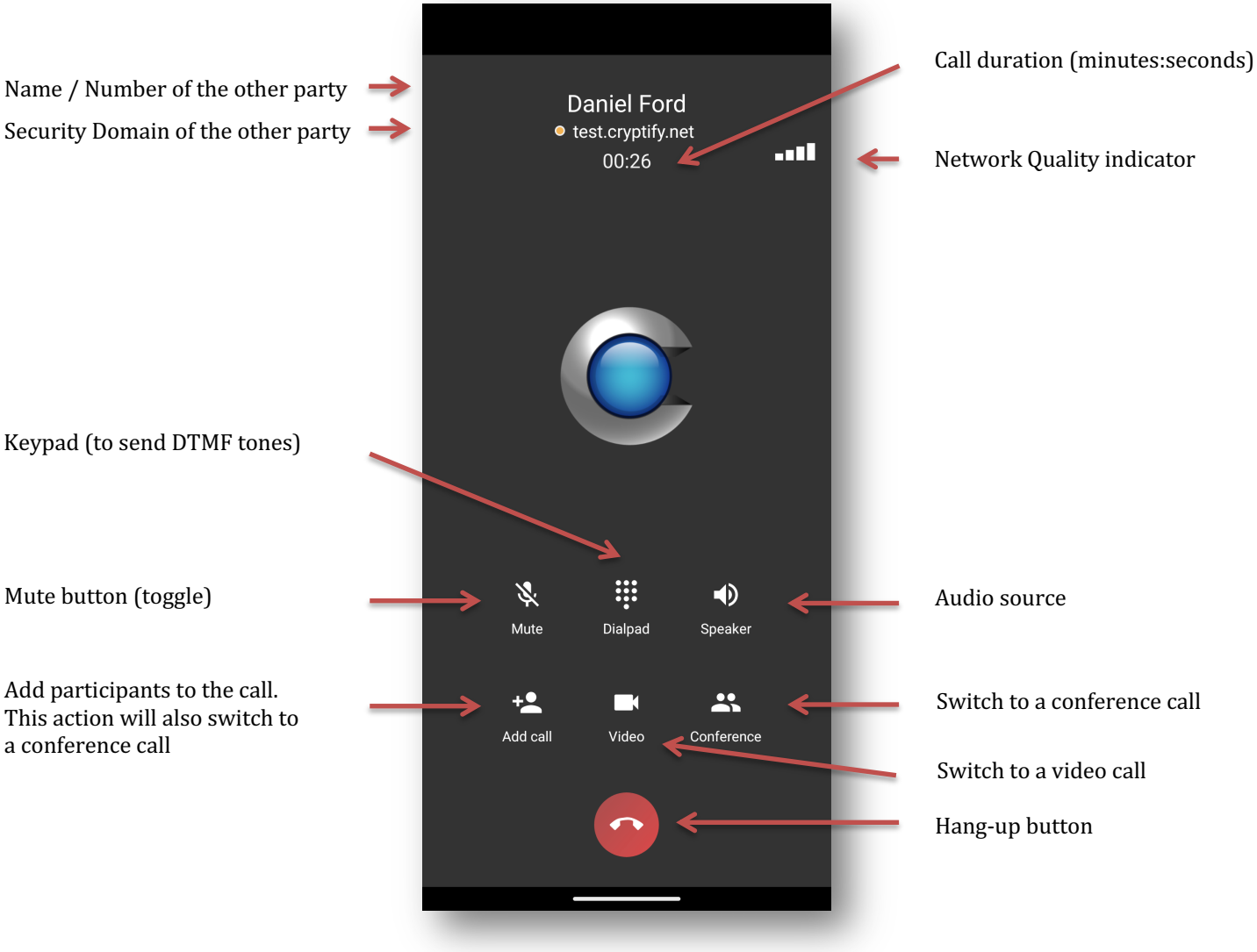




On the lock screen, the call is accepted by swiping the *accept button* to the left, or rejected by swiping the *decline button* to the right. Otherwise, simply tap the accept or decline button.

During a call

When a secure call is active the user is presented with relevant information about the ongoing call.

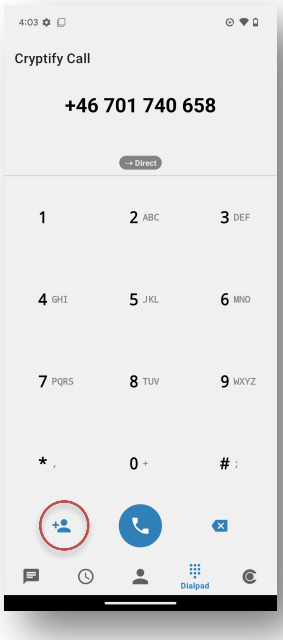


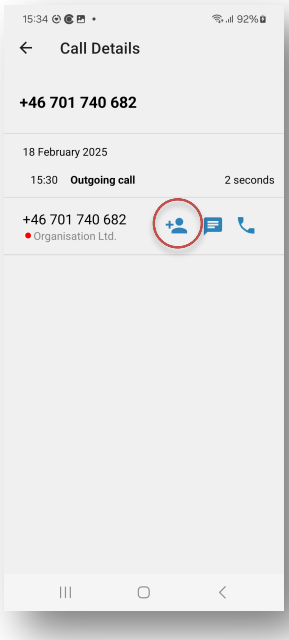
The Network Quality indicator shows the quality of the data connection, which might differ from the signal strength indicator provided by Android. An example is cell congestions; where the signal strength might be excellent but no data can be transmitted over the cellular network.

Video calls are automatically disabled when the other party, or an intermediate server, does not support video calls. Note that video calls have much higher bandwidth requirements and transfers much more data compared to regular secure calls.

Adding Personal Contacts

A *personal contact* is added by tapping the *personal contact* button for a phone number that is not already in a contact source, or by using the "+"-button in the Contacts tab.



