DENCRYPT

Dencrypt Communication Solution

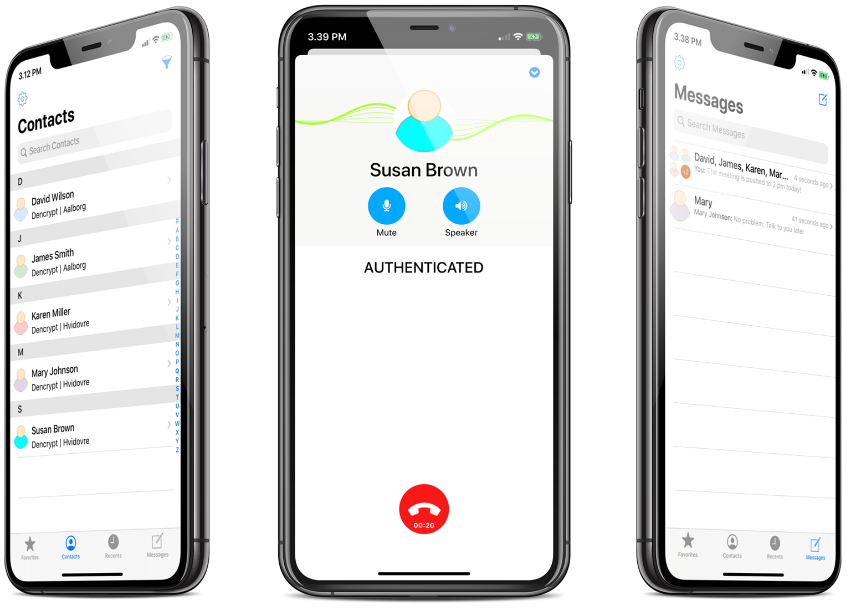
Dencrypt Connex

Dencrypt Talk

Dencrypt Message

Preparative guide

Version 2.9



28 May 2020

Public

Contents

1 Product versions:

This document is applicable for:

- Dencrypt Talk v4.9 for iOS
- Dencrypt Message v1.5 for iOS
- Dencrypt Connex v1.0 for iOS
- Dencrypt Talk v4.3 for Android
- Dencrypt Message v1.5 for Android

2 Introduction

This guide is intended for:

- End-users of Dencrypt applications received from public app stores.
- System administrators of the Dencrypt Communication Solution, which distribute the applications to end-users via Mobile Device Management (MDM) System.

This guide provides instructions on how to receive and install the Dencrypt applications in a secure way.

3 Security instructions

The Dencrypt applications connect to the Dencrypt Server System, which shall:

- be installed and operated in a physically 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.
- shall be configured to deliver activation links by email for user provisioning using the organisation´s 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.
- ensures that the activation link is one-time and only valid for a limited period.

For end-user instructions on how to securely operate the Dencrypt applications, refer to the Operational User Guide [Receiving documentation 5].

4 Deliverables

An application delivery consists of:

- Application itself, available from public app store and pushed by a MDM.

- Documentation:
  - Preparative guide: `Dencrypt_Preparative_Guide.pdf` (this document).
  - Operational User Guide: `Dencrypt_"appname"_Operational User_Guide.pdf`.

where `x.y` denotes the document version.

The documentation components are available for download from `https://www.dencrypt.dk/downloads`, which also contains links to the application on the public appstores.

5 Receiving documentation

The end-user shall be familiar with both documents and have understood the security instructions before taling the application into use.

Receive documentation

Step 1: Download from `dencrypt.dk/downloads` or receive from the system administrator

(a) `Dencrypt - Preparitive Guide.pdf`

(b) `Dencrypt "appname" - Operational User Guide.pdf`

Step 2: Verify that the document applies for the specific application type and version. This information is available from `Product Versions` section.

6 Receive applications from public app stores

First time installation

Step 1: Locate the application in the public apps store by searching the application name or use the links from `dencrypt.dk/downloads`.

Step 2: Verify that the version number in the app store matches the version number published on `dencrypt.dk/downloads`.

Step 3: Tap `Get` (iOS) or `Install` (Android) to download and install the app. Only the latest version is available.

Step 4: Complete the activation process as described in the Operational User Guide.

Once installed, the app is per default updated automatically, when a new version becomes available on the public appstores. Dencrypt will notify system administrators of any new version, which in turn will notify the end-users.

