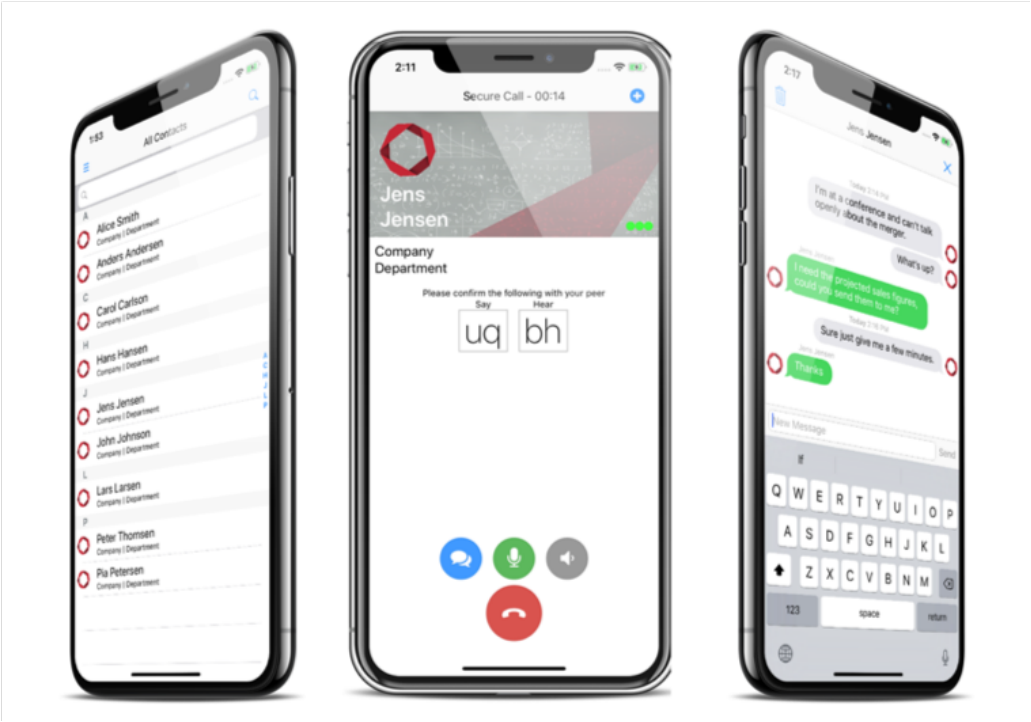
DENCRYPT

Dencrypt Talk

Version: 4.9

Preparative Guide

for Customer's System Administrator



February 2020

Contents

1 Introduction

This guide is intended for System Administrators of the Dencrypt Communication Solution and provides guidance on how to receive and install the Dencrypt Talk mobile client to the organisation'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 is delivered by Apple as a public App Store application or as custom Business-to-business (B2B) application by Apple's Volume Purchase Program (VPP). For the latter, the organisation deploys the Dencrypt Talk application as a member of Apple's VPP in the organisation's Mobile Device Management (MDM) system and distributes Dencrypt Talk to the end-users through the MDM. Dencrypt does not provide the MDM-system nor recommend specific models or vendors. Therefore, the installation guidance is informative and provides general guidance for a secure installation. For specific installation instructions, please refer to the user manual of the MDM-system.

The Dencrypt Talk application communicates with the Dencrypt Server System, which is installed and operated within the organisation's IT environment. The Dencrypt Server System shall be working properly and operated in a physically secured environment by trained and authorised 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:

- Prerequisites to receive and deploy the Dencrypt Talk application.
- Information about the publishment process from Dencrypt to the organisation
- Installation guidelines – informative guidance on how to install the Dencrypt Talk application.

2 Prerequisites

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 a secured environment; be working properly and be operated by trusted and trained personnel only.
- The MDM-system shall be configured to accept iOS applications.
- End-user devices shall be enrolled to the MDM-system in supervised mode. The devices shall be 'Company owned'.
  > Note, Apple offers the service Device Enrolment Program (DEP) to automatize device enrolment during first power-on of an iOS device. Please contact your iOS device reseller for details about DEP.
- Each end-user 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 a limited time period.
- Dencrypt Talk VPP application is associated with a specific Apple VoIP Push certificate which is needed for incoming calls. Dencrypt installs the required Apple VoIP Push certificate on the Dencrypt Server System.