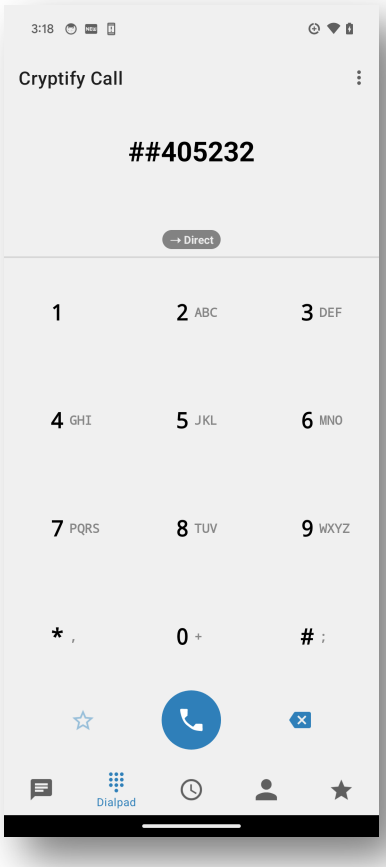


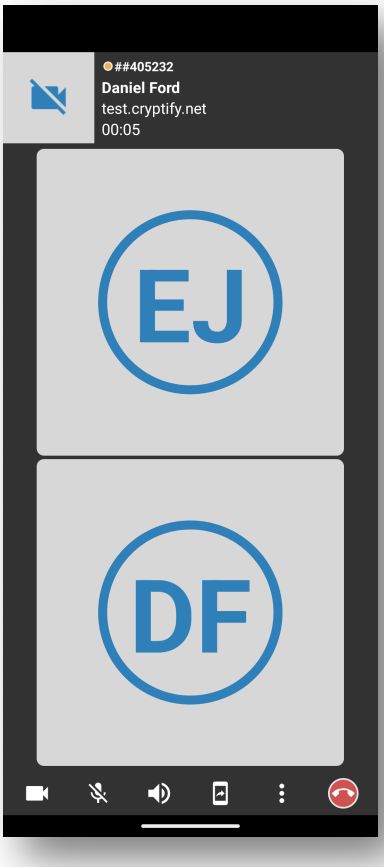
Conference calls

Cryptify Call supports secure, end-to-end encrypted conference. Participating in a secure conference is just as easy as calling a regular conference bridge, and a *conference host* controls which callers are allowed to join the conference.

Dial in to a conference

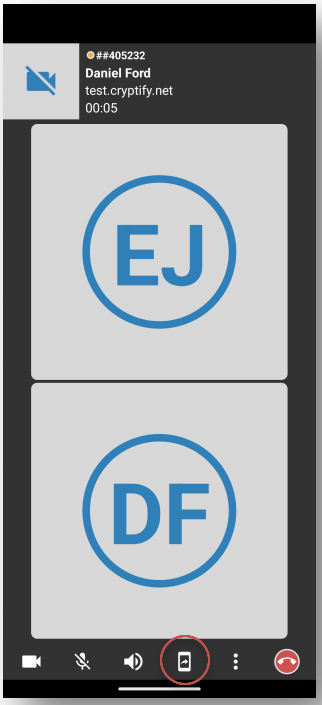
To dial in to a conference you simply dial the six-digit number given to you by the conference host on the dial pad, prefixed by "##". While you wait for the conference host to accept your participation, the screen displays "Waiting for host" and an ordinary ring back tone is played in the speaker. Once accepted by the host you can see the other participants.

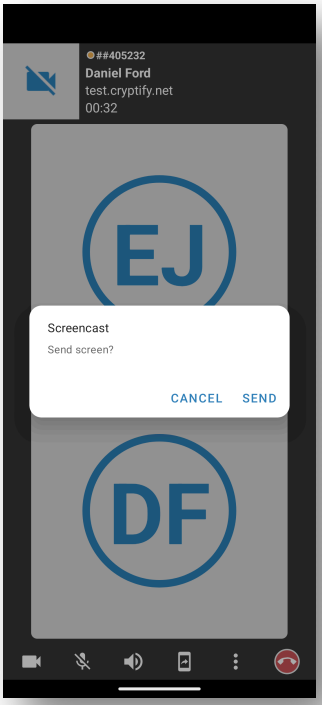




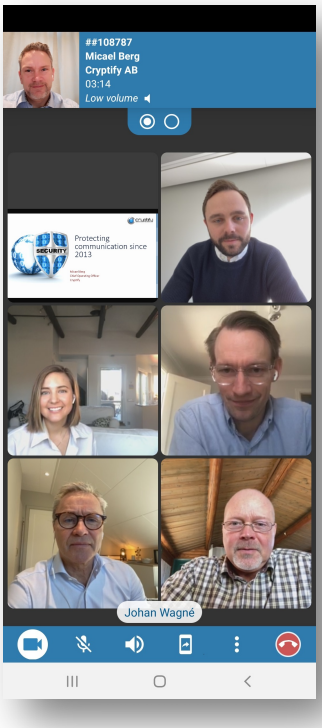
Screen sharing

Participants can share their screen during a conference by pressing the *Screencast* button from the menu.





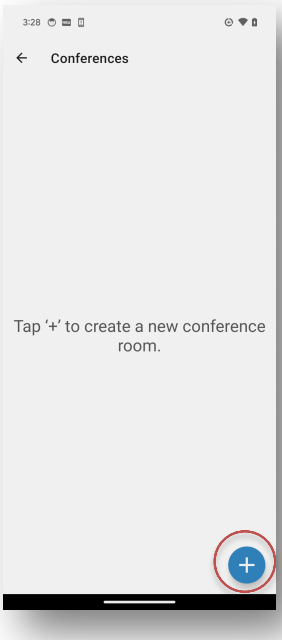
Shared content from other participants will be presented in their video tile. Pressing on a video tile will present that participant in in full screen.

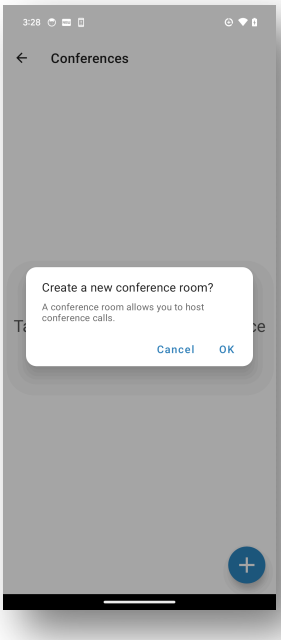


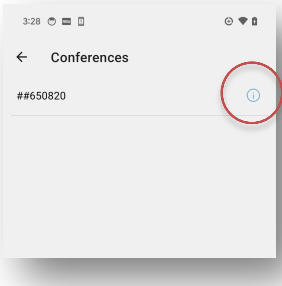
Hosting a conference

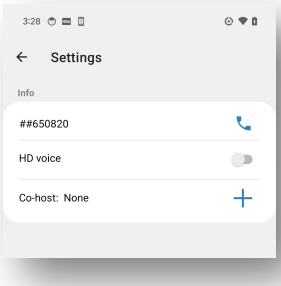
To host a conference, you must first create a *conference room*. A conference room is identified by a six-digit number, which the system automatically generates. Once a conference room has been created, it can be used indefinitely.

