DENCRYPT

Dencrypt Communication Solution

Operational user guide

Dencrypt Message 1.2

for Android

Version 1.0

05 March 2021

Public

Contents

Version

This guide applies for:

- Dencrypt Message v. 1.2 for Android devices

1 Introduction

Dencrypt Message is an application for sending encrypted messages and content sharing from Android devices. It uses the patented Dynamic Encryption technology to apply state-of-the-art, end-to-end encryption information sharing between devices.

This guide is intended for end-users of the Dencrypt Message application and provides instructions to operate and use the application in a secure way.

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

2 Dencrypt Communication Solution

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

The solution consists of:

- **Dencrypt Talk** , Android smartphone application for secure voice communication.
- **Dencrypt Message** , Android smartphone application for secure messaging.
- **Dencrypt Server System** provides the infrastructure for establishing secure communication.

The Dencrypt Server System is responsible for setting up the encrypted calls, routing messages, and for distributing an individual phonebook to each device, defining to whom calls can be made. The server system is also responsible for initiating the provisioning process for the first-time activation.

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

The Dencrypt Message application is pushed to the smartphone by a Mobile-Device-Management (MDM) system. The Dencrypt Server System is managed by the system administrator.

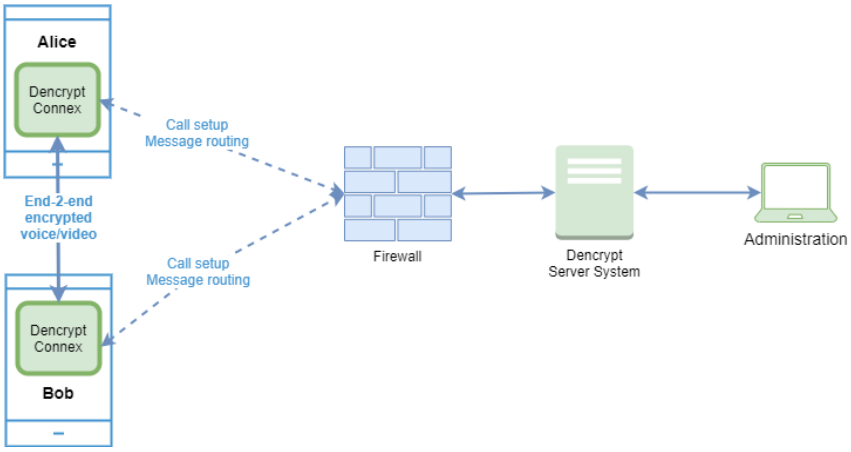


Figure 1: Dencrypt Communication Solution.

2.1 End-2-end encrypted instant messaging

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 2.

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

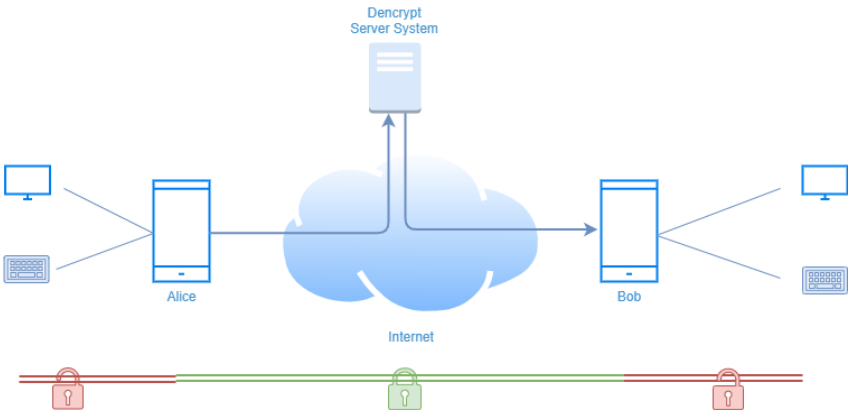


Figure 2: Area of protection for instant messaging

2.2 Authenticated connections

All communication between the Dencrypt Message 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 activation.

2.3 Encryption keys

All encryption keys for both voice/video calls and 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 the app is closed or put in the background.