2.1 Deployment of Dencrypt Talk as custom B2B application

If any customisation of Dencrypt Talk is requested, the following actions are required to get a custom B2B Dencrypt Talk application through Apple's VPP:

1. Enrol as member of Apple's Volume Purchase Program.
2. Provide the VPP enrolled Apple-ID to Dencrypt.
3. Optional: Provide Dencrypt with information for possible customisation of Dencrypt Talk.
4. Deploy an MDM system where the VPP enrolled Apple ID is used to sign into the B2B App Store.

The following sections describe the prerequisites in more detail.

Enrolment to Apple's Volume Purchase Program

The Volume Purchase Program by Apple offers corporate customers to automate device deployment, purchase and distribute content. The organisation has to sign-up to this Apple program which is independent from Apple Developer and Enterprise programs. More information about VPP enrolment is provided by Apple, e.g. `https://developer.apple.com/programs/volume/b2b/`

Provide VPP enrolled Apple ID

When Dencrypt distributes the Dencrypt Talk application through VPP, a VPP enrolled Apple-ID specifies the receiver of the custom B2B application.

Note, it is possible to share a B2B application between several organisations by relating multiple Apple IDs to the same application.

Optional: Provide information for customisation

Since the VPP distributed application is customer specific, Dencrypt Talk may be tailored to the organisation by customizing icon, app name or skin. This requires an agreement with Dencrypt to define the customisation of Dencrypt Talk. Dencrypt suggests that a different app name than "Dencrypt Talk" shall be displayed to distinguish from the public App Store version.

Deploy an MDM System with VPP Apple ID

The MDM system shall be associated with the VPP membership. Thus, the MDM system shall sign into Apple services with the VPP enrolled Apple ID.

2.2 Deployment of Dencrypt Talk as a public application

If the organisation does not require customisation of Dencrypt Talk and trusts the Dencrypt root certificate for connections between Dencrypt Talk and the Dencrypt Server System, the public Dencrypt Talk application found in the public App Store can be deployed directly by the organisation's MDM system.

3 Publishment Process

3.1 Publishing a custom B2B Dencrypt Talk application

The publishing process consists of the following steps which are specified in detail later:

1. Dencrypt releases a custom B2B version of Dencrypt Talk for the organisation.
2. Dencrypt uploads the Dencrypt Talk VPP version to Apple for review
3. Once the Apple review has been passed, the Dencrypt Talk VPP version is visible in the organisation's VPP account.

Release of Dencrypt Talk VPP Application

Dencrypt has to release a specific Dencrypt Talk bundle which is sent to Apple for VPP distribution. This specific bundle is identified by a unique and Apple specific "*AppID"*. From Apple point of view, this identifies a unique iOS application which is completely independently from any other application. However, Dencrypt's release process ensures that the delivered application, is Common Criteria compliant and includes the agreed customisations.

Upload Dencrypt Talk VPP Application

Dencrypt uploads the released Dencrypt Talk VPP bundle to Apple for a VPP application review. Dencrypt associates the uploaded Dencrypt Talk application with the VPP Apple ID of the organisation. Note, the application review is independent from the associated Apple IDs.

Once a Dencrypt Talk VPP has been reviewed and approved, additional Apple IDs may be associated by Dencrypt.

Publishment of Dencrypt Talk Application

Once the Dencrypt Talk VPP application has passed the Apple review, the application is published to all associated VPP Apple IDs.

The organisation can view the Dencrypt Talk VPP item by signing into Apple VPP's portal `https://vpp.itunes.apple.com/`

The application is also visible through the organisation's MDM. Please refer to MDM user manual.

The organisation is informed by Apple, through the MDM system, of new versions. Please refer to MDM user manual.

3.2 Publishing a public Dencrypt Talk application

The public Dencrypt Talk application is published similarly to the custom B2B Dencrypt Talk application, but the availability is not limited to specific Apple-IDs but to all Apple IDs.

Dencrypt regularly publishes Dencrypt Talk release on the App Store. A new Dencrypt Talk App Store release is aligned with a new custom B2B Dencrypt Talk release. Additional B2B releases is required for customized apps.

4 Installation guidelines

These 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.

4.1 Installation and deployment

Once the Dencrypt Talk VPP application is published by Apple, 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.

