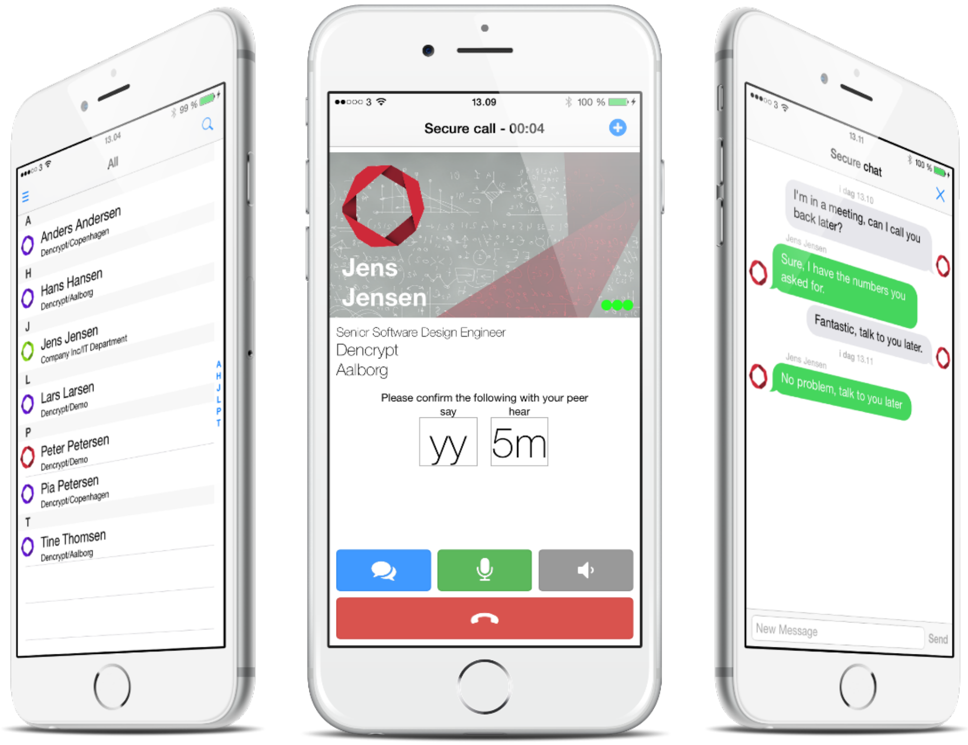
# Preparative Guide

## Dencrypt Talk v. 4.2 (iOS)



# Table of Contents

# Product version

This guide applies for:

- DencryptTalk, version 4.2.794

# 1. Introduction

This guide is intended for System Administrators of the Dencrypt Communication Solution and provide guidance on how to receive and install the Dencrypt Talk mobile client to the organization's Mobile Device Management (MDM) system in a secure way. The guide is applicable for both new installations and for updating an existing application.

The Dencrypt Talk mobile client is an iOS smartphone application, which shall be distributed to end-users through the organisation's Mobile Device Management (MDM) system. Dencrypt do not provide the MDM-system nor recommend specific models or vendors, therefore the installation guidance is informative and provide general guidance for a secure installation. For specific installation instructions, please refer to the user manual of the MDM-system.

The DencryptTalk application communicates with the Dencrypt Server System, which is installed and operated within the organization's IT environment. The Dencrypt Server System shall be working properly and operated in a physically secured environment by trained and authorized personnel only. See [1] for details.

Refer to the Operational Guide – Dencrypt Talk [2] for end-user instructions on how to securely operate the Dencrypt Talk application.

This document contains:

- Delivery procedures – guidance on how to securely receive the Dencrypt Talk application.
- Installation guidelines – informative guidance on how to install the Dencrypt Talk application.

# 2. Delivery procedures

The delivery procedures applies for both first-time installation and for maintenance and security updates. The installation file is delivered as an openPGP encrypted file and assumes that the receiver has created a private-public key pair; that Dencrypt has received the public key and verified the fingerprint  (See [3] for details on openPGP standard). The delivery procedures consist of the following steps, which are further explained below:

1. Provide an openPGP public key to Dencrypt.
2. Dencrypt will send a notification email, when new updates are available.
3. Download the SW package file and unzip to extract installation file and documentation.
4. Verify signature and decrypt the installation file.
5. Verify the version number.

