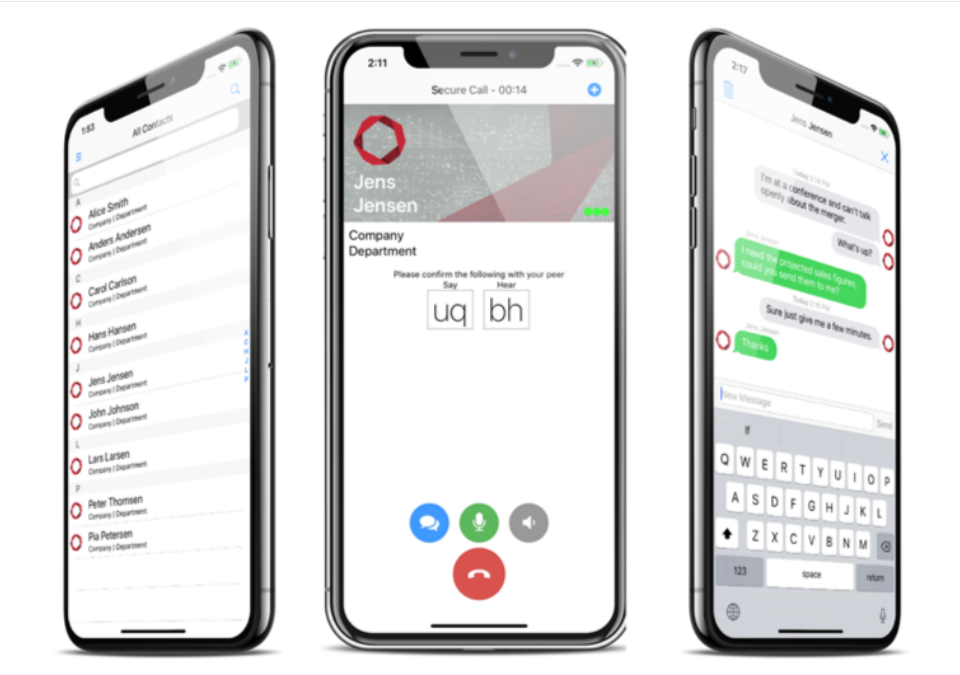
Dencrypt Communication Solution

Dencrypt Connex
Dencrypt Talk
Dencrypt Message

Preparative guide

Version 2.13



18 February 2021

Public

Contents

1 Product versions

This document is applicable for:

- Dencrypt Connex v. 6.0 for iOS
- 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 or received via an MDM. It provides instructions on how to receive and install Dencrypt Connex 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 either:
  - 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, or
  - support MDM-assisted provisioning (section 9.1), where only apps with a pre-installed certificate can connect to the Dencrypt Server System. In this case, activation links can be provided over insecure connections, such as email or SMS.
- 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

- Application itself, available from public app store or pushed by an MDM.
- Documentation:
  - Preparative guide: Dencrypt_Connex_Preparative_Guide_xx_yy.pdf (this document).

- Operational User Guide: Dencrypt_Connex_Operational_User_Guide_xx_yy.pdf.

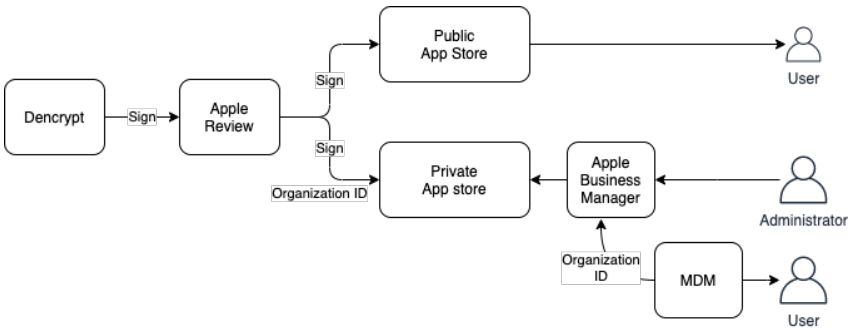


Figure 1: Distribution options.

The Private App store is accessed by the Custom App catalogue of the Apple Business Manager (ABM). The ABM replaces the Apple Volume Purchase Program (VPP).

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 taking the application into use.

Receive documentation

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

(a) Dencrypt_Connex_Preparative_Guide_xx_yy.pdf (this document)

(b) Dencrypt_Connex_Operational_User_Guide_xx_yy.pdf

Step 2: Verify that the documentaion applies for the intended application, platform 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 app 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: For iOS: Tap `Get` to download and install the app.

