

Operations Guidance

Cryptify Call

Contents

1	Introduction	3
1.1	Identity Management	3
1.2	Federating with other Cryptify Call systems	4
2	Roles and Responsibilities	4
2.1	CMS Operator	4
2.2	CRS Operator	5
2.3	End User	5
3	Secure System Operation	6
3.1	CMS Protection	6
3.2	CRS Protection	6
3.3	Software and Platform Maintenance	7
4	Provisioning and Lifecycle Management	7
4.1	Initial Enrolment	7
4.2	Monthly Key Rotation	7
4.3	Device Replacement	8
5	Backup, Monitoring and Routine Operations	9
5.1	Backup	9
5.2	Monitoring	9
6	Compromise Recovery	9
6.1	CMS Compromise	9
6.2	CRS Compromise	9
6.3	Device or Initiation letter	9

1 Introduction

This document provides operational guidance for the secure deployment and operation of a Cryptify Call system.

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 Identity Management

The CMS is the central authority for End User identity and cryptographic provisioning. It establishes and maintains the authoritative association between the End User, the End User's MSISDN (the central End User identity in Cryptify Call), authorized devices, and the cryptographic credentials assigned to the End User.

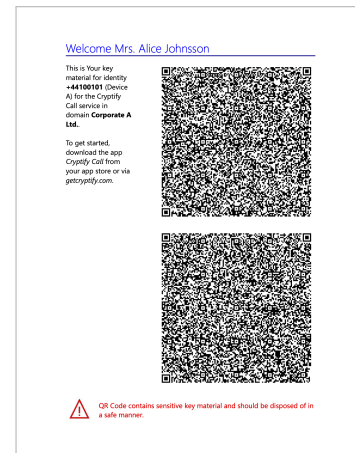
The CMS is the system authority for End User identity and cryptographic provisioning. It establishes and maintains the association between:

- the End User's MSISDN (i.e. the mobile number in international format)
- the End User's authorized devices (a End User may have up to three authorized devices associated with the same MSISDN)
- associated public keys and certificates
- the policies and cryptographic credentials assigned to the End User

Central identity attestation is a fundamental security property of Cryptify Call.

By performing this binding centrally and ensuring that the credentials are provisioned only to the End User to whom the MSISDN is assigned, the CMS provides a trusted root of peer identity authentication.

Consequently, no separate key-authentication or key-verification procedure is required when users establish secure communication with other enrolled users; the authenticity of the peer's cryptographic credentials is derived from the CMS's centrally established identity-to-key binding.



1.2 Federating with other Cryptify Call systems

Cryptify Call systems may be configured to communicate with other authorized Cryptify Call domains.

Trust between domains is established and controlled through the CMS.

The CCA will only accept identity attestations from peer CMS authorities that have been authenticated and attested by the End User's own CMS.

The CMS attestation and the assigned *Domain Security level* are clearly visible to the End User. When communicating with a peer in another Cryptify domain, the End User can identify the CMS that has attested the peer's identity and associated cryptographic credentials.

The trust relationship between CMS authorities is established and controlled by the local CMS. End Users do not independently assess or validate the legitimacy of a peer CMS or its cryptographic credentials.

2 Roles and Responsibilities

2.1 CMS Operator

The CMS Operator is a highly trusted administrative role responsible for the security-critical functions of the system and for maintaining the association between End Users and their cryptographic identities.

The CMS Operator shall:

- protect physical access to the CMS
- attest the correct association between the End User, the MSISDN, and the cryptographic credentials assigned to the End User
- ensure that the correct End User receives the corresponding initiation letter during enrolment

- ensure that public keys and certificates are associated with the correct End User and authorized device
- manage End User and device lifecycle
- generate and distribute cryptographic updates
- manage security policies
- create and manage multiple contact lists, each comprising:
 - the contact information mapping between End User name and MSISDN
 - a distribution list specifying the End Users who shall receive that contact list
- follow the applicable CMS security and recovery procedures

For federated Cryptify Call systems, the CMS Operator shall:

- verify the peer domain name and the authenticity of its public signing keys
- configure or update the domain name and security level, where required
- attest the domain information and associated public keys
- add or remove trusted domains as required

CMS access shall be limited to the minimum number of highly trusted personnel required to operate the system.