**Delivery of an openPGP public key.**

The openPGP public key shall be shared in order for Dencrypt to prepare an encrypted installation file. It is assumed that a public-private key pair has been created following the openPGP standard [3]. The procedure is as follows:

1. Send an email to support@dencrypt.dk with the public key as an attachment or as plain text in the body message.
2. Dencrypt will send the Dencrypt production public key to the Customer. Ensure that fingerprint has been verified.
    a. Key-ID: DD91A365
    b. Fingerprint: F67C217A16B3ACACBF38554D0EA3CD29DD91A365
3. Dencrypt will call the Customer to verify the fingerprints of both certificates, orally.

Notice: This procedure is only needed for the first installation; if certificates have expired or if a new administrator has been assigned.

### Notification email

Dencrypt will notify the customer by email, when updates to Dencrypt Talk are available. The email will contain an URL to the destination, where the encrypted installation file can be downloaded, and the version number of the application package.

### Download and decrypt the installation file

Dencrypt provides the installation package as an openPGP signed and encrypted file *DencryptTalk_[XX]_[YY]_[ZZ].xcarchive.tgz,* where:

[XX] is the major version number
[YY] is the minor release number
[ZZ] is the build number.

The encryption ensures the integrity and completeness of the file. The file is contained in a zip-file: *DencryptTalk_[XX]_[YY]_[ZZ].zip* available for download at the Dencrypt web-page.

The *DencryptTalk_[XX]_[YY]_[ZZ]*.zip has the following content:

- The signed and encrypted SW installation package: *DencryptTalk_[XX]_[YY]_[ZZ].xcarchive.tgz.gpg*
- Dencrypt public PGP key: *dencrypt_public_DD91A365.asc*
- The preparative guide: *Dencrypt talk - Preparative guide.pdf* (This document)
- The operational user guide : *Dencrypt Talk – Operational User Guide.pdf*

Follow these steps to download, verify and decrypt the installation file:

1. Download DencryptTalk_[XX]_[YY]_[ZZ].zip from the URL address provided in the notification email and un-zip.
2. Verify and decrypt the file: DencryptTalk_[XX]_[YY]_[ZZ].xcarchive.tgz.gpg. (See instructions for your openPGP application).
3. The installation package is now available: *DencryptTalk_[XX]_[YY]_[ZZ].xcarchive.tgz*.