2.4 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 system administrator generates the phonebooks, and any updates are pushed automatically 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 concept supports two-way and one-way conversations. Hence, it is possible to receive calls from a person not in the phonebook and without being able to call back.

2.5 Push notifications

Push notification services from Google alerts of incoming secure calls and messages. The push messages content is either empty or encrypted. Content data is never displayed on a locked screen.

3 Security instructions

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

3.1 General security measures

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

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

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 Message shall only be received from the Apple Appstores. Either as a direct installation from the public Apple Appstore or from the Apple Volume Purchase Program 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 that there are no critical side-effects. Therefore, the Dencrypt Message 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 specific users or make the entire system unavailable until the issue has been resolved.

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

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

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

Lost or stolen devices shall immediately be reported to your system administrator or to Dencrypt support (+45 7211 7911).

3.2 Avoid screen exposure

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

3.3 Other security recommendations

- **Don't take screenshots** – Screenshots are saved unencrypted on the devices and are not deleted when the app is closed.
- **Don't use copy/paste** – Don't use the copy/paste functionality during messaging.
- **Avoid auto-correction and predictive text features** - Avoid using keyboards, which includes autocorrection or predictive text features. It is recommended to disable spell checking and predictive text from the settings menu.

4 Getting started

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

1. Installation
2. Activation
3. Set permissions

4.1 Installation

Dencrypt Message is installed to end-user devices via Google Play store or via an MDM. Once the app is installed, it is launched by tapping the Dencrypt Message icon.

4.2 Activation

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

The activation link is time-limited and can only be used once and comes in the form of a web-link (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:

- an email containing a web-link send to the device.
- an email or physical letter containing a QR-code to be scanned by the camera application [1].
- SMS is supported but is not considered a secure transmission form.

Emails shall be encrypted or transmitted using encrypted connections.

Activating the link will start the provisioning process to configure the Dencrypt Message with certificates and credentials to connect to the server system and download the phonebook. Only when the activation process has successfully completed, the Dencrypt Message 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 web-link or by scanning the QR-code using the camera application. The user may be prompted to open the link in the Dencrypt Message .

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

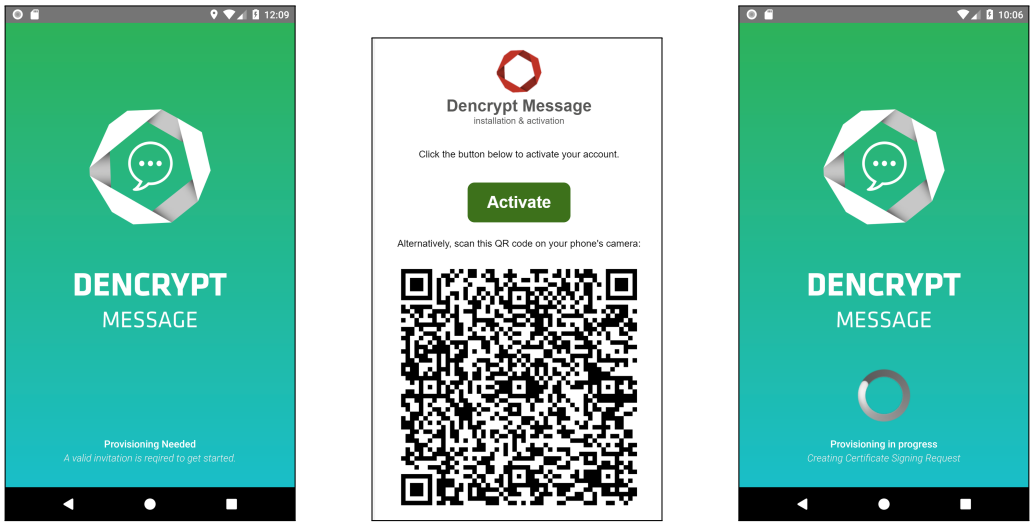
Step 4: Once completed, tap *OK* to open the app.

Step 5: The app will request permissions to device resources for full functionality. Tap *Allow* for each permission. See [Set permissions 4.3].

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

Step 7: Dencrypt Message is now ready for use.