To create a conference room, select “Conferences” under the “More” menu, tap the “+” button and confirm the creation. A new conference room is then created and assigned a randomly selected number, which is used by participants to join the conference. Tapping the details button allows you to define a co-host that can host conference calls using your conference room number. You can also enable HD-voice which offers higher quality audio but also requires better network conditions.







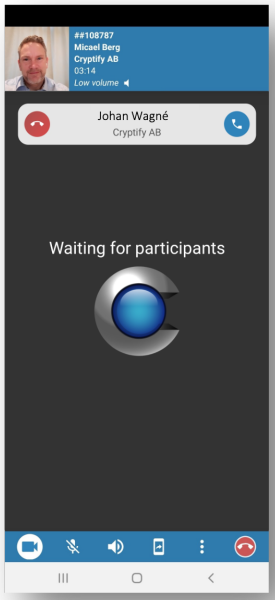


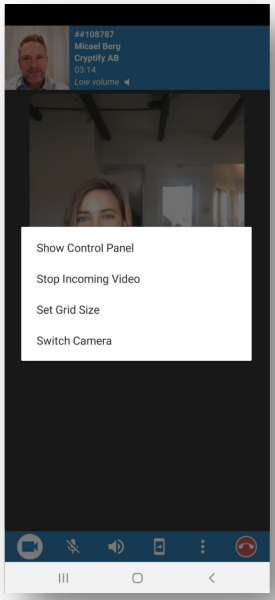
If desired, you can create multiple conference rooms and use them for different meetings, but you can only host one conference at a time. To remove a conference room, simply long press the desired row and tap the delete button.

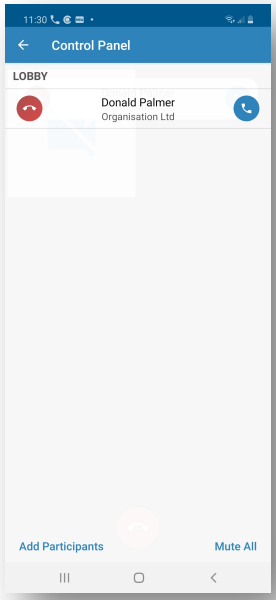
The conference room number is distributed to the participants, along with the date and time for the conference. As the conference room number plays no role in the security of the conference, the number can be distributed to the participants in any form, for instance via email or by using a shared calendar.

When the conference should begin, the host simply dials the conference room number on the dial pad, prefixed by "##", or uses the call button in the list of conferences.

The host manages the conference using the *Control Panel*, where the host can admit, invite and mute participants.







In addition to participants dialing into the conference, the host can invite participants using the *Add Participants* function in the *Control Panel*.

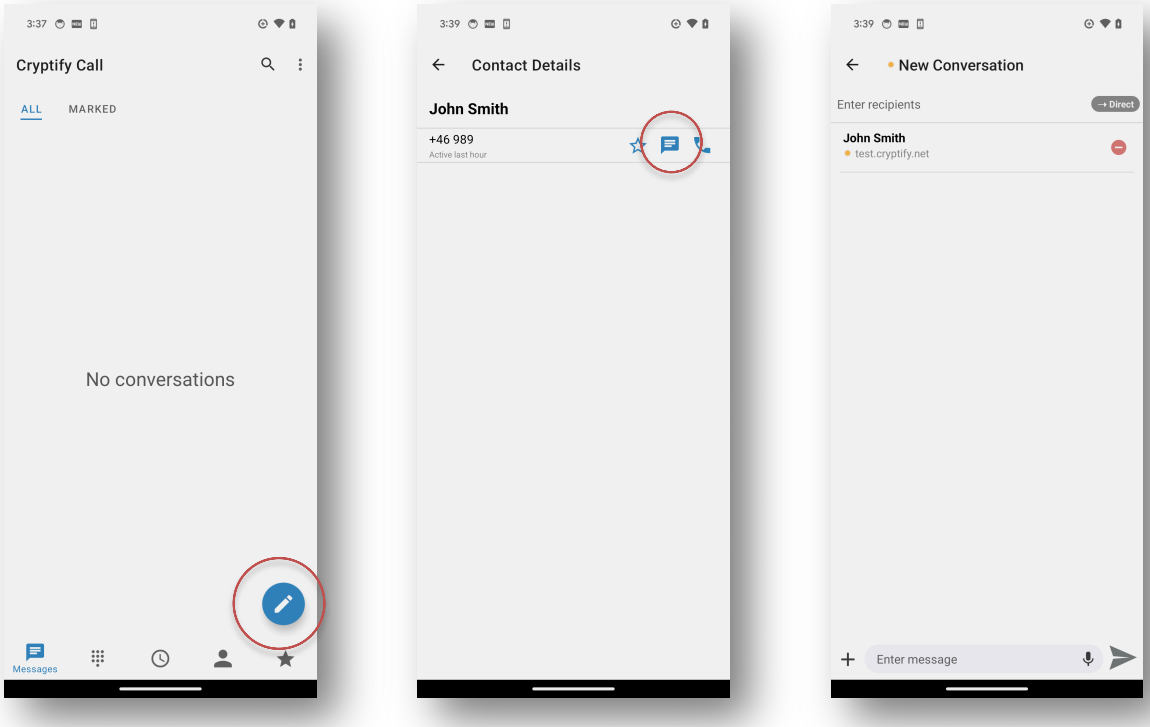
Accepting a caller into a conference is a one-way process, and it is not possible to force a caller to leave an ongoing conference. For this reason, users who have been accepted into the conference are also automatically accepted if they lose network connectivity and dial into the conference again.