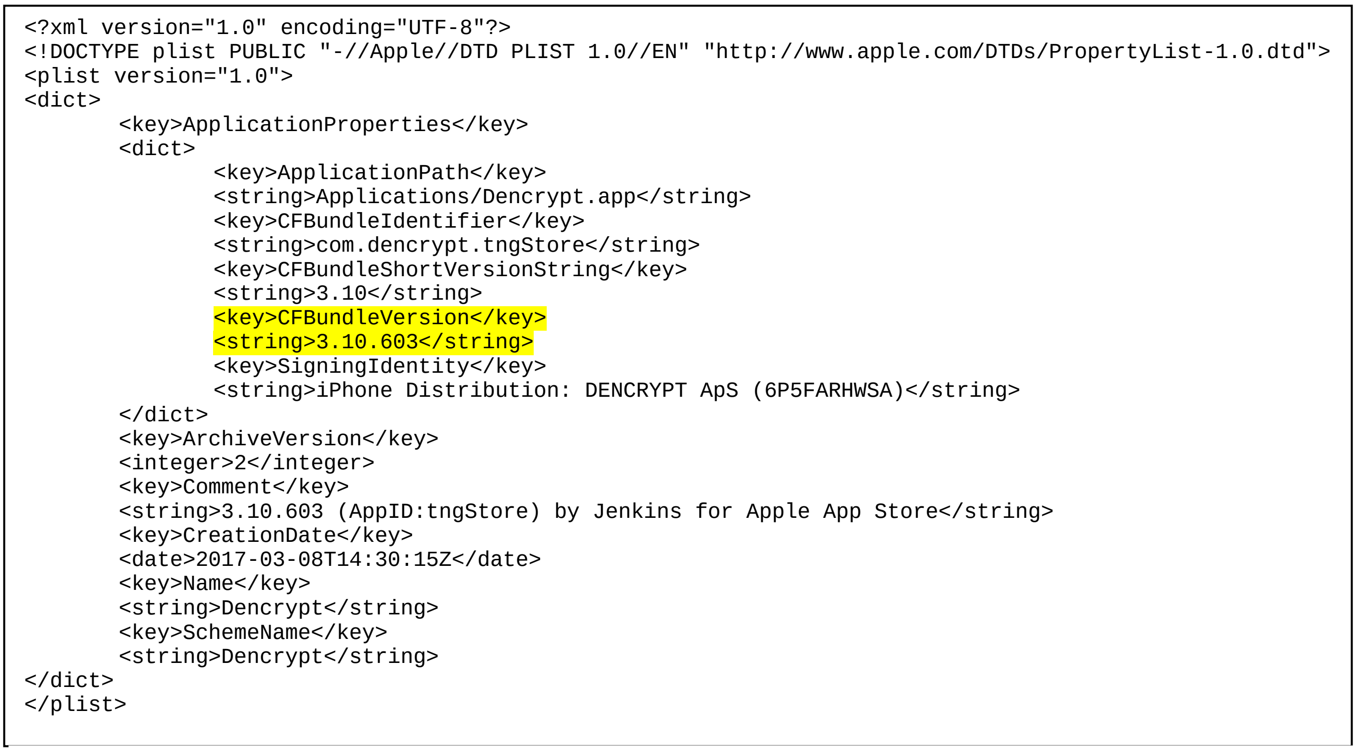
Contact Dencrypt Technical Support in case the file cannot be decrypted or if the signature validation fails.

### Verify version number

After decryption, the version number shall be verified by examing the file: *info.plist*. The MDM-system may automatically provide the version number, when installing the app. Alternatively, follow these steps:

1. Unzip and extract the .tgz file using any zip-application.
2. Locate the file: info.plist and open it in a text viewer.
3. Locate the string: *<key>CFBundleVerison<\key>* and observe the version number, which are contained in the line below between *<string> and <\string>*. In the example provided in Figure 1, the version number is: 3.10.603.

4. Compare the version in the *info.plist* file with the version  number provided in the email notification. If there is a mismatch, check if the correct file has been downloaded.  Otherwise, contact Dencrypt Technical Support.



```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
        <key>ApplicationProperties</key>
        <dict>
                <key>ApplicationPath</key>
                <string>Applications/Dencrypt.app</string>
                <key>CFBundleIdentifier</key>
                <string>com.dencrypt.tngStore</string>
                <key>CFBundleShortVersionString</key>
                <string>3.10</string>
                <key>CFBundleVersion</key>
                <string>3.10.603</string>
                <key>SigningIdentity</key>
                <string>iPhone Distribution: DENCRYPT ApS (6P5FARHWSA)</string>
        </dict>
        <key>ArchiveVersion</key>
        <integer>2</integer>
        <key>Comment</key>
        <string>3.10.603 (AppID:tngStore) by Jenkins for Apple App Store</string>
        <key>CreationDate</key>
        <date>2017-03-08T14:30:15Z</date>
        <key>Name</key>
        <string>Dencrypt</string>
        <key>SchemeName</key>
        <string>Dencrypt</string>
</dict>
</plist>
```

*Figure 1 Identification of version number from info.plist*

# 3. Installation guidelines

This sections provide guidelines for a secure installation or update of the Dencrypt Talk application to the organization's MDM-system and for distributing the application to end-users. Most modern MDM-systems have automated procedures for installing and updating an app. Hence some of the actions listed in these guidelines may be inherently performed by the MDM-system.

## 3.1 Preconditions

The following preconditions shall be observed prior to installing and taking the Dencrypt Talk application into use.

Related to the MDM-system:

- The MDM-system shall be installed in secured environment; be working properly and be operated by trusted and trained personnel only.
- The MDM-system shall be configured to accept iOS applications.
- An Apple Push Notification Service (APNS) certificate is created and installed.
- End-user devices shall be enrolled to the MDM-system in supervised mode. The devices shall be 'Company owned'.
- Each end-users device shall have an email account to which emails can be received for secure provisioning.
- Ensure that the MDM device policy requires encrypted backups.
- Ensure that the MDM system preserves the version number .