4.2 Customer Provided Root Certificate

The customer might require the Dencrypt Server System to deploy another root certificate than the Dencrypt root certificate. Dencrypt Talk's root certificate storage contains per default only the Dencrypt's root certificate. However, the MDM that manages the mobile devices, can push a new set of root certificate(s). The MDM distributed root certificate(s) replace the DCA's installed root certificate in the current point of time. There is no need for a customised version due to the different set of root certificate(s), i.e. the standard Apple Store version of Dencrypt Talk can be distributed by the MDM to implement customer specific root certificate(s).

> Note: The provisioning process deploys iOS native browser which does not use Dencrypt Talk root certificate storage. However, an MDM offers the feature to add customer specific root certificates to the iOS root certificates, too.

4.3 User provisioning

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

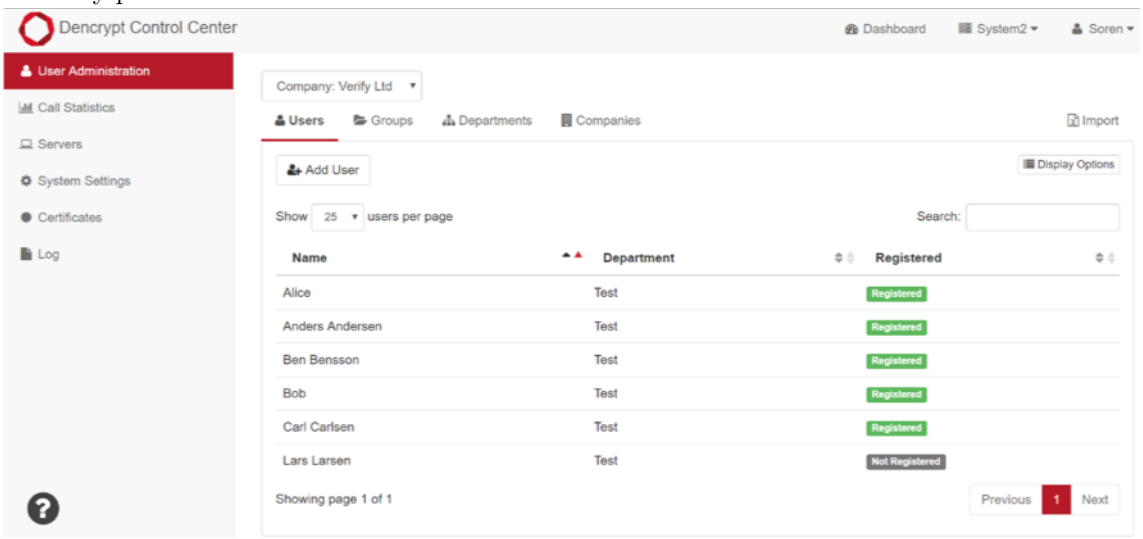
The system administrator will create the user in the Dencrypt Server System and send an invitation email with an activation link (URL). The end-user opens the email on the target device and taps the activation link to start the provisioning of the target device. The application will receive and install 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]{.underline} 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 activation-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 1):

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. **Revoke the account immediately!**
4. If the registration status is "Not Registrered" an error may have happened during the provisioning process. You may provide the user with a new invitation email.



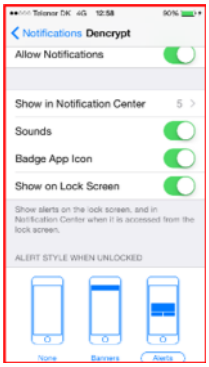
User provisioning is required for the initial installation and deployment but is usually not required for updates.

4.4 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*



5 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).

6 References

[1] Dencrypt, "Dencrypt Server System - Preparatory guide and hosting requirements"
[2] Dencrypt, " Operational User Guide - Dencrypt Talk"
[3] Dencrypt, "Operational User Guide - Dencrypt Server System"

7 Change History

Revision	Date	Author	Comment
1.0	2017-08-31	SS	Released for version 4.2
1.1	2017-12-07	FDP	Change Dencrypt Talk version number
2.0	2018-08-16	JC	Dencrypt Talk distribution only through VPP as public App Store or custom B2B application
2.1	2018-08-20	SS	Clarifications and use term *public* instead of *standard* for App Store application
2.2	2018-11-14	FWH, JC	Talk version 4.6
2.3	2019-10-02	JC	Talk version. 4.7
2.4	2019-10-09	JC	Convert to Markdown; Talk version. 4.8
2.5	2020-02-10	JC	MDM distributed root certificate