Note also that the entire conference is protected by a secret randomly generated by the conference host each time he or she (re-)enter the conference. If the conference host hangs up the conference continues, but new participants cannot be accepted. Should the conference host dial in again, the conference will start anew after a brief interruption whilst rekeying.

Best practice for allowing an external party, say, to participate only in the latter part of a conference is to maintain two conference rooms, and move to the second conference room when the external party should join.

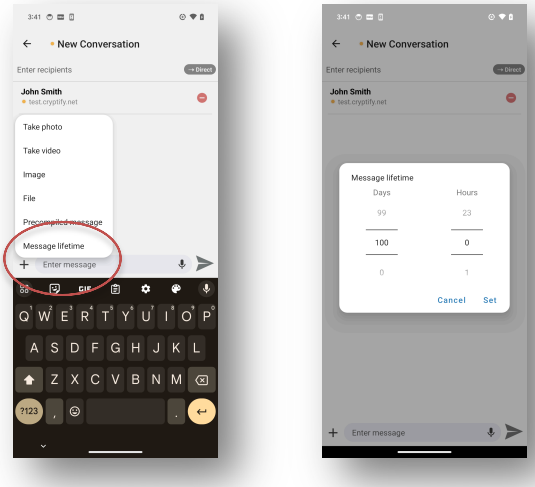
Secure text messages

To start a new conversation, tap the new message floating action button in the *Messages* view or tap the new message button on the *Contact Details* view.



To post a new message in an existing conversation, open that conversation and select the input field to bring up the keyboard. To attach an image or a video to the message, tap the paper clip and select an image from the phone's library or take a new picture or video. Press the send button to send.

The administrator can limit for how long messages can be viewed in the app, in which case messages expire at a specific point in time. Note that messages may expire before the recipient has viewed them. The maximum lifetime cannot be increased, but it is possible to select a shorter message lifetime by selecting "Message lifetime" from the "+"-menu.

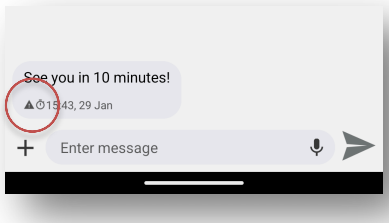


A message that will expire is marked with a timer icon next to the message time stamp. To show when the message will expire, long press the message and select “Status”.

The status of an outgoing message is displayed next to the timestamp:

- *Sending* – the message is being uploaded to the server.
- *Sent* – the message has been transferred to the server.
- *Notified* – iOS recipients only. The recipient has been notified of the message.
- *Delivered* – the message has been delivered to the recipient.
- *Read* – the recipient has opened the conversation.
- *Failed* – sending the message failed; long press the message and select “Status” for more information or “Resend” to immediately try again.

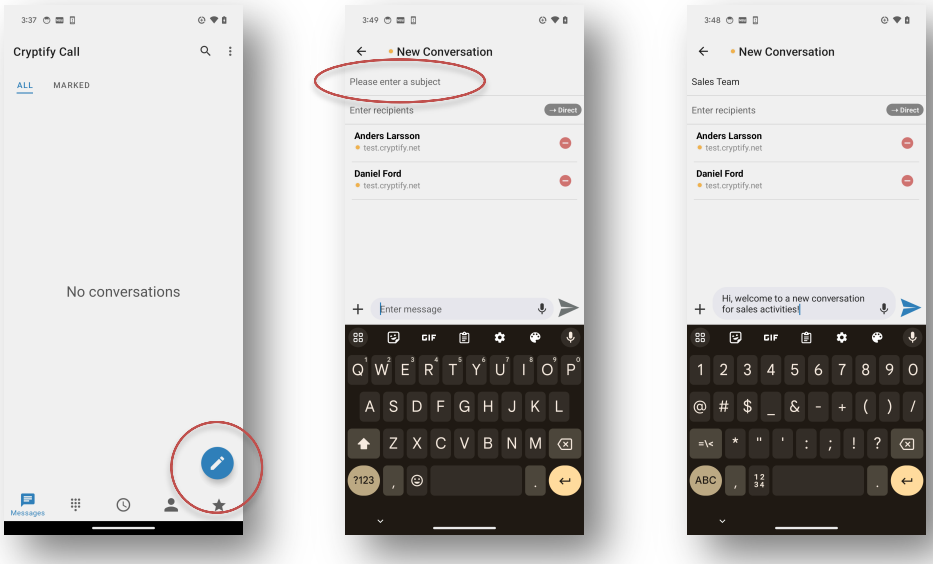
To show the sender’s compose time of an incoming message, long press the message and tap “Status”. If this timestamp differs more than 5 minutes from when the message was received, a warning icon is shown.



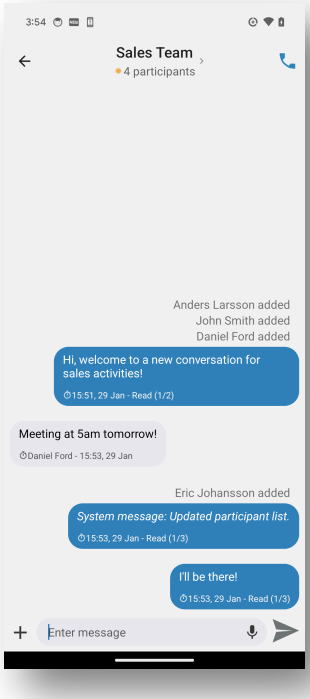
Groups

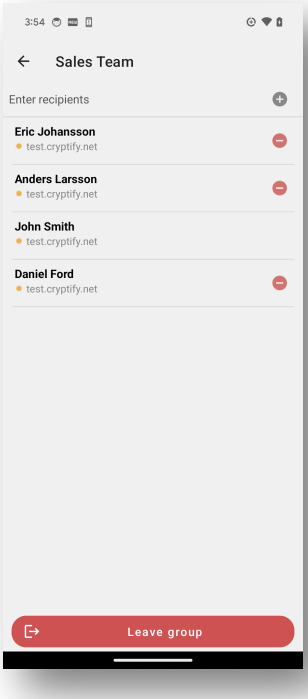
Setting up a group conversation is as easy as sending a regular text message. The *instant group conversations* replace the *managed groups* concept found in older versions of Cryptify Call.