Related to the Dencrypt Server System:

- The Dencrypt Server System shall be installed and  operated in a physical secured IT-environment; be working properly and be operated by trusted and trained personnel only. Please refer to [1] for guidance on securing and configuring the IT-environment.
- The Dencrypt Server System shall be configured to deliver invitation emails for user provisioning using the organizations internal mail server, so the emails are delivered in a secure way and the link is not disclosed to any other persons than the intended user.
- The Dencrypt Server System ensures that the invitation link is available for a single attempt only. Furthermore, the Dencrypt Server shall be configured, so invitation link is active only for limited time period.

## 3.2 Preparing a customer owned application

The DencryptTalk application shall be installed and distributed as a company-owned app. The actions required to create a company owned application package are illustrated in Figure 2 and detailed in the following. The MDM-system may automate these steps; alternatively Dencrypt provides a script (resign.sh) to facilitate the process (see Appendix B).

1. The app ID shall be changed to the organization's app ID in info.plist (see Appendix A)
2. Entitlements needs to be updated using organization's app ID; keychain and team ID. (see Appendix A)
3. The organizations's provisioning profile shall be embedded.
4. The app ID is required to register the app for production Apple Push Notification Service (APNS). A private and a public key signed by Apple is created. The key pairs shall also be used by Dencrypt to configure the Dencrypt Server System. Please follow the instructions from Apple Developer Program to export and share APNS keys pairs.
5. The installation package shall be signed using the organization's private distribution certificate.

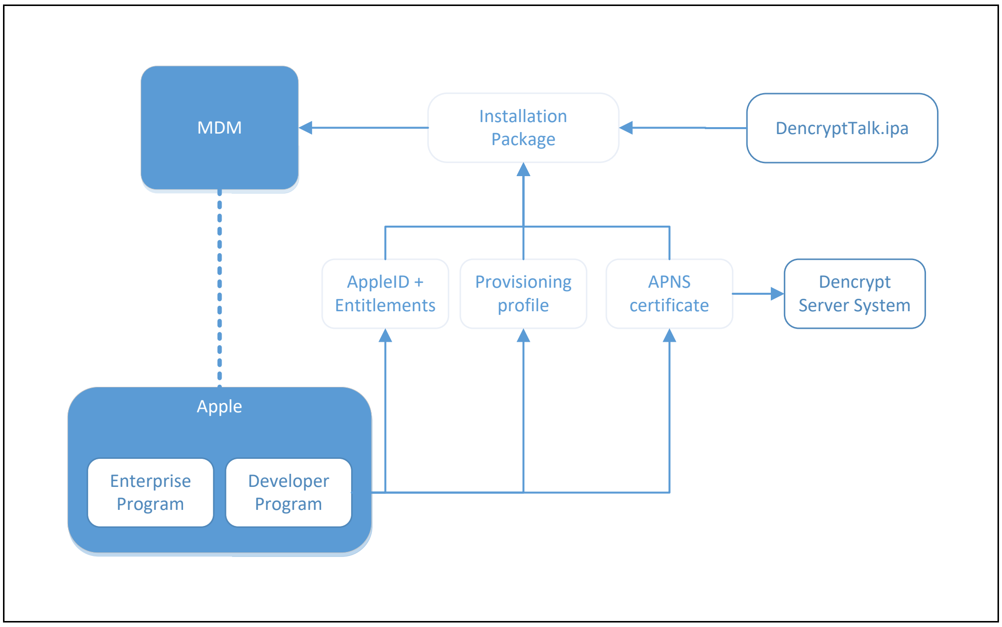


*Figure 2 Procedure for adding Dencrypt Talk application to the organization's MDM.*

## 3.3 Installation and deployment

Once a company-owned application has been created the following steps are required by the system administrator to install and deploy the app to end-users:

1. Add the app to the MDM-system. Please refer to MDM user manual.

2. Deployment of the app to end-users. Please refer to MDM user manual.
3. Verify that end-users have the correct app and correct version installed. This can usually be verified by examining the device details. Please refer to MDM user manual.