2.2 CRS Operator

The CRS Operator is responsible primarily for availability, infrastructure security and service operation.

The CRS Operator shall:

- restrict CRS administration to authorized personnel
- maintain the underlying operating system and security controls
- restrict network access to required services and ports
- monitor the CRS for suspicious or unauthorized activity
- maintain appropriate backup, recovery and availability arrangements.

The CRS Operator shall not have access to CMS key material.

2.3 End User

The CCA is designed to provide secure communication without requiring End Users to perform cryptographic key validation or other cryptographic administration.

End Users shall nevertheless:

- protect their authorized devices
- prevent unauthorized persons from accessing the application or provisioning material

- follow applicable organisational information-security requirements
- report suspected device or provisioning compromise promptly

In particular, End Users are not responsible for determining the legitimacy of the cryptographic keys or certificates used by the parties with whom they communicate. The authenticity and association of cryptographic credentials with authorized End Users and devices are established and controlled through the CMS.

3 Secure System Operation

3.1 CMS Protection

The CMS is the cryptographic authority of the system and shall be operated as an offline system.

The CMS shall:

- never be connected to an IP network
- be physically protected against unauthorized access
- be operated only by authorized CMS Operators
- be maintained using controlled and verified software and media
- be backed up and restored only according to the applicable CMS procedures

The CMS environment shall be treated as the highest-security component of the deployment.

3.2 CRS Protection

The CRS shall be operated as a security-relevant infrastructure component, even though it does not possess the cryptographic keys required to decrypt communications.

The CRS shall:

- be accessible only through explicitly authorized network paths and ports
- be protected by an appropriate firewall
- run supported and security-patched software
- be administered only by authorized personnel
- be monitored for unauthorized access and suspicious activity

A CRS compromise shall be treated as a potential availability and metadata-security incident.

By default, no events are logged on the CRS. If there is an operational requirement to persist event logs, the optional *Cryptify Log Module (CLM)* can be installed on the CRS. For further information, please refer to the CLM manual [6].

When hosting a CRS, particular consideration shall be given to the legal and jurisdictional circumstances of the hosting environment, especially when event data is

persisted. The hosting location and applicable legal framework shall be assessed to understand the applicable data-protection requirements, lawful-access obligations, and potential disclosure requirements. The deployment shall therefore be designed to avoid unnecessary exposure of event data to jurisdictions or legal regimes that are not appropriate for the intended use of the CRS.

3.3 Software and Platform Maintenance

Only software obtained from an authorized source and verified as authentic shall be installed.

CMS, CRS and CCA software shall be maintained at supported versions. Underlying operating systems and hardware shall receive applicable security updates. Platforms that no longer receive required security updates shall be upgraded or replaced.

Devices and platforms shall be configured in accordance with an appropriate security policy and applicable security guidance, such as the NCSC Device Security Guidance [7].

4 Provisioning and Lifecycle Management

4.1 Initial Enrolment

Initial enrolment is performed using CMS-generated provisioning data.

The provisioning data is transferred to the CCA using one or two QR codes. The QR code(s) contain the user-specific initial cryptographic and configuration data required to establish the device, including the per-user update key and applicable policies.

Where operationally appropriate, QR data may be scanned directly from the CMS without printing an initiation letter.

Where an initiation letter is used:

- it shall be handled according to the classification of the system
- transport shall be controlled and secure
- access shall be limited to the intended recipient
- the letter shall be securely destroyed immediately after successful use

Detailed provisioning procedures are defined in the CMS manual [2] and CCA manuals, which are available for *iOS* [3], *Android* [4], and *Windows* [5].