To start a new *instant group conversation* simply tap the new message floating action button in the *Messages* view and add the recipients. If more than one recipient is added an *instant group conversation* is created and a *Subject* field is presented.



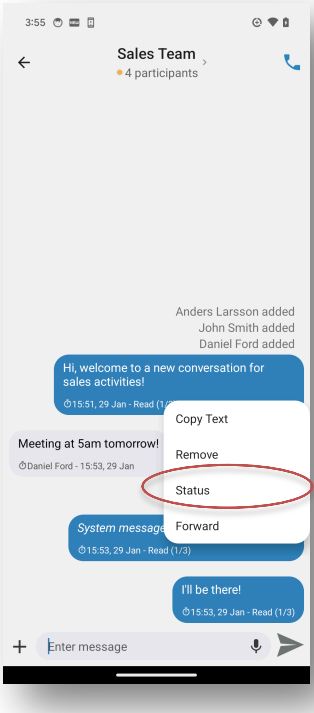
To add and remove recipients from the group conversation tap the group name.

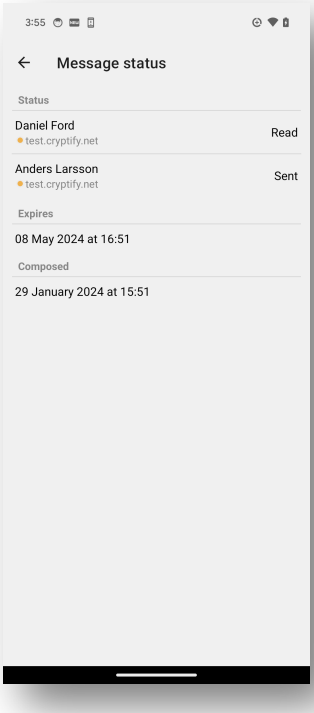




Each received message is marked with the identity of the sender as well as a timestamp of when the message was received. The history of added and removed are presented in the conversation.

To view the delivery status a posted message, long press on the message to bring up a pop over menu and select *Status*

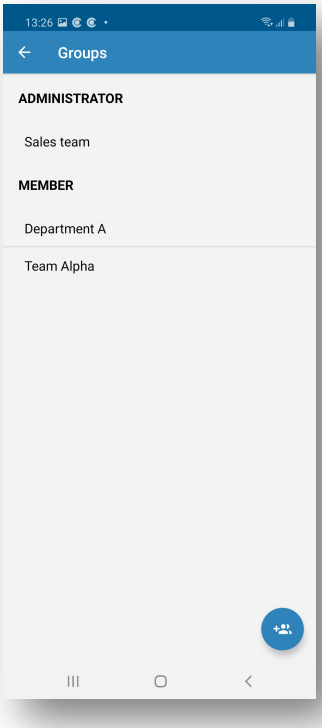


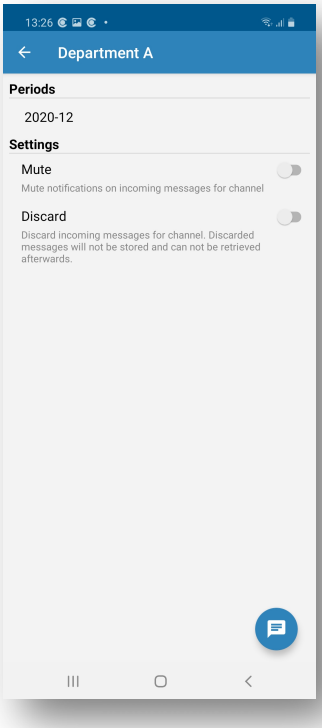


Channels

In addition to Groups, Cryptify Call also supports so called *channels*, which are message groups that are centrally managed by the CMS operator. Channels are particularly well suited for large groups, such as everyone in an organization, and there is no extra step where the user accepts or declines membership.

Channels are shown in the list of Groups under “Member” and work just as regular message groups. However, as channels supports thousands of users, it is for performance reasons not possible to see when a particular user has received or read a message.





By default, and just as for regular text or group text messages, each incoming message to a channel renders a notification. It is, however, possible to *mute* a channel, which prevents notifications on incoming messages to that channel. Only the notification is blocked, ensuring that the messages can be read if they are decrypted within 14 days (unless prevented by message expiry).

It is also possible to configure that incoming messages to a channel should be discarded immediately when received, without ever being decrypted or notified. Discarded messages are permanently deleted and cannot be retrieved at a later time.

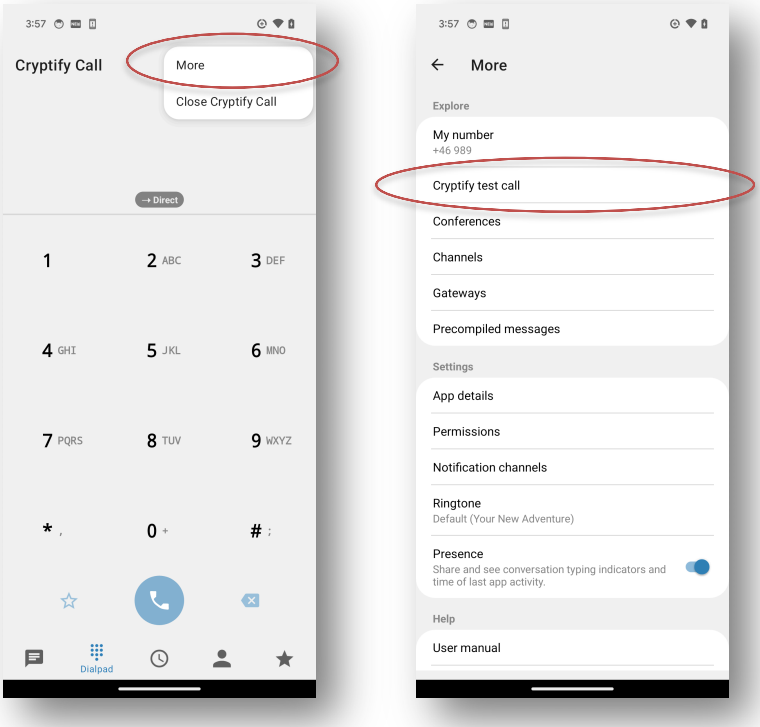
If a device is to be offline for an extended period of time, it is recommended to configure any high traffic channels to discard incoming traffic. Otherwise, once the device goes online, the app may become unresponsive while it decrypts the messages that have been queued up.

