Manual

Cryptify Management System
3.16.x

Table of Contents

Scope

This document describes how to install, configure and maintain the Cryptify Management System (CMS).

Target audience is administrators of the CMS.

It is expected that the reader have basic knowledge in the following areas

- Windows 10
- Handling of restricted material

Setup

The CMS is installed on a standard Windows 10 computer equipped with Intel Core i5 or i7, generation 3 or later, processor.

The computer shall have access to a local laser printer, a DVD burner (if not embedded in the computer). To simplify configuring connected domains, it is recommended that the computer is also equipped with a web camera, although this is not required.

Please remember that the computer *must* never be connected to any network (neither wired, nor wireless), this means that any updates or additional SW required, e.g. drivers for the laser printer, needs to be handled using DVD.

Pre-requisites

Windows 10 installed
Local laser printer working
DVD burner working

Please make sure the following information should be available.

License settings is provided from Cryptify:

License Settings	Value
System ID	
License key	

A suitable name for Your Security Domain:
The Security Domain is presented as the entity that has attested the user's identity, i.e. when a user from this domain communicates with a user from another domain this Security Domain name will be displayed to the other user. The recommendation is to use the registered company/government/department name

CMS Settings	Value
Security Domain	

The CRS settings is provided from the CRS host:

CRS Settings	Value
CRS address	
Account ID	
Shared Secret[1]	

[1] Please use the `Courier` font to easily distinguish between capital "i" and "1"

Procedures

Installation and configuration

Please make sure you have access to the CMS installer file.

Run the installer package and accept the default options.

Enter the information gathered above in the corresponding fields during the installation wizard process.

The initial license key will be limited in time. Please provide your Cryptify sales representative with the installation checksum (found in Settings->License Settings), and you'll receive a new license key for this checksum. Please refer to "User Expansion" for how to apply a new license key.

Upgrade

Please make sure you have access to the CMS installer file with the new version.

Run the installer package and accept the default options.

Back-up and restore

Back-up

To backup all settings, user data and layouts, please navigate to the Backup/Restore menu and chose backup. Insert an empty CD/DVD into the burner and press the burn button.

All configuration data is stored in a ZIP archive on the CD/DVD.

Please note that the backup contains all cryptographic keys for the complete system (master keys and all user keys) and hence needs the same level of protection as the CMS itself!

Restore

To restore from a backup on the same machine, please navigate to the Backup/Restore menu and chose Restore.

To restore a backup to a new machine please follow the installation wizard and chose “Restore from backup”. As the license key is directly linked to the checksum of the CMS installation a new license key is required in case of restoring to a new machine!

To receive a new / re-generated license key, please query Cryptify for a new temporary license key, and once the restore process is completed navigate to the Setting menu to retrieve the checksum for the new machine.
Please provide the new checksum to Cryptify to retrieve a permanent license key for the new installation.

Add a single user

Please navigate to the Users menu.

Please type in the name and mobile number of the user in the Add User fields and press “+”
Please note that the mobile number *must* be in international format, i.e. starting with a “+”, e.g. +46706764287.

User details

To view user details, select a user and click on the “Details” button. In this view, additional lines can be assigned to a user, which Cryptify Call for Windows can utilize to setup teleconference calls. In case a user locks the messages view in Cryptify Call with a PIN code and forgets the code, the view can be unlocked by entering the PUK code on the phone. Note that the PUK code changes every month.

Import user data

This function enables an administrator to add multiple users in batch by importing user data from a file.

Please navigate to the Users menu.

Select Import in the Tools sub-menu, and select the file containing users to be imported. Once selected press the Import button to start the import process. Please note that this step can take a while since new keys are generated for each user.

The format of the import file must follow a strict TSV format as defined below:

- File extension “.txt” and file encoding UTF-8 (or ASCII).
- One line per user
- Four columns per line, separated by a tab character.
    - First column: First name
      must NOT contain any of the following characters: " , ' ; <tab>
    - Second column: Last name
      must NOT contain any of the following characters: " , ' ; <tab>
    - Third column: mobile number
      must be in international format, i.e. starting with a “+”, e.g. +46706764287.

- Fourth column: comment
  must NOT contain any of the following characters: " , ' ; <tab>

Example:

John□Doe□+44777666555□Project Alpha

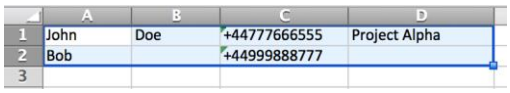
Dana□Doe□+44999888777□

where "□" denotes a tab character.