The application version can always be verified from the `Settings` menu in the application. Refer to the `Operational user guide` for details.

7 Receive applications from a B2B apptore

Applications may also by published as a custom B2B-application by Apple's *Volume Purchase Program (VPP)* [5] or *Android Enterprise* [7] for integration with a Mobile Device Management system, which in turn distributes the application to the end-users.

Dencrypt does not provide the MDM-system nor recommend specific models or vendors. Therefore, the installation guide is informative and provides general guidance for a secure installation. For specific instructions, please refer to the user manual of the MDM-system.

7.1 Prerequisites

The following preconditions regarding the MDM shall be observed before installing and taking the Dencrypt applications into use:

- The MDM-system shall be deployed 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 (and Android) applications.
- End-user devices shall be enrolled to the MDM-system in supervised mode. The devices shall be *company owned*.
  - Apple applies the Device Enrolment Program (DEP) to automatize device enrolment at first power-on of an iOS device. Please contact your iOS device reseller for details about DEP [4].
  - Android Enterprise allows both company-owned and BYOD enrolment scenarios, where both requires a work profile on a managed Google Play app store[7], [8].
- Each end-user device shall have an email account to which emails can be sent for secure provisioning[1]. Alternatively, provisioning may be performed using QR-codes .
- Ensure that the MDM device policy requires encrypted backups.
- Ensure that the MDM system preserves the version number.

7.2 Receiving a B2B applications from Apple VPP

The following actions are required to get a custom B2B Dencrypt applications through Apple's Volume Purchase Program (VPP).

Receive an application from Apple VPP

Step 1: Enrol as a member of Apple's Volume Purchase Program [5]

Step 2: Provide the VPP enrolled Apple-ID to Dencrypt.

Step 3: Provide Dencrypt with information for possible customizations of Dencrypt Talk (optional).

Step 4: Deploy an MDM system where the VPP enrolled Apple ID is used to sign into the B2B App Store.

The following sections describes the steps in more detail.

[1] Android devices require that a browser app is installed to open the provisioning link

- **Enrolment to Apple's Volume Purchase Program.**
  The Volume Purchase Program by Apple [5,] offers corporate customers to automate device deployment, purchase, and distribute content. The Customer organisation must sign-up for the Apple Volume Purchase program. Please refer to [6] for more information about VPP enrolment.
- **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. It is possible to share a B2B application between several organisations by relating multiple Apple IDs to the same application.
- **Provide information for customization (optional).**
  Since the VPP distributed application is customer-specific, Dencrypt applications may be tailored to the organisation by customizing icon, app name or skin.
- **Deploy an MDM System with VPP Apple ID.**
  The MDM system shall be associated with the VPP membership account. Thus, the MDM system shall sign into Apple services with the VPP enrolled Apple ID.

7.2.1 Dencrypt publishing process to Apple VPP

The section is information only and described process, which Dencrypt applies to publish an B2B-application on the Apple VPP store.

Publishing a custom B2B Dencrypt application

Step 1: Dencrypt releases a B2B version of a Dencrypt application.

Step 2: Dencrypt uploads the Dencrypt applications VPP version for Apple review.

Step 3: Once the Apple review has been successful, the Dencrypt application VPP version is available in the VPP account.

Step 4: Dencrypt will notify the Customer by email including the application name and version.

- **Release of Dencrypt VPP applications.**
  Dencrypt will release a specific Dencrypt application bundle which is sent to Apple for VPP distribution. This bundle is identified by an unique, and Apple-specific, *"AppID"*. From an Apple point of view, this identifies a unique iOS application which is independent from any other applications. However, the Dencrypt release process ensures that the delivered application, is Common Criteria compliant and includes any agreed customisations.
- **Upload of Dencrypt application to VPP.**
  Dencrypt uploads the released Dencrypt application VPP bundle to Apple for a VPP application review. Dencrypt associates the uploaded Dencrypt application with the Customer's VPP Apple ID. Once a Dencrypt VPP application has been reviewed and approved, additional Apple IDs may be associated by Dencrypt.
- **Publishment of Dencrypt applications.**
  Once the Dencrypt VPP application has passed the Apple review, the application is published to all associated VPP Apple IDs. The Customer can view the Dencrypt VPP application item by signing into Apple VPP's portal `https://vpp.itunes.apple.com`. The application is also becomes visible in the MDM.