The channel settings are also visible under Settings > Channels.

Cryptify Test Call

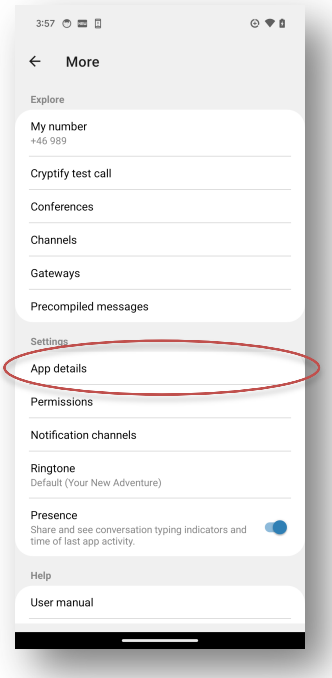
A user can make a Cryptify Test Call to verify the call quality.

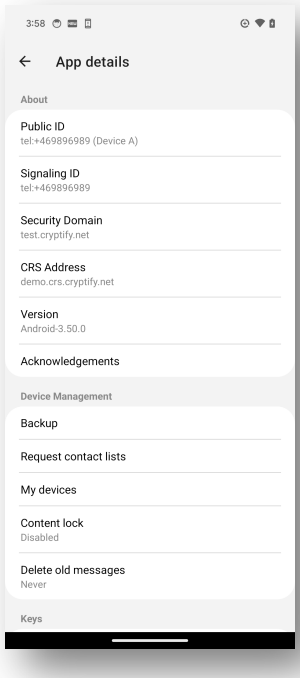
In the *More* menu select *Cryptify Test Call* and follow the audio instructions.



App details

In the *More*–menu select *App details* to display detailed information of the Cryptify Call application.



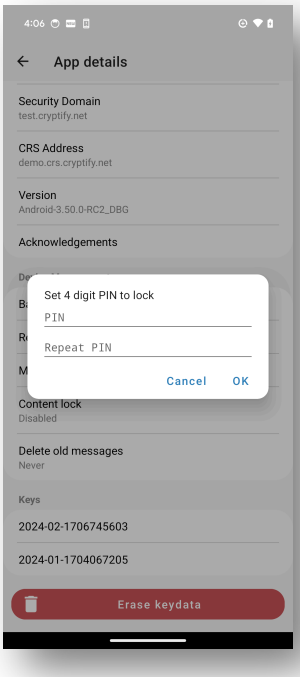


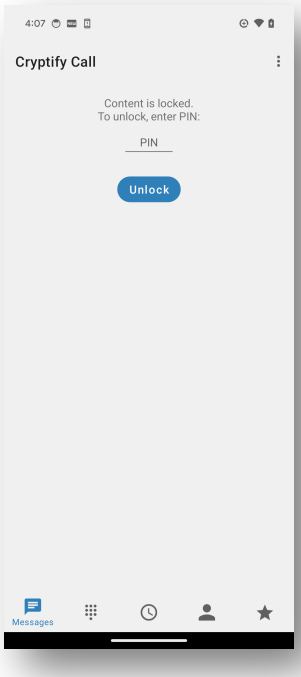
Name	Description
Public ID	This is the users public cryptographic identity
Security Domain	This is the identity of the Cryptify Management System (CMS) that has issued the cryptographic keys for the user
CRS Address	This is the Fully Qualified Domain Name (FQDN), or IP address of the Cryptify Rendezvous Server (CRS) serving the user
Keys	Valid keys are listed. There could be two keys during the grace period. Syntax is YYYY-MM-XXXXXXXXX, where YYYY-MM is the year and month the key is valid

NB! *Erase Keydata* will prompt the user to erase all content and settings for the Cryptify Call application! The app will not be usable until a new QR code has been scanned.

Content Lock

Contacts, messages and call history can be locked with a PIN code by tapping “Content Lock” and entering a 4 digit PIN code. If the PIN code is forgotten, the message tab can be unlocked with a PUK code available in the Cryptify Management System.



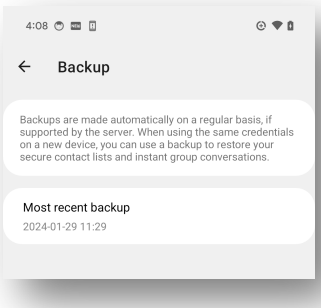


Backup

The app will automatically create a backup and deposit on the CRS. The backup is protected with a key derived from the update key, i.e. as long as the update key is unchanged the backup can be used to restore settings on a new device.

The backup contains the following data:

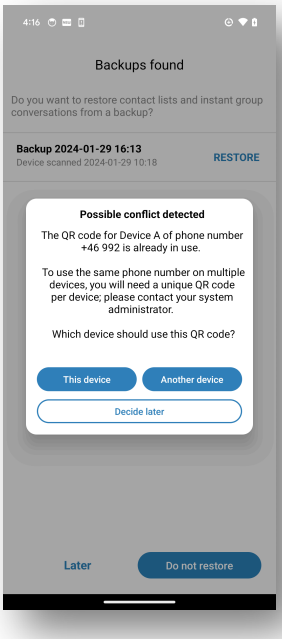
- Contact lists
- Group conversation participants

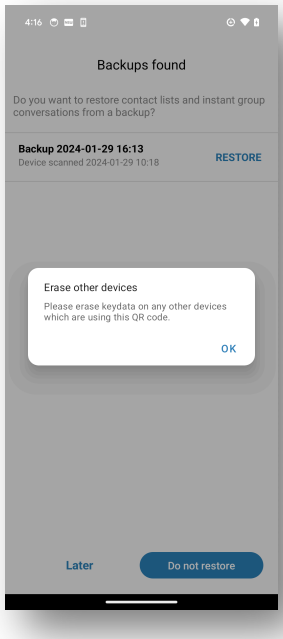


Restore

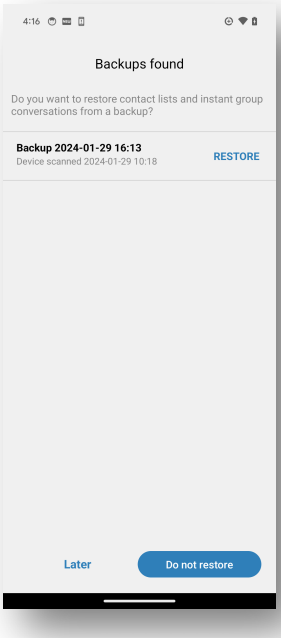
When switching to a new device, the latest backup is automatically restored on the new device when the same QR-code is scanned.