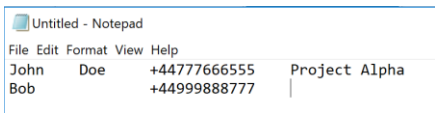
NB: Please note that both fields (Name and Number) must be of the type "text" in case Microsoft Excel, or other spreadsheet programs manage the TSV file.

Creating a TSV-file

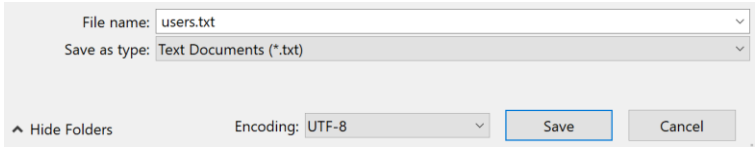
It is easy to create a valid TSV-file using Excel and Notepad (or TextEdit on macOS).



Step 1: Select a range of cells containing four columns and choose copy the cells using Edit > Copy (or control-C).



Step 2: Paste the result into a new document in Notepad. (If using TextEdit on macOS, select Format > Make Plain Text before pasting the data.)



Step 3: Save the document, and make sure to select UTF-8 encoding.

Export user data

This function enables an administrator to export user data, i.e. name and mobile number for multiple users, and store the data to a file. The export file only contains name and number of the users, and does not contain any cryptographic keys.

Please navigate to the Users menu.

Mark the selected users and press Export in the Tools sub-menu to start the export process.

The user data is stored in TSV format on the file.

User Initiation Letters

There are three methods to distribute the initiation letters (including the QR code) from the CMS.

1. User scan the QR code from the CMS screen.
   Please mark the selected user, chose “Details” and select “view”,
2. Print the initiation to a local laser printer
3. Burn the initiation letter(s) in PDF format to a CD/DVD.
   Please mark the selected users and press “Burn PDF”. The "Burn PDF" button is enabled when the CMS detects the presence of a burner, and one or more users are selected in the user list.

Please note that the initiation letter contains the users private keys and hence needs to be protected accordingly!

It is also possible to protect the QR-code with AES-128-CBC and HMAC-SHA-256 using a random 128-bit key. In this case, the user will need to enter the QR Code Key, visible under User Details, after scanning the QR-code in the app.

To adapt the format/text in the initiation letters, please select the Layout button and edit the various fields according to Your preference. Please see chapter “Customisation of initiation letters” below in this document for a list of variables that can be used.

Compromise recovery – User

Please navigate to the Users menu.

Follow this operation in case a device is, or is suspected to be, compromised.

Mark the compromised user(s) and press the “Destroy Keys” in the Tools sub-menu. This will prevent comprised device(s) from rekeying, as the update key used to protect the monthly key updates will be changed.
Please note however that MIKEY-SAKKE keys for the identity, i.e. the mobile number, and any channels the user had access to will remain compromised for the current month and any future months that are already distributed to the phone.

When running CRS version 4.19.0 or later, create a monthly key update and apply it on the CRS to prevent the compromised user(s) from accessing the CRS, without interfering with the rekeyed user(s). For earlier CRS versions, please follow the Block User procedure in the CRS manual to prevent the compromised user(s) from accessing the CRS using the already distributed keys. In either case, the compromised user(s) are prevented from further communication.

In case the device is managed using a MDM system please follow the appropriate procedure to remotely wipe the device.

Delete a user

Select the user(s) and press “Delete”.

Channel management

Channels offer a complement to the end-user managed messaging groups that scales to thousands of users. Currently, channels do not extend to connected domains.

Channel messages work in the same manner as regular secure text messages, both in terms of cryptography and signalling: messages are end-to-end protected using MIKEY-SAKKE and a message to a channel is distributed by the CRS to all the users of the channels.

Instead of a telephone number, which is what identifies a user, a channel has a randomly generated identifier. This identifier, however, is normally not visible to the end user, who instead sees the manually chosen channel name. The channel name, as opposed to the random identifier, is only visible to those users that have been added to the channel – in particular, it is not accessible on the CRS.

Create

Navigate to the "Channels" tab, enter a name for the channel and press the "+"-button. Up to 50 channels can be added.

To add users, see "Modify" below.

Modify

Navigate to the "Channels" tab, select the channel to modify and press the "Details" button.

In the list of users, access for each user can be set (No access, Read & Post, Read-only and Post-only). It is also possible to add or remove a user to a channel on the User details page, available under "Users".

