Operation Guidance

Cryptify Call

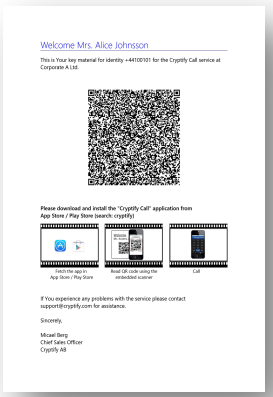
1 Introduction

This document is an overview description of the Cryptify Call solution and a set best practice recommendations how to operate the system.

Cryptify Call is a modern digital communication solution that enables secure communication both within the business and with external partners. The solution gives you as a customer complete control and ownership of everything from cryptographic keys to personal data.

The Cryptify Call app is available for free on AppStore and Google Play. Once installed, a unique QR code needs to be scanned into the app. This QR code contains this user's unique cryptographic keys.

A unique QR code is printed by the Cryptify Management System on an initialization letter along with a short instruction on how to install the app and scan in the QR code. The management system is the only place where the secret keys are stored.



Cryptify Call is broadly recognized for being easy to use and intuitive. Using it is as simple as making an ordinary phone call or sending an ordinary text message. Cryptify Call uses the existing devices, has a familiar user interface, and utilises the ordinary phone numbers. The solution works in parallel with the ordinary functions of the phone, enabling users to choose whether to make a secure or an ordinary call.

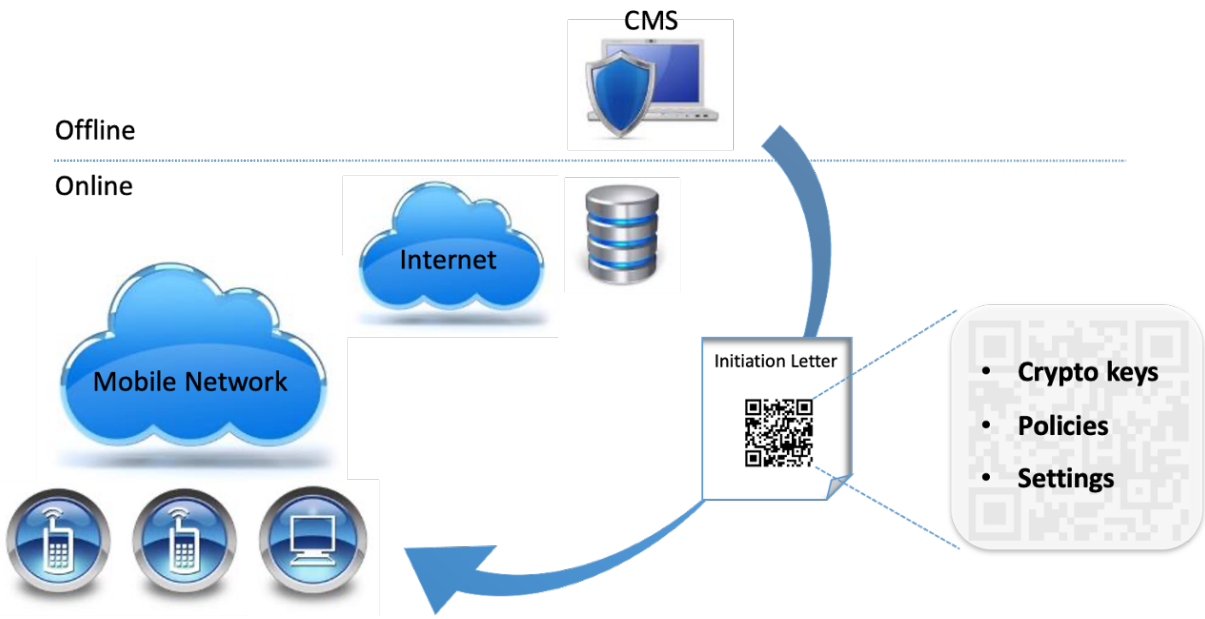
With the shift to a more and more mobile workforce the need for secure and reliable collaboration tools becomes increasingly critical, not just for communication within the own organization, but also with customers, suppliers and business partners.

Cryptify Call is developed to enable easy yet secure collaboration between individuals and groups. One example is the group messaging capability, which enables flexible, yet secure, creation of short- or long-lived communication groups. The groups can be used both for group messaging and a secure contact directory, where contact details never leave the protected Cryptify Call environment.

2 Solution

The solution consists of the app “the Cryptify Caller Application”, which is available for iPhone [3], Android [4] and Windows [5], and two central functions; the Cryptify Management System and the Cryptify Rendezvous Server.

The architecture divides the central functions in a security domain where the Cryptify Management System (CMS) [1] is handling all sensitive information, and an open domain for VoIP traffic, where no sensitive information is exposed unencrypted, handled by the Cryptify Rendezvous Server (CRS) [2].



Using encryption algorithms, users can now establish an end-to-end encrypted session with each other that both guarantees **confidentiality**, i.e. that only the intended *recipient* can decrypt the content, and **integrity**, i.e. that the *recipient* can verify the identity of the *initiator* and that contains not been tampered with or destroyed along the way.

