User Guide v1.3

CryptoMon, Version 1 Release 1 Level 3

Second Edition (December 2009)

This document applies to CryptoMon Version 1 Release 1 Level 0 (preview version)

Introduction

An organization's very existence may depend on the quality of its security. Cryptography – the encrypting and decrypting of information that is deemed to be private and confidential – is an extremely important component of an organization's security program. It provides an additional level of security should an intruder breach other aspects of your security system. To help you implement cryptography in your mainframe site, the z/OS system provides several hardware and software components, be they IBM's or third-party products.

ICSF (Integrated Cryptographic Service Facility) is the IBM licensed program that provides access to the hardware cryptographic feature. It supports hashing, digital signature, conventional as well as public-key cryptography and other cryptographic features. Its main strength is secure key cryptography: secret keys or private keys can never be found in a readable form outside the cryptographic hardware.

The issue here is that the people in charge of security have very little information about how cryptography and ICSF are implemented. The cryptographic control data sets that ICSF uses may contain errors or be out of sync. Cryptographic keys may have been created, that you know nothing about. Problems may be looming, such as keys that are about to expire as well as digital certificates (that are in fact a specific type of key). RACF may not correctly protect keys or ICSF services. Several types of exceptions and concerns are checked. Security violations of all sorts or some important cryptographic events may occur and go unnoticed.

CryptoMon has been specifically designed to display the missing information. It is the ideal product for enterprise data centers that make an everyday use of cryptography and want to know what happens under the cover. Not only does it provide you, the user of z/OS cryptography, with a comprehensive tool for readily monitoring your cryptographic system, but it also enables you to invoke crypto services to accomplish some specific housekeeping tasks.

As a non-invasive mainframe product, CryptoMon is also quite easy to install and implement. The first real world use of the product is a matter of hours, since its ISPF interface is very straightforward.

This manual is intended for any person who wants to become familiar with the CryptoMon product. It reviews the functions provided with the product and benefits of their use. It will be useful for technical staff who will be installing or using the product.

1. Installation of CryptoMon

1.1 Description

CryptoMon is delivered with the following libraries:

- MCYISPF: ISPF elements (panels, messages)
- MCYCNTL: JCLs and parameters
- MCYLOAD: load modules (executable programs)
- MCYINST: installation file, contains all other libraries in XMIT format

You will find below the installation steps.

1.2 Unloading

The binary file (MCYINST.XMI) that you received must be transferred to MVS into a sequential LRECL 80 file.

Perform the following steps to unload the product.

1. Upload the XMI file shipped to you to your mainframe host using the binary transfer method (the receiving file should be pre-allocated with LRECL 80).

2. From ISPF option 3.4, pull up the file you uploaded in step #1.

3. Tab down to the file and enter the following TSO command against the file:

```
RECEIVE INDA(/)
```

You will be prompted with text similar to the following:

```
INMR901I Dataset MCY.V110.MCYINST from IBMUSER on NODENAME
INMR906A Enter restore parameters or 'DELETE' or 'END' +
```

4. Respond as follows to the "Enter restore parameters…." message, above:

```
DA('desired.installation.dataset.name')
```

or :

```
DA('desired.installation.dataset.name') VOL(desired.allocation.volume)
```

You will then see IEBCOPY messages and control statements appear on your screen as the XMI file is unloaded to your production data set. Your 'desired.dataset.name' file is now ready. It will be a partitioned data set.

5. Adapt and submit member **RECEIVE**. This will create and upload all libraries from the installation members. You should not change the last dsn qualifier of the libraries (for example: MCYLOAD).

1.3 Setting the license code

CryptoMon requires a license code. Adapt member **PASSWORD** in library MCYCNTL by specifying the temporary or permanent license code that was granted to you by the vendor, then submit the JCL.

1.4 APF authorization

Several functions of the product need authorization through the MCYTASK started task. In order to start it, you have to specify in the PROGxx member of the current PARMLIB the dsname of the CryptoMon load-module library, and the name of the disk volume it resides on, for example:

```
        . . .
APF ADD  DSNAME(PROD.MCY.V110.MCYLOAD)  VOLUME(VOL001)
        . . .
```

Make sure the new entry is taken into account by the system: this requires an IPL, or a SET PROG=xx command, or the SETPROG command:

```
SETPROG APF,ADD,DSN=PROD.MCY.V110.MCYLOAD,VOL=VOL001
```

An alternate option consists in copying CryptoMon modules to a system library or to an existing APF library.

1.5 Starting the MCYTASK started task

Several functions of the product need authorization through a started task that is provided in MCYCNTL(MCYTASK). Copy this member in one of your system PROCLIBs. Have the started task MCYTASK launched just after IPL. This task does not require any particular authorization but should always be active. The STEPLIB must be APF-authorized (see paragraph « APF authorization »).

1.6 Controlling access to the product (optional)

Because CryptoMon displays information that either is not, or should not, be accessible to anybody, access to CryptoMon features requires authorization.

In this purpose, you must define a new profile in the RACF FACILITY class. You may use the following command:

RDEF FACILITY MCY.MONITOR UACC(NONE)

Only users that have READ access to the MCY.MONITOR profile are allowed to use the CryptoMon ISPF interface. This permission can be granted using the following command:

PE MCY.MONITOR CLASS(FACILITY) ID(userid) ACC(READ)

You may also have to refresh the class: SETR REFR RACLIST(FACILITY)

If the MCY.MONITOR profile is not defined, then anybody that has access to CryptoMon libraries may use the product.

1.7 Installing the ISPF interface

The REXX exec MCY in the MCYCNTL library should be adapted and installed in a common SYSPROC or SYSEXEC library. The alternative would be to call it directly via a TSO EXEC ‘MCY.MCYCNTL(MCY)’ command.