It is also possible to delete an entire channel by instead pressing the "Delete" button in the list of channels. Note that deleting a channel does not delete any existing conversation on the end-user devices.

As usual, modifications do not take effect until a crypto update has been published on the CRS and downloaded by the end-user device.

Contact list management

Centrally managed contact lists offer a complement to the end-user managed secure contact list. Currently, centrally managed contact lists do not extend to connected domains.

Centrally managed contact lists cannot be disabled by the user, and the names listed override those found in the user's own contact book or in contact lists shared by end-users.

Create

Navigate to the “Contact lists” tab, enter a name for the contact list and press the “+”-button. Up to 50 contact lists can be added.

To add users, see “Modify” below.

Modify

Navigate to the “Contact lists” tab, select the contact list to modify and press the “Details” button.

For each user, it is configured (i) whether the user appears as an entry in the contact list and (ii) whether the user should get a copy of the contact list.

To delete a contact list, press the “Delete” button in the list of contact lists.

As usual, modifications do not take effect until a crypto update has been published on the CRS and downloaded by the end-user device.

Add a Gateway (CIG)

Please navigate to the Gateways menu.

Please type in the name, tel-uri number and the desired number of Crypto Engines of the gateway in the Add Gateway fields and press “+”. Note that it is not possible to assign less than three Crypto Engines to a single gateway. Please note that the URI *must* be in international format, i.e. starting with a “+”, e.g. +8888.

Gateway Initiation Letters

There are two methods to distribute the initiation letters from the CMS.

1. Print the initiation to a local laser printer
2. Burn the initiation letter(s) in PDF format to a CD/DVD.
   Please mark the selected gateway(s) and press “Burn PDF”. The "Burn PDF" button is enabled when the CMS detects the presence of a burner, and one or more gateways are selected in the user list.

Please note that the initiation letter contains the private keys of the gateway and hence needs to be protected accordingly!

To adapt the format/text in the initiation letters, please select the Layout button and edit the various fields according to Your preference. Please see chapter “Customisation of initiation letters” below in this document for a list of variables that can be used.

Delete a gateway (CIG)

Select the gateway(s) and press “Delete”.

Modify a gateway (CIG)

To modify the name or the number of crypto engines of a gateway, select a gateway and press “Edit”.

My Domain certificate

Please navigate to the Connected Domains menu.

The domain certificate can either be printed to the attached printer, or burned as a PDF to a DVD/CDR.
Please select Print or “Burn PDF “from the “My Domain” sub-menu

To adapt the format/text in the domain certificate, please select the Layout button and edit the various fields according to Your preference. Please see chapter “Customisation of initiation letters” below in this document for a list of variables that can be used.

Add a peer Domain

Please navigate to the Connected Domains menu.

Select one of the “Add Domain” buttons from the sub-menu to either scan a domain QR-code or to manually enter the row data, in case the CMS is not equipped with a camera. Note that domain certificates generated by CMS versions before 3.11.0 only contain QR-codes and must hence be scanned using a camera.

The authenticity of the public certificate is of vital importance! You shall never add a domain if you are unsure of the origin of the certificate.
The recommended procedure is to meet the CMS administrator of the other Security Domain and exchange the public certificates in person.

If scanning a QR-code, place the QR code containing the public certificate of the peer in front of the camera. Else, manually enter the domain parameters row-by-row. Each row of data has an embedded checksum, and entry of the next row is not possible until the current row has been successfully entered.

Please verify that the domain name and Id of the Connected Domain is what you expect. This domain name will be displayed to your clients when they communicate with users belonging to this Security Domain.

Once a Connected Domain has been added that domain’s credentials must be provisioned to the CRS, who in turn will distribute the clients.
This is done by providing the CRS with a new update file. Please refer to the “Monthly key updates” chapter.

Please note that both parties (you and the peer) must perform these actions in order to allow cross domain communication.

Delete a peer Domain

Please navigate to the Connected Domains menu.

Select the Connected Domain to delete and press “Delete”.

Once a domain have been deleted that domain’s credentials must be revoked from the CRS.
This is done by providing the CRS with a new update file. Please refer to the “Monthly key updates” chapter.

Monthly key updates

Please navigate to the Update menu.

3. Insert a blank CD/DVD in the burner and follow the instructions on the screen.
   The system will generate an update file for the current and the next month. The update file contains one entry per user. Each entry is protected by a unique secret shared by the CMS and each user
4. Insert the CD/DVD into a computer that is connected to the Internet and send the update file to Your CRS host (in case this is Cryptify please send to support@cryptify.com)

Please make sure to send the update file at least 3 days before the start of the month, e.g. for May 2013 the update file shall be sent before the 27th of April 2013.

