DENCRYPT

Dencrypt Communication Solution RESTRICTED

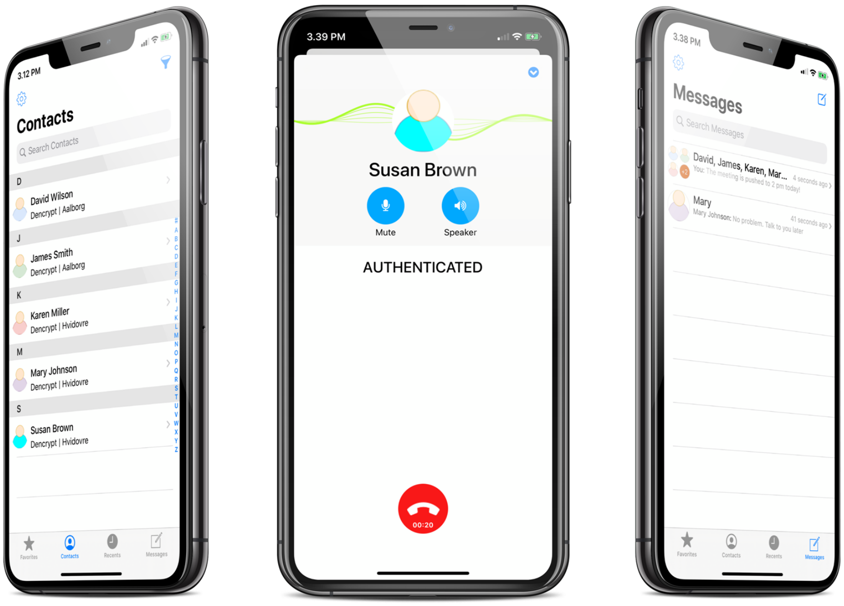
Dencrypt Support 24/7: +45 7211 7911

Dencrypt ConnexR

Security Instructions

End-users

Version 1.0



January 2021

Company Restricted

Contents

1 Introduction

This document contains the security instructions and guidance for systems administrators of Dencrypt Communication Solution RESTRICTED (DCS-R). The instructions concerns:

- Accepted use and handling of Dencrypt ConnexR .
- Incident response handling and reporting

The security instructions shall be read and understood before operating the system.

The following role definitons are used throughout the document:

End-user Users of Dencrypt ConnexR for exchange of classified information.

User admin Manages end-user and call groups within allocated companies.

System admin Dencrypt technical personnel, which performs system configuration and maintenance and enrollment of Customer organizations.

2 Security policies

These security instructions apply to end-users of the Dencrypt ConnexR application for the exchange of classified information. These security instructions shall be read and understood before taking the Dencrypt ConnexR application into use.

2.1 Classifications

The Dencrypt ConnexR may be used for the exchange of classified information up to Danish RESTRICTED.

2.2 Accepted use

End-users apply Dencrypt ConnexR for exchange of classified information and shall:

- End-users shall have a valid security clearance for at least Danish RESTRICTED or similar. Alternatively, be a person elected by the people for the Danish Parliament, Danish Regions, or Danish City Councils.
- be trustworthy, non-hostile, and be capable of following instructions.
- have received and understood the *Security Instructions for Dencrypt ConnexR* [1] (This document).
- be familiar with the *Dencrypt Connex - Operational User Guide* [2].
- only iOS-based devices enrolled to a compliant Mobile Device Management (MDM) is allowed.

2.3 Access control

Access to the communication services is provided by the User- or System Administrator. It is not possible for the end-user to add contacts or alter contact groups.

2.4 Device handling

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 ConnexR 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 certain users or make the entire system unavailable until the issue has been resolved.

Pincode and biometrics The device shall use a 6-digit pin code and biometric authentication.

Screen lock Display auto-lock shall be 1 minute or less.

Benign applications The Dencrypt ConnexR application protects information during the data transmission and when stored on the device. 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.

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

Unattended devices Devices left unattended for more than 24 hours shall be switched off.

Lost or stolen devices shall be reported to the User Administrator or Dencrypt immediately.

Repairs The Dencrypt ConnexR shall be deleted or account revoked before sending the device for repairs.

Disposal The Dencrypt ConnexR shall be deleted or account revoked before disposing of the device.

2.5 Dencrypt ConnexR - Secure usage

Some precautions must be observed to use Dencrypt ConnexR in a secure way and to avoid disclosure of confidential information. Please observe the following before taking the application into use.

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.

Avoid acoustic coupling It is not recommended to use encrypted voice or video calls in hotel rooms and like, which cannot be considered secure. Never exchange classified information through the Dencrypt ConnexR application when other unclassified telephones, radio transmitters, or similar are being used in the immediate proximity. Locations that are well suited to making calls may be public spaces, where the caller's presence has not been pre-arranged. Using secure messaging is an alternative communication in areas, where acoustic coupling is a possibility.

Avoid screen exposure Consider the surroundings when using Dencrypt ConnexR for secure video calls and messaging to ensure that the screen can not be observed by others. Be aware of the location of windows and cameras.

Do not use wireless headsets The data connection from the device to the headset is not encrypted. Use wired headsets as an alternative.

Do not use handsfree car systems The data connection from the device to the handsfree car system is not encrypted. Disable Bluetooth to avoid automatic connection and use wired headsets as an alternative.

Avoid using loudspeker Use the Dencrypt ConnexR loudspeaker only with care and in locations, which are protected from acoustic coupling.

Don't take screenshots Screenshots are saved unencrypted on the devices and are not deleted when the app is closed. The Dencrypt ConnexR will show a warning when screenshots are taken.

Don't use copy/paste The copy/paste functionality is disabled for Dencrypt ConnexR .

Don't use 3rd party voice recordings 3rd party voice recordings are saved unencrypted on the devices and are not deleted when the app is closed.

Disable 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.

Avoid using apps with speech recognization Avoid using applications, which makes use of speech recognition features, such as speech-to-text applications.

3 Incident response handling

Security incidents and risk shall always be reported to::

- Own User Administrator, or alternatively:
- Contact Dencrypt Support: +45 7211 7911 or support@dencrypt.dk.

- Lost or stolen devices shall be reported immediately.
- Dencrypt ConnexR shall be deleted from the device before repairs or disposal.

References

[1] Dencrypt. *Dencrypt ConnexR - Security Instructions. End-users*. Available from Dencrypt upon request.

[2] Dencrypt. *Dencrypt Connex - Operational User Guide*. URL: https://www.dencrypt.dk/downloads.

Abbreviations

CFCS	Center for Cyber Security
DCS-R	Dencrypt Communication Solution RESTRICTED
MDM	Mobile Device Management

Change history

Revision	Date	Author	Description
1.0	30 January 2021	SS	Initial version for Center for Cyber Security (CFCS)