4.2 Monthly Key Rotation

Cryptographic updates are generated and controlled exclusively by the CMS.

Each End User may have multiple authorized devices. Each authorized device is assigned a unique update key. Prior to transmission from the CMS environment, the update data is encrypted using the update key associated with the intended authorized device. Consequently, the protected update can only be decrypted by the corresponding authorized device.

The protected update follows the following processing flow:

1. generated by the CMS
2. transferred from the CMS to the CRS using offline media
3. distributed by the CRS to the relevant CCA
4. verified and decrypted by the CCA
5. installed by the CCA

The CRS has no knowledge of the update keys and therefore cannot decrypt the protected update contents. The CRS acts solely as an intermediary for the distribution of protected update data.

A fresh, blank optical medium shall be used for each CMS-to-CRS transfer in accordance with the applicable security procedures.

Cryptographic credentials are aligned with the applicable calendar-month lifecycle. Accordingly, the required updates shall be generated and distributed in advance of the applicable transition so that all authorized devices remain provisioned for the subsequent period.

Detailed update procedures are defined in the CMS manual [2] and the CRS manual [1].

4.3 Device Replacement

In the event of device replacement, where there is no indication or reasonable suspicion that the previous device has been compromised, the following procedure shall be followed:

- Execute *Erase keydata* on the previous device to remove its cryptographic key material.
- Follow the procedure specified in chapter 4.1 (*Initial Enrolment*) to provision the replacement device.

The client regularly produces an encrypted backup containing contact lists and group conversation metadata (list of participants and the subject), which is uploaded to the CRS. When scanning a new QR-code for the same number and CMS device identifier on a new phone, the CCA automatically restores this data. Note, however, that the content of messages is never included in the backups uploaded to the CRS.

Furthermore, when assigning multiple devices for the same phone number in the CMS, the devices will automatically synchronize data between themselves. When a new device is scanned, the new client will automatically query the other devices for contact lists and group conversation metadata, which is then sent as an encrypted and signed system message to the new device.

5 Backup, Monitoring and Routine Operations

5.1 Backup

CMS and CRS backups shall be performed according to the applicable product manuals and the organisation's backup policy.

Backup and restore procedures shall be periodically validated.

5.2 Monitoring

The CRS shall be monitored for:

- service availability
- unexpected or suspicious administrative activity
- unauthorized access attempts
- relevant system or security events

CMS activity shall be controlled primarily through physical and administrative protection because the CMS is intentionally isolated from the network.

6 Compromise Recovery

6.1 CMS Compromise

A suspected compromise of the CMS shall be treated as a critical security incident because the CMS is the cryptographic authority of the system.

The affected CMS shall be isolated and the applicable Cryptify CMS compromise-recovery procedure shall be followed.

6.2 CRS Compromise

A suspected CRS compromise shall be investigated as an infrastructure and availability/security incident.

Although the CRS does not possess the cryptographic keys required to decrypt communications, compromise may expose metadata or disrupt service.

6.3 Device or Initiation letter

A suspected compromise of a CCA device or Initiation letter (containing the QR code) shall result in the affected device being removed and re-provisioned according to the applicable recovery procedure.

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>.
- [3] Cryptify AB. *CAB-12:049, CCA iPhone Manual*. URL: <https://cryptify.com/resources>.
- [4] Cryptify AB. *CAB-13:013, CCA Android Manual*. URL: <https://cryptify.com/resources>.
- [5] Cryptify AB. *CAB-17:011, CCA Windows Manual*. URL: <https://cryptify.com/resources>.
- [6] Cryptify AB. *CAB-18:006, Cryptify Log Module*. URL: <https://cryptify.com/resources>.
- [7] NCSC. *Device Security Guidance*. URL: <https://www.ncsc.gov.uk/collection/device-security-guidance>.