Installation Guide

Cryptify Call Solution

Table of Contents

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 (CAB-12:048) and the CRS Manual (CAB-12:047).

1.1 References

[1] *Manual - Cryptify Management System*
CAB-12_048, Cryptify AB

[2] *Manual - Cryptify Rendezvous Server*
CAB-12_047, Cryptify AB

2 Overview

Cryptify Call is realized by three system entities developed by Cryptify.

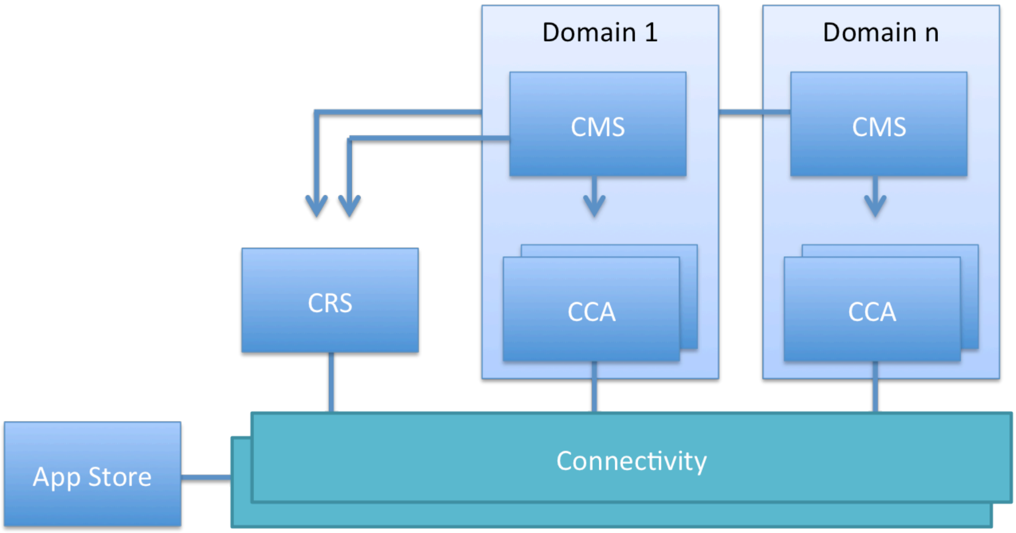

Figure 1: System entities

- **Cryptify Rendezvous Service (CRS):** A service that implements call setup signaling and relaying of monthly update material. This service does not implement any of the security functions and is merely a relay of already protected information. As such it may be deployed and operated on standard Internet servers or on a cloud-based platform. One CRS can handle multiple CMS Domains, where each CMS Domain is assigned a unique account on the CRS.
- **Cryptify Management System (CMS):** A desktop application operated by an appointed security manager that facilitates generation and distribution of crypto credentials for the end-users within a CMS domain represented as a QR code. The QR code contains settings and credentials for the current month and an update key used to protect future re-keying including credentials to access the CRS, i.e. there is no need to update the CRS when a new user is added.
- **Cryptify Call Application (CCA):** An end-user application that is installed on smartphones. This application allows secured voice and text messaging communication in the same fashion as with ordinary telephony services e.g. between ordinary participating telephone numbers. The CCA software is downloaded from the applicable market place (e.g. App Store for iOS, and Google Play

Store for Android). By using the embedded QR code scanner in the Cryptify Call app the client scan the QR code provided by the CMS.

Connectivity between clients and the CRS is typically made over publicly available cellular packet data protocol (PDP) connections or over WLAN.

3 Preparations

Please make sure the following is available:

Documents (available at cryptify.com)

- CAB-12_047-CRS_Manual-<version>.PDF
- CAB-12_048-CMS_Manual-<version>.PDF

SW

- CRS SW (crs_<version>-1_amd64.deb)
- CMS SW (cms_<version>_x86.exe)

License letter from Cryptify AB containing

- System ID
- License Key

4 Installation Procedure

Please use the following procedure to set up a complete Cryptify Call from scratch.

1. CRS Installation
    a. Please follow instructions in the “Initial Installation and Configuration” chapter in the CRS Manual
2. Create an account for each CMS Domain on the CRS
    a. Follow the instructions in “add an account” in the CRS Manual
    b. Note down the account-id and the shared secret generated for the CMS Domain.
3. CMS Installation
    a. Preparations

i. Fill in the table in the pre-requisites chapter in the CMS Manual
    1. CMS Info
       Security Domain: select an appropriate text string that represents this particular installation of the CMS, e.g. legal company name, company and unit name, etc.
    2. License Info
       As per the license letter received from Cryptify AB
    3. CRS Info
       CRS Name: this is the DNS name of the CRS server(s) that are queried by the devices.
       Account ID: As per procedure 2.a above
       Shared secret: As per procedure 2.b above

b. Please follow the instructions in the “Installation and Configuration” chapter in the CMS Manual.