The same procedure applies for updating an existing application.

The end-user may be required to accept the installation on the device.

## 3.4 User provisioning

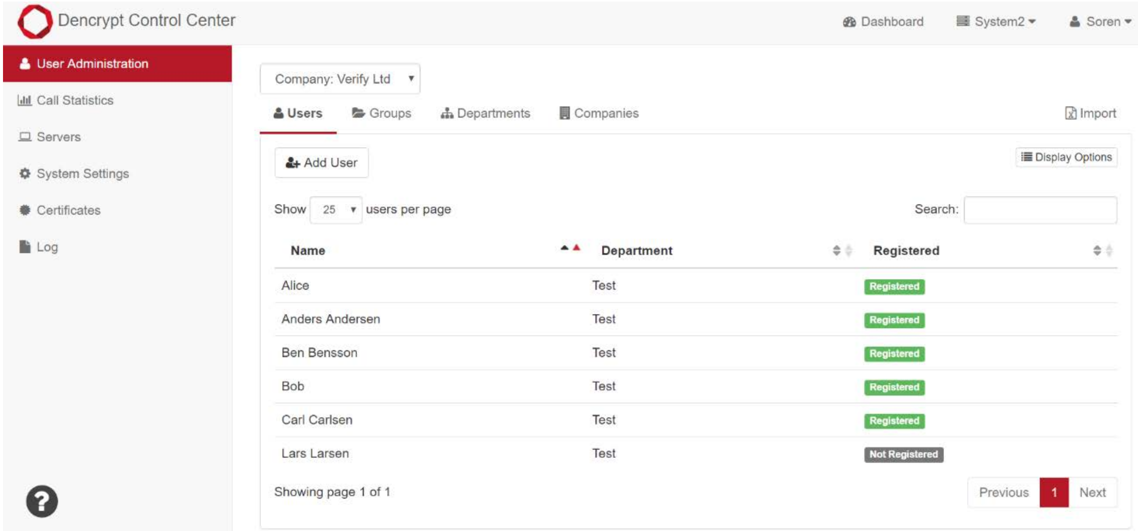
The Dencrypt Talk application is not activated before the end-user has been provisioned.

The system administrator will create the user in the Dencrypt Server System and send an invitation email with an activation link (URL). The end-user opens the email on the target device and taps the activation link, which starts the Dencrypt Talk application. The application will receive and install the configurations settings and phonebook. This may take a couple of minutes. Once completed the application is ready for use.

Notice:
**The invitation email shall be delivered in a secure way using an encrypted email connection through a mail server controlled by the organisation. If the invitation link is delivered in any other way, do not activate the link and contact your system administrator.**

The web-link can only be used once and will expire after limited time period. If this happens, the end-user will receive an "Invite error"-message and asked to contact the system administrator. In this case, the system administrator shall perform the following actions to verify that the end-user is not already registered on the server (see Figure 4):

1. Login to the Dencrypt Control Center and select "User Administration".
2. Identify the end-user and verify the registration status in the "Registration" column. If the "Registration" column is not shown: Press "Display options" and select "Registration"
3. If registration status is "Registered", a potential attacker may have used the invitation to register itself to the system. **Delete the account immediately!**
4. If the registration status is "Not Registrered" an error may have happen during the provisioning process. You may provide the user with a new invitation email.



| Name | Department | Registered |
|---|---|---|
| Alice | Test | Registered |
| Anders Andersen | Test | Registered |
| Ben Bensson | Test | Registered |
| Bob | Test | Registered |
| Carl Carlsen | Test | Registered |
| Lars Larsen | Test | Not Registered |

Showing page 1 of 1

*Figure 3 Verification of end-user registration status.*

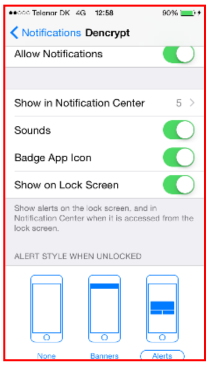
User provisioning is required for the initial installation and deployment, but is usually not required for updates.