Step 4: For Android: Tap `Get` (iOS) or `Install` (Android) to download and install the app. Only the latest version is available.

Step 5: 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 appstore

Applications may also by published as a custom application by Apple Business Manager [5] or Android Enterprise [7] for integration with a Mobile Device Management system, which in turn distributes the application to the end-users.

8 Link a Dencrypt application to an MDM

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.

This section is intended for system administrators distributing Dencrypt applications via an MDM.

8.1 Prerequisites

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

- The MDM-system shall be 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 Bussines Manager allows to automatize device enrolment at first power-on of an iOS device. Please contact your iOS device reseller for details about device assignment which replaces Device Enrollment Deployment (DEP) [5].
  - 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].
- For provisioning, each end-user device shall have an email account to which emails can be sent securely.
- Depending on local security policy:
  - Provisioning may also be performed using QR-codes.
  - Provisioning may also be performed using SMS.
  - MDM-assisted provisioning (section 9.1) may be deployed to provision over non-secure email or SMS.
- Ensure that the MDM device policy requires encrypted backups.
- Ensure that the MDM system preserves the version number.

8.2 Receiving a custom application from Apple Business Manager

The following actions are required to get a custom Dencrypt application through the Apple Business Manager.

Receive an application from Apple Business Manager

Step 1: Enrol for the Apple Business Manager [5]

Step 2: Provide the Organization ID of the Apple Business Manager to Dencrypt.

Step 3: Deploy an MDM system which accesses the Custom App catalogue of the Apple Business Manager.

The following sections describes the steps in more detail.

- **Enrolment to Apple Business Manager**
  Apple Business Manager [5] offers corporate customers to automate device deployment, purchase, and distribute content. The Customer organisation must sign-up for the Apple Business Manager. Please refer to [6] for more information about Apple Business Manager enrolment.
- **Provide Apple Business Manager Organization ID.**
  When Dencrypt distributes the custom application through Apple, the customer's Apple Business Manager Organization ID specifies the receiver of the custom application. It is possible to share a custom application between several organisations by relating multiple Organization IDs to the same custom application. An application cannot be published on both on the public Appstore and the Custom App catalogue in the Apple Business Manager.
- **Deploy an MDM System with Apple Business Manager.**
  The MDM system shall be associated with the Apple Business Manager account by downloading an Apple Business Manager token which needs to be imported to the MDM.

8.3 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.

8.4 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.

8.4.1 Installation and deployment - iOS

Once the Dencrypt custom 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.

8.4.2 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.

The root certificates are pushed by the MDM when deploying Managed Configuration of the MDM controlled application. MDM vendors may require a configuration file in XML format or generates it based on given key-value pairs. The technical Dencrypt contact assists your organisation to format and wrap the organisation's root certificates accordingly.

8.5 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.

8.5.1 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 or SMS 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.

9.1 MDM-assisted provisioning

Provisioning requires a secure distribution of the activation link, e.g. the invitation mail is received by secure mail on the device. To comfort the initial setup of the Dencrypt applications, the provisioning connection is secured by a provisioning client certificate distributed by the MDM. Once the iOS device is enrolled to the MDM, and the MDM is configured to push the provisioning client certificate [4], the activation link can be distributed on unsecure channels such as SMS.

The provisioning client certificate and key pair are pushed by the MDM when deploying Managed Configuration of the MDM controlled application. MDM vendors may require a configuration file in XML format or generates it based on given key-value pairs. The technical Dencrypt contact assists your organisation to format and wrap the provisioning client certificate and key pair accordingly.

MDM-assisted provisioning is currently supported by Connex iOS only.

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

[2] Dencrypt, Operational User Guide - Dencrypt Talk

[3] Dencrypt, Operational User Guide - Dencrypt Server System

[4] Dencrypt, MDM-assisted provisioning

[5] Apple,Getting Started Guide Apple Business Manager,https://www.apple.com/business/docs/site/Apple_Business_Manager_Getting_Started_Guide.pdf.

[6] Apple, Distributing Custom Apps,https://developer.apple.com/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
2.10	2020-06-30	SS	Updated based on atsec comments
2.11	2020-07-08	SS	Updated based on atsec comments
2.12	2020-10-14	JC	Updated for CC release of Connex 6.0
2.13	2021-02-18	JC	ABM replaces VPP and DEP and MDM-assisted provsioning