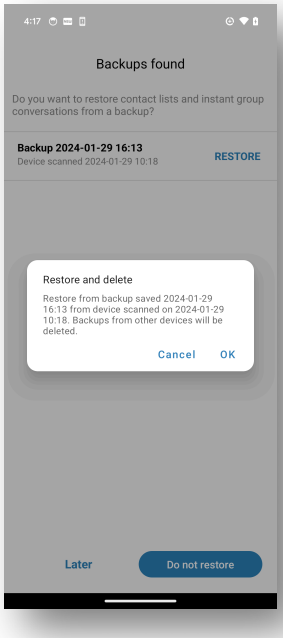
To use the same phone number on multiple devices, QR-codes for separate devices (Device A, Device B or Device C) must be generated in the Cryptify Management System. If, on the other hand, the same QR-code is used on multiple devices at the same time – which is not supported – the app will detect the reused QR-code and ask the user to resolve the conflict.

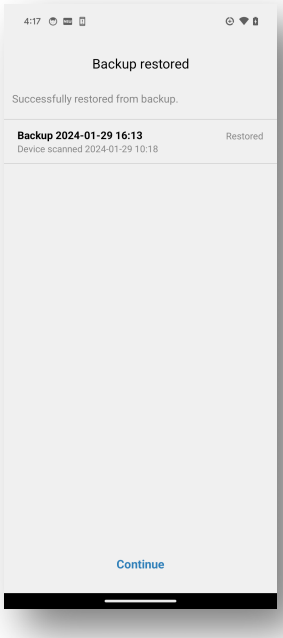




If continuing, available backups will be presented and the user can select to restore.







However, if the update key is changed between the backup and newly scanned QR code the restore operation will fail as the app cannot decrypt the content.

Application update

To guarantee full functionality and security within the application it is important that users keep Cryptify Call up to date.

If users are permitted to update their apps, they will receive notifications from the Play Store when a new version is available. When the Play Store indicates that an update is available, the user should open the Play Store app, select the update tab, and click the update button for Cryptify Call if shown.

Play Store enables automatic updates of apps. To disable automatic updates, please open Google Play Store.

All apps

- Menu -> Settings
- Un-check “Auto-update apps”

Cryptify Call specifically

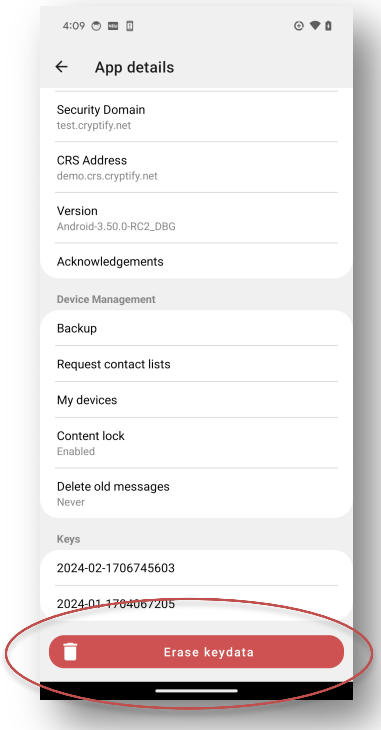
- Select “Cryptify Call” under “My apps”
- Menu -> uncheck “Auto-update”

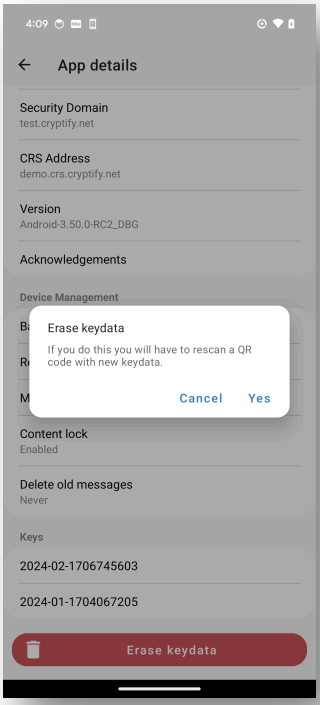
Otherwise, administrators for the local system may ask to update the apps when these updates are available on behalf of their users.

Manual key removal / replacement

This procedure is in case the keys should be deleted from the device, or if the CMS administrator decides to perform a manual key replacement. Normally keys are updated automatically without any user intervention.

In the *More* view, select *App details* and then *Erase keydata* and press the *"Yes"* button.





The application will now search for the QR code containing the key update.

NB! Erase keydata will prompt the user to erase all content and settings for the Cryptify Call application, including stored messages, call history, and stored favorites!

New keys must be received by the user in the form of a QR code, see Provisioning user credentials above.

Configuration

Application specific configuration

Parameters that can be configured by the users are presented in the *Settings* menu.

Ringtone
This is the ringtone played during incoming calls.
The user can select from a list of different ring tones.