[1] Some Android devices may not support reading QR-codes using the camera.



(a) Provisioning required. (b) Email invitation (c) Provisioning in-progress.

Figure 3: Activation.

4.3 Set permissions

Dencrypt Message requests access to some of the device resources. Permission to notifications shall be granted to perform alerts of incoming messages. Spme permissions are optional but will limit the functionality if not granted. It will still be possible to send text messages but without attachments.

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

Permission	Reason
Notifications	Required to alert for incoming calls.

(a) Mandatory permissions

Permission	Reason
Location	Required to include GPS locations in messages.
Camera	Required to capture images to attach to messages.
Images, media, files	Required to attach images and files from library.

(b) Optional permissions

Table 1: Permision usage.

5 Secure messaging

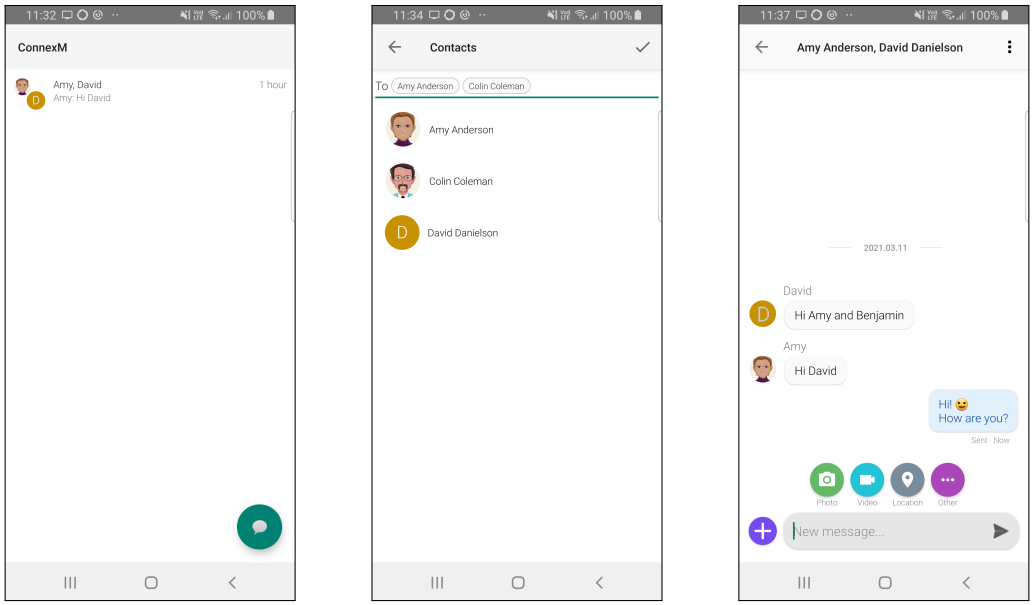
5.1 Conversations

When the app opens, the *conversation list* is shown listing the *chatrooms* for ongoing conversations. The timestamp indicates time passed since last activity.

Tap a *chatroom* to enter the conversation or create a new conversation by tapping the green 💬-button (figure 4a).

The *chatroom* displays the past message exchanges. *Chatrooms* can be both one-on-one conversation or group conversations.

Tapping the ••• in the upper-right corner, opens a menu to change the conversation title. The change is visible for all participants in the *chatroom*.



(a) Conversation list. (b) Selecting contacts (c) Group conversations

Figure 4: Conversations

5.2 Create a new conversation

Create a new conversation

Step 1: Tap a *chatroom* to enter the conversation or create a new conversation by tapping the green 💬-button

Step 2: Select particiapants form the contact list.

Step 3: Start typing the first message (section 5.3).

5.3 Sending a secure message

Send a message

Step 1: Enter a *chatroom* or start a new conversation.

Step 2: Write the message in the compose field.

Step 3: Tap ⊕ to open the options for attachments (figure 4c).

Step 4: Tap 📷 to attach photos.

Step 5: Tap 📹 to record a video clip.

Step 6: Tap 📍 to open maps and share a position.

Step 7: Tap ••• to share files.

Step 8: Tap ▸ in the compose field to send the message.

File size is limited to 30 MB.