Note that it’s recommended to use CD instead of DVD as a DVD can take a long time (~5 min) to finalize.

Since the CMS is offline and preferably powered off when not in use, it is recommended that the administrator add reminders for the monthly update activities in the ordinary calendar, e.g. a reminder 3 days before the end of each month. It is also possible to subscribe to Cryptifys update reminder mailing list at the partner area at cryptify.com.

User expansion

To expand the number of allowed users please acquire desired licenses.

Please select “New License” in the *Settings* menu and enter the new license key provided from Cryptify.

CRS migration

This procedure described how to make a smooth migration of users to new CRS. Information of which CRS to attach to is provided to the users both as part of the QR code, and in the monthly updates.

It is recommended to make the migration in conjunction with a monthly key update in order to make a smooth, synchronized migration.

1. Create an account on the new CRS, and note the following information

CRS Info	Value
CRS address	
Account ID	
Shared Secret	

2. Update the CRS information in the *Settings* menu.

   N.B. *Users added after the changes are made will be directed to the new CRS even for the current month and hence unable to communicate with the other users still located on the old CRS!*

3. Follow the *Monthly Key Update* procedure above

4. When all the users are migrated the account can be removed from the old CRS

Compromised recovery – CMS

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

Please follow the Delete an Account procedure to remove the compromised CMS from the CRS. This will prevent all users belonging to the compromised CMS from further secure communication.
Create a new account on the CRS with a new shared secret.

Subject to the nature of the compromise, the user data, e.g. name and mobile number, can be exported from the compromised CMS using the "Export user data" procedure.

Using a new / clean machine please follow the procedure for Pre-Installation, Install and Configure as well Initial key distribution to create a new CMS and to provision users with new key material.
In case it was possible/suitable to export the user data from the compromised CMS, please follow the import user data procedure.

NB! It is NOT possible to restore from a backup as the master keys of the system are compromised!

Please follow the Manual Key Updates procedure in the CCA manual to install the new keys onto each of the phones that was previously provisioned on the compromised CMS.

New pairing is required to enable cross domain communication again as the domain certificate is linked to the new master keys of the system. Please follow the procedure to print Your domain certificate and add your peers again. Please make Your peers aware of the new certificate Id.

CMS Parameters

CMS

Security Domain

The Security Domain shall uniquely identify the instance of the CMS. The Security Domain will be presented to calling/called users to identify which security entity that has attested the other party's identity, e.g. when communicating with users from a Connected Domain.

License

System ID

This is a unique identity of the CMS, e.g. if an organization have several CMS:s where each CMS must have a unique System ID.

The System ID is provided by Cryptify, together with the License key.

Checksum

The checksum uniquely identifies the installation of one CMS instance.

License key

The license key is valid for a specific System ID and enables the CMS administrator to create the number of users purchased.

CRS

The CRS host shall provide the following parameters:

Account ID

The Account ID uniquely identifies the CMS in the CRS.

CRS address

The CRS address is the IP or FQDN used by the clients to connect to the CRS. In case of FQDN the DNS server can be set up to provide two IP addresses to the clients to enable load sharing across the CRS servers.

Shared Secret

The shared secret is used to derive per user unique TLS credentials used for protecting the communication between the user and the CRS.
Please note that the TLS protection is unrelated to call and messaging security, which uses end-to-end encryption mechanisms, i.e. MIKEY-SAKKE for key exchange and AES for media.

Settings and compatibility

Message lifetime

For the domain, it is possible to configure that text messages should expire at a specific point in time, calculated relative to the point in time when the message was sent. Clients will not display the contents of expired messages.

Note that message expiry is only supported by Cryptify Call version 3.18.0 or later for iPhone, Cryptify Call version 3.19.0 or later for Android, Cryptify Call version 3.6.0 for Windows or Cryptify Interconnect Gateway version 2.5.0 or later. Enabling maximum message lifetime will prevent all other clients and gateways from using any part of the system.

Users may manually specify a shorter message lifetime for each outgoing message. Recent clients also have support for a default message lifetime, which is applied unless the user manually chooses a shorter or longer (up to the configured maximum) message lifetime. Clients that do not support default message lifetime simply ignore it and instead apply the maximum lifetime; if the client is then updated, the default message lifetime will be applied once the next crypto update is published.

