



Installation Guidance

Cryptify Call

1 Introduction

This document gives an overview guide of how to install and configure a Cryptify Call solution, covering the CRS and the CMS. It is assumed the reader is familiar with, and has access to, the CMS Manual [2] and the CRS Manual [1].

Cryptify Call provides end-to-end encrypted communication between *Cryptify Call Application* (CCA) instances. The solution is designed to ensure that the deploying organisation retains complete ownership and operational control of its cryptographic key material, enrolled identities and security configuration.

Cryptify Call consists of three principal components:

- The *Cryptify Management System (CMS)* – the cryptographic authority and root of trust. The CMS operates off-line and hence is completely isolated from internet threats.
- The *Cryptify Call Application (CCA)* – clients that offer end-to-end encrypted communication and run on mobile devices (iPhone and Android) or desktop computers (Windows).
- The *Cryptify Rendezvous Server (CRS)* – a backend server responsible for signalling, message storage and distribution, and media relay, while having no access to cryptographic keys or plaintext communication content.

Detailed installation, administration and recovery procedures are provided in the respective manuals.

1.1 Installation

A single CRS can host multiple CMS installations. Each CMS is associated with a unique account on the CRS. Follow the procedure below to install and configure a complete Cryptify Call system.

1. Install and configure the CRS
 - (a) Follow the instructions in the *Initial Installation and Configuration* chapter of the CRS Manual [1].
2. Create a CRS account for the CMS
 - (a) Follow the instructions in the *Add an Account* chapter of the CRS Manual [1].
 - (a) Record the *Account ID* and the generated *Shared Secret*. These credentials are required when configuring the CMS.
3. Install and configure the CMS
 - (a) Prepare the CMS installation
 - i. CMS information
Security Domain: Specify a text string that uniquely identifies this CMS installation. Suitable values include the legal name of the organization, or the organization name combined with the relevant department or business unit.

- ii. License information
Enter the license information provided in the license letter issued by Cryptify AB.
 - iii. CRS connection information
CRS Name: Specify the IP address or FQDN of the CRS server(s) queried by the CCA.
Account ID: Enter the *Account ID* recorded when creating the CRS account in Step 2.
Shared Secret: Enter the *Shared Secret* recorded when creating the CRS account in Step 2.
- (a) Follow the instructions in the *Installation and Configuration* chapter of the CMS Manual [2].

References

- [1] Cryptify AB. *CAB-12:047, CRS Manual*. URL: <https://cryptify.com/resources>.
- [2] Cryptify AB. *CAB-12:048, CMS Manual*. URL: <https://cryptify.com/resources>.