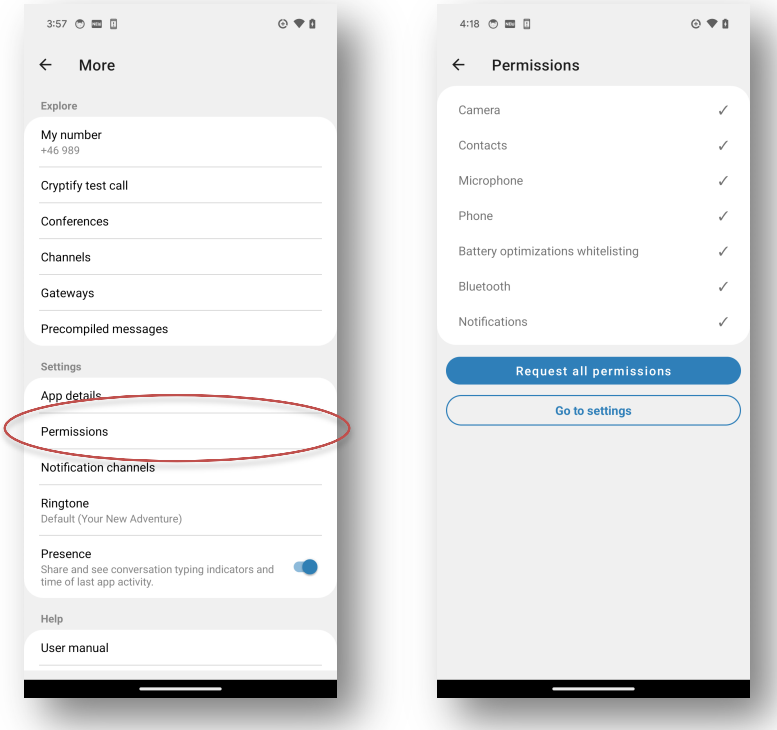
On Android 10 and later, the ringtone is instead configured using the notification channel settings in the System settings app.

Notification sound
This is the sound played during incoming messages.
The user can select from a list of different ring sounds.

On Android 8 and later, the notification sounds are instead configured using the notification channel settings in the System settings app.

Permissions

Please verify that your settings are as presented below



Troubleshooting

Reason Codes

Unsuccessful call establishment

Reason Code	Description
Not Found	There is no match for the called number. Either the called number does not have a Cryptify Call subscription, or the called number belongs to another Cryptify Call domain not connected to callers' domain. To request another Cryptify Call domain to be connected / approved, please contact Your local Cryptify Call support.
Not Available	The called number is currently not connected to the system, e.g. when the phone is powered off, or in airplane mode, or if the called party have manually terminated the Cryptify Call application.
Busy	The called party declined the call, or is currently occupied by another call, either an ordinary call or a secure Cryptify Call.
Communication Failure	This could be caused by an incompatible software version. Please make sure Your and called party's Cryptify Call applications are up-to-date. If this happens repeatedly please contact Your local Cryptify Call support.
Authentication Failure	Cryptographic failure. Please contact Your local Cryptify Call support!
No Answer	The called party has not answered the call within one minute.

Dropped call

Reason Code	Description
Network Failure	No audio received the last 30 seconds. The network problem could be either you, or the other party. This problem is normally triggered when going out of cellular coverage, e.g. a building, underground, etc.

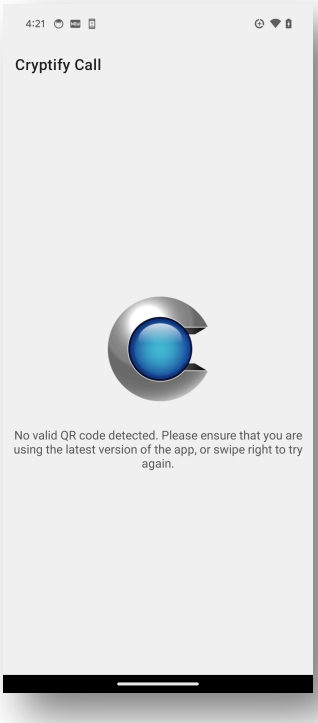
Unsuccessful messaging

Reason Code	Description
Failed, user not found	There is no match for the recipient number. Either the recipient number does not have a Cryptify Call subscription, or that number belongs to another Cryptify Call domain not connected to callers' domain.

	To request another Cryptify Call domain to be connected / approved, please contact Your local Cryptify Call support.
Failed, bad network	Several failed attempts to send the message. This is caused by unstable network connection. If You are using Wi-Fi, please disable Wi-Fi and try again. If this happens repeatedly please contact Your local Cryptify Call support.
Failed to authenticate	Cryptographic failure. Please contact Your local Cryptify Call support!
Failed, invalid	This could be caused by an incompatible software version. Please make sure Your and called party's Cryptify Call applications are up-to-date. If this happens repeatedly please contact Your local Cryptify Call support.
Failed, no support	This could be caused by an incompatible software version. Please make sure Your and called party's Cryptify Call applications are up-to-date. If this happens repeatedly please contact Your local Cryptify Call support.

FAQ

Q: Why do I get a failure when scanning a QR code?



A: Failure to scan a QR code can be subcategorized into the following subcategories

1. Video quality problem
   Symptom: The app is unable to detect the QR code and keeps on recording
   Description: if the captured video feed does not have high enough quality it will not be possible to decode images containing the QR code.
   Remedy: This is normally due to a malfunctioning camera or distorted paper copy of the QR code.
2. QR code not created by a Cryptify Management System
   Symptom: Error message stating, "No valid QR code detected"
   Description: the Cryptify Call app will only accept a QR code that is created by a Cryptify Management System
   Remedy: Please request a QR code from your system administrator
3. Obsolete app version
   Symptom: Error message stating, "No valid QR code detected"
   Description: In case the system administrator enables mandatory policies only Cryptify Call version compliant with such policies will accept the QR code.
   Remedy: Please update to the latest version of the Cryptify Call app in the Google Play Store.

Q: Why doesn't my app get the monthly update?
A: Failure to get monthly update can be subcategorized into the following subcategories

1. Network problem
   Symptom: "Unable to connect" in the Cryptify Call service notification
   Description: The app must be able to connect to the Cryptify Rendezvous Server in order to download new updates and to use the Cryptify Call service.
   Remedy: Please acquire network connectivity in order for the device to connect to the Cryptify Rendezvous Server
2. Obsolete app version
   Symptom: Key for the period is not listed under More->App details. Keys for September 2020 will have the syntax "2020-09-NNNNNNNNNN"
   Description: In case the system administrator enables mandatory policies only Cryptify Call version compliant with such policies will accept the update.
   Remedy: Please update to the latest version of the Cryptify Call app in the Google Play Store.
3. Changed update key
   Symptom: Key for the period is not listed under More->Advanced. Keys for September 2020 will have the syntax "2020-09-NNNNNNNNNN"

Description: In case the system administrator has deleted the account or performed a “re-key” operation the existing update key stored is no longer valid.
Remedy: Please request a QR code from your system administrator