The Customer is informed by Apple, through the MDM system, of new versions.

7.3 Receiving a B2B applications from Android Enterprise

The following actions are required to get a Android B2B Dencrypt applications through managed Google Play.

Receive an application from Android Enterprise

Step 1: Enrol for a managed Google Play account for the organisation [7]

Step 2: Provide the *Organisation ID* to Dencrypt.

Step 3: Provide Dencrypt with information for possible customizations of the Dencrypt application (optional).

Step 4: Deploy an MDM system where the managed Google Play account is used to sign into the B2B app store.

8 Installation guidelines

These sections provide guidelines for a secure installation or update of the Dencrypt applications 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.

8.1 Installation and deployment - iOS

Once the Dencrypt VPP applications are published by Apple, the following steps are required by the system administrator to install and deploy the app to end-users (please refer to the MDM manual for details):

Install and deploy iOS applications

Step 1: Add the app to the MDM-system. Only the latest version of the app is available.

Step 2: Verify the application name and version against the Dencrypt email notification.

Step 3: Push the app to end-users. It is recommended to enable automatic updates to ensure that end-users always have the latest app version.

Step 4: Verify that end-users have the correct application version installed. This can usually be verified by examining the device details from the MDM.

Step 5: Repeat 2-4 for updating an existing application.

8.1.1 Customer root certificate

By default, a Dencrypt application applies only a Dencrypt root certificate. In case, the Dencrypt Server System applies a Customer provided root certificate, the MDM shall push a new set of root certificates to the applications.

The MDM distributed root certificate(s) replace the application pre-installed Dencrypt root certificate.

8.2 Installation and deployment - Android

Once the Dencrypt applications are published by Google, the following steps are required by the system administrator to install and deploy the app to end-users (please refer to the MDM manual for details):

Install and deploy - Android applications

Step 1: Add the app to the MDM-system. Only the latest version of the app is available.

Step 2: Verify the application name and version against the Dencrypt email notification.

Step 3: Push the app to end-users. It is recommended to enable automatic updates to ensure that end-users always have the latest app version.

Step 4: Verify that end-users have the correct application version installed. This can usually be verified by examining the device details from the MDM.

Step 5: Repeat 2-4 for updating an existing application.

8.2.1 Customer root certificate

Customer Provided Root Certificates are currently not supported by Dencrypt's Android applications.

9 Provisioning

The Dencrypt applications are not activated before the end-user has completed the provision process.

The system administrator will create the user in the Dencrypt Server System and send an invitation email with an activation link (URL or QR-code). 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 configuration settings and phonebook. This may take a couple of minutes. Once completed, the application is ready for use. The activation-link can be used only once and will expire after a time period.

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

Refer to the `Security Instructions` in the `Dencrypt Server System - Operational User Guide` for secure enrollment of end-users.

10 Dencrypt Technical Support

Dencrypt technical support can be reached on:

- **Dencrypt Support portal:** https://servicedesk.dencrypt.dk/servicedesk/customer/portal/1
- **Email:** support@dencrypt.dk
- **Phone:** +45 7211 7911

References

[1] Dencrypt, *Dencrypt Server System - Preparatory guide and hosting requirements*, Version 4.2, 2019.

[2] Dencrypt, *Operational User Guide - Dencrypt Talk*, Ver 4.8, 2019.

[3] Dencrypt, *Operational User Guide - Dencrypt Server System*, Ver. 4.2, 2019.

[4] Apple, *Apple Deployment Programs. Device Enrollment Program Guide*, https://www.apple.com/business/docs/site/DEP_Guide.pdf.

[5] Apple,*Apple Deployment Programs. Volume Purchase Program Guide*,https://www.apple.com/business/docs/site/VPP_Business_Guide.pdf.

[6] Apple, *Distributing Custom Apps for Business*,https://developer.apple.com/business/custom-apps/.

[7] Google, *Android Enterprise*, https://www.android.com/intl/en_uk/enterprise/management/.

[8] Google, *Android Enterprise Overview*, https://developers.google.com/android/work/overview.

Change History

Revision	Date	Author	Description
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
2.6	2020-03-17	SS	Converted to Latex. Made general for Talk and Message.
2.7	2020-03-23	SS	Updated for Android
2.8	2020-05-15	SS	Updated for DT iOS 4.9
2.9	2020-05-28	SS	Updated for Connex. Aligned with delivery guide