The CMS gives the organization complete and exclusive control over all key material. As the CMS is not connected to any IP network, it is completely isolated from threats from the Internet.

3 Secure Operation

3.1 General

The following recommendations outline a configuration for Cryptify Call that is in line with the NATO RESTRICTED requirements. These requirements should be followed unless there is a strong business requirement not to do so. Such instances should be discussed with your Chief Information Officer.

Please note that CMS contains the Key Management Server (KMS), Master Secret, KMS Secret Authentication Keys and, for certain cipher suites, the private keys for all the users.

Please make sure that:

- The latest version of the Cryptify software is used (CMS, CRS, apps, ..), obtained from a reputable source and that it has not been tampered with or replaced with malicious software. To maintain system integrity all software, including updates, must be verified as originating from Cryptify AB before installation.
- The underlaying platform have applied available security patches.
- Upgrade Operating system and/or Hardware in case security updates are no longer provided.

The CMS must never be connected to any network at any time.

The CMS must never be physically accessible by unauthorized users.

Please note that while the CRS is not involved in any encryption operations, it is still vital for the availability of the service and could potentially be subject to attack where the ultimate targets are the mobile devices.

The CRS must only be managed by trusted administrators and under the control of the deployment organization, and those administrators must audit the CRS to ensure no malicious activity is taking place.

Only specific devices shall be able to connect to the CRS (and then only over specific ports) protected by a hardware firewall that only allows TLS and other required protocols.

Such devices, when provisioned, shall be configured to only connect to a specific CRS.

3.2 Pre-installation

Before installing Cryptify Call it is recommended that you take the following actions:

Configure the device in accordance with the Device Security Guidance, please see reference [7].

Make sure the pre-requisites, as described in the Cryptify Call product documentations are fulfilled, refer to the manuals for the CMS [1], CRS [2] and CCA for iPhone [3], CCA for Android [4] and CCA for Windows [5].

Please familiar yourself by reading the “Installation Guide” [6].

3.3 User device installation and configuration

It is recommended to install the Cryptify Call application as part of the provisioning process using a Mobile Device Management (MDM) solution.

Please follow the “add a single user” procedure in the CMS manual (reference [1]) to create necessary keys and configuration data for the user.

3.4 Initial key distribution

It is recommended to scan the QR code directly from the screen from the CMS computer in order to avoid printing the private keys. This is done by selecting view QR code in the user details menu.

If printed versions of the QR codes must be used (for example because the device configuration is being performed at a different location to the CMS), they must be marked with the classification of the system, transported and, as soon as they have been used, destroyed in accordance with the highest classification of the data to be carried by the system.

For further reading please read the “User Initiation Letters” section in the CMS Manual [1].

3.5 Monthly key update

The Cryptify Call system implement a monthly key-rotation scheme where credentials are aligned with calendar months, i.e. each month the users must be provisioned with new key material as previous months keys will be revoked.

Please follow the Monthly key updates procedure in the CMS manual (reference [1]), and the CRS manual (reference [2]).

A fresh blank CD-R should be used for each transfer to avoid the possibility of introducing malicious code onto the CMS.

3.6 Routine tasks

<u>Backup</u>

Please follow the Backup routine in the CMS manual (reference [1]) and the CRS Manual (reference [2])

Logs

The logs available on the CRS should be checked at least monthly before the keys for the following month are loaded to check for unexpected entries. The available logs are described in the CRS manual (reference [2]).

Service monitoring

Use best practice IT tools to monitor the CRS and its connectivity towards external services, e.g. the Cryptify Push Server (“CPS”) and Apple Push Notification Service (“APNS”).

3.7 Restore

This operation is in case a device, or a server, needs to be restored, and there is no possibility that the device or server has been compromised.

For the CMS, please follow the Restore instructions in the CMS Manual (reference [1]) to restore the CMS from a backup archive.

For the CRS, please follow the Restore instructions in the CRS Manual (reference [2]) to restore the CRS from a backup archive.

For a device, please follow the “Initial key distribution” chapter above

3.8 Compromise recovery – CMS

Please follow this operation in case the CMS is, or is suspected to be, compromised.

Please follow the “Compromise recovery – CMS” chapter in the CMS Manual [1].

3.9 Compromise recovery – User device or QR code

Follow this operation in case a device or an Initiation letter containing the QR code is, or is suspected to be, compromised.

Please follow the “Compromise recovery – User device” chapter in the CMS Manual [1].

4 References

Latest versions of the documents below published by Cryptify AB are available at https://www.cryptify.com/downloads

[1] CMS Manual, Cryptify Call, CAB-12_048, Cryptify AB
[2] CRS Manual, Cryptify Call, CAB-12_047, Cryptify AB
[3] CCA iPhone Manual, Cryptify Call, CAB-12_049, Cryptify AB
[4] CCA Android Manual, Cryptify Call, CAB-13_013, Cryptify AB
[5] CCA Windows Manual, Cryptify Call, CAB-17_011, Cryptify AB
[6] Installation Guide, Cryptify Call, CAB-13_021, Cryptify AB
[7] Device Security Guidance, https://www.ncsc.gov.uk/collection/device-security-guidance, NCSC