Example: Suppose the maximum message lifetime is 30 days and that the default message lifetime is set to 12 hours. Any message outgoing will then by default expire 12 hours after being sent, but the user may optionally configure any other lifetime between 1 hour and 30 days when sending the message. The same rules apply for incoming messages, and all messages – even those from a connected domain with different maximum message lifetime – will expire after at most 30 days.

Authorized intercept with minimal key exposure
Data ownership, including support for legal or authorised interception is an important property of the MIKEY-SAKKE standards and critical for certain use cases, e.g. legal compliance when operators are providing communication services, auditing requirements for banks, etc.

For the avoidance of doubt, interception is only possible if the appropriate keys are retrieved from the CMS!

In MIKEY-SAKKE the session key is encrypted using SAKKE algorithms so that only the receiver can decrypt it using its Receiver Secret Key (RSK).

Authorized intercept with minimal key exposure is a measure to limit the key exposure to the target of interception's RSK only, whereas the default MIKEY-SAKKE protocol will require the RSKs of the all the communication peers as well.

Authorized intercept with minimal key exposure is supported by Cryptify Call for iPhone version 3.19.0 or later and Cryptify Call for Android version 3.20.0 or later. Enabling authorized intercept with minimal key exposure will prevent all other clients and gateways from using any part of the system.

Multipath networking
Cryptify Call can be configured to make simultaneous use of multiple network interfaces, which improves the connectivity and audio quality when a secondary network offers better quality than the default network.

A typical example is a phone that is slow to switch over from a WiFi network to the cellular network when the user moves away from the access point. Note also that a WiFi network that works well for activities such as browsing the web or access email might perform badly for voice calls, due to the time sensitive nature of VoIP.

When using VPN in conjunction with multipath networking, however, the app may in some configurations end up bypassing the configured VPN. This is, in general, not undesirable since voice calls have low-latency requirements and all traffic from the app is already encrypted.

Multipath networking is supported by Cryptify Call for iPhone version 3.20.0 or later, or Cryptify Call for Android version 3.21.0 or later. If a user is running a version of Cryptify Call for iPhone before 3.13.0 or Cryptify Call for Android before 3.14.0 when multipath networking is enabled, then the change will not take effect until after the updated client has received a crypto update, which may take up to one month.

Log settings
By default, the CMS only writes log events to its internal event log, but it can be configured to also write the log entries to the standard Windows event log.

Channels
Channels are configured under the "Channels" tab. Support for channels is available in Cryptify Call for iPhone version 3.22.0 or later, Cryptify Call for Android version 3.23.0 or later and Cryptify Call for Windows version 3.7.0 or later. Furthermore, the CRS must run version 4.14.0 or later.

Users running earlier versions should not be added to any channel, as doing so will prevent the user from consuming future crypto updates.

Centrally managed contact lists
Centrally managed contact lists are configured under the "Contact lists" tab. Support for centrally managed contact lists is available in Cryptify Call for iPhone and Android version 3.37.0 or later and Cryptify call for Windows version 3.18.0 or later. Furthermore, the CRS must run version 4.26.0 or later.

Customisation of initiation letters

Environment variables have been introduced in order to enable customisation of initiation letters and the domain certificate. These can be used to include the name of the recipient, crypto date and domain, and the export date.

Variable	*Example*
Name	
$FULLNAME	*John Göran Smith*
$FIRSTNAME	*John*
$MIDDLENAMES	*Göran*
$LASTNAME	*Smith*

$SURNAME	*Smith*
Crypto	
$URI	*+46001*
$CRSACCOUNT	*DEMOACCOUNT_1*
$CRSADDRESS	*crs.example.net*
$DOMAIN	*domain.example.net*
$PERIOD	*2013-09*
$CRYPTOMONTH	*September*
$OWN-DOMAIN-ID	*0246 ABEF*
$OWN-DOMAIN-FINGERPRINT	*E3B0 C442 98FC 1C14 9AFB F4C8 996F B924 27AE 41E4 649B 934C A495 991B 7852 B855*
Time	*2013-09-07T20:23:09+02:00*
$YEAR	*2013*
$SINGLEYEAR	*13*
$MONTH	*09*
$SINGLEMONTH	*9*
$THEMONTH	*September*
$MMMM	*September*
$MMM	*Sept*
$MM	*09*
$M	*9*
$WEEKDAY	*Saturday*
$DAY	*07*
$SINGLEDAY	*7*
$DAYSUFFIX	*th*
$HOURS 20	
$12HOURS	*08*
$12SINGLEHOURS	*8*
$MINUTES	*23*
$SECONDS	*09*
$AMPM	*PM*
$ZZZ	*+02:00*
$ZZ	*+02*