## 3.1 Permissions and notifications

At the first launch of the Dencrypt Talk application, the user must accept access to the microphone and notifications.

Incoming calls are alerted by a push notification. The end-user is recommended to set the alert style to “Alerts” to have both visual and audible call alerts.

On iOS devices:  Go to: `Settings/Dencrypt Talk/ Notifications`



Telenor DK 4G 12:58 90%

Notifications **Dencrypt**

Allow Notifications ●

Show in Notification Center 5 >

Sounds ●

Badge App Icon ●

Show on Lock Screen ●

Show alerts on the lock screen, and in Notification Center when it is accessed from the lock screen.

ALERT STYLE WHEN UNLOCKED

None Banners [✓ Alerts]

# 4. Dencrypt Technical Support

Dencrypt Technical can be reached on the Dencrypt Customer Support portal or  on support@dencrypt.dk or on +45 72 11 79 11 (mon-fri 8- 16).

# 5. References

[1] Dencrypt, "Dencrypt Server System - Preparatory guide and hosting requirements.," 2017.

[2] Dencrypt, " Operational User Guide - Dencrypt Talk," 2017.

[3] "openPGP," [Online]. Available: http://openPGP.org.

[4] Dencrypt, "Operational User Guide - Dencrypt Server System," Dencrypt, 2017.

# 6. Change History

| Revision | Date | Author | Comment |
|---|---|---|---|
| 1.0 | 2017-08-31 | SS | Released for version 4.2 |

# Appendix A. iOS app package

The Dencrypt Talk application package (.xcarchive) has the following content.

- *App binary* – executable file delivered by Dencrypt.
- *Bundle resources* – Pictures, sounds etc .used by the app.
- *info.plist* - Contains app metadata.
- *Entitlements* – The entitlements contain the capabilitries used by the app, i.e. push notification. It also contains team ID, key chain and Bundle ID. The key chain is an ID to identify the key used sign the app.
- *embedded.mobileprovisoning* – This is the direct copy of the mobile provisioning profile, which defines how the app shall be distributed. The profile is generated by Apple Developer Center and shall be replaced by the customers provisioning profile.
- *_CodeSignature* – The purpose of the code signature is to verify that every byte within the app file is exactly the same as when it was signed by it's creator (specified by the signing identity).

# Appendix B. Script: resign.sh

The script *resign.sh* is provided by Dencrypt to facilitate the conversion to a company owned application.

Current version: 5

SHA-256:73e5f960c8b6b21b3e326ff5d5db8388aa5a77c3a0b1cc020ab86f209475cea0 resign.sh

## Syntax

```
resign.sh
      -i        Input file
      -c        Identity ID of the distribution key in keychain.
      -p        Provisioning profile of the company owned app.
      -v        (Optional) Version Add. Concatenate existing build version string with given string.
      -d on     (Optional) Gives out debug info during execution
      -n        Name to display on devices.
      -j on     (Optional) Enable if script is used for Jenkins only!
      -o        Output file (*.ipa)
```

## Prerequisites

- MacOS laptop
- Apple Xcode installed
- Distribution key in keychain
- App ID with Push notification for company-owned Dencrypt Talk. Created from Apple Developer Center.
- Provisioning profile for the app ID for company-owned app.

## Usage

1. Create a folder where *resign.sh* is stored.
2. Copy *DencryptTalk_v[XX]_[YY]_[ZZ].xcarchive.tgz* into the same folder
3. Copy the provisioning profile for the company owned app into the same folder.
4. Locate the *codesign* identity of the distribution key. Execute: `security find-identity`

   Example output:

   ```
   Policy: X.509 Basic
   Matching identities
   149690279A5EAD9AC872F653A22E91AAD1DB2FA8 "iPhone Distribution: DENCRYPT"
   ```
5. Move to the folder creted in 1) and execute *resign.sh*. Example:

   ```
   ./resign.sh -c 149690279A5EAD9AC872F653A22E91AAD1DB2FA8 -p myDencrypt.mobileprovision -n
   DencryptTalk -v .myMDM -i DencryptTalk_3_10_603.xcarchive.tgz  -o
   DencryptTalk_3_10_603_myMDM.xcarchive.tgz
   ```