CPM Objective

To begin to bring full transaction and data security into the Mojaloop Ecosystem, including the management of keys and signing/encryption of data approportionate to risk (For OSS) and/or as mandated by compliance requirements (For Hub Operators)

Max Gysi

Lead Security Architect

Mojaloop Cryptographic Processing Module

Low Level Design Overview

Table of Contents

[Overview 3](#_Toc49771657)

[Glossary 4](#_Toc49771658)

[System 5](#_Toc49771659)

[Overview 5](#_Toc49771660)

[Message formats 5](#_Toc49771661)

[Commands Adapter 5](#_Toc49771662)

[Security Adapters 6](#_Toc49771663)

[Key update Adapters 6](#_Toc49771664)

[High level Flows 7](#_Toc49771665)

[Key Add/Update/Delete Flow 7](#_Toc49771666)

[Add/Update Key 7](#_Toc49771667)

[Delete Key 7](#_Toc49771668)

[Hardware HSM adapter Flow 7](#_Toc49771669)

[Start-up 7](#_Toc49771670)

[Shut-down 7](#_Toc49771671)

[Process Message 8](#_Toc49771672)

[Health Checks 8](#_Toc49771673)

[Software HSM adapter Flow 8](#_Toc49771674)

[Start-up 8](#_Toc49771675)

[Shut-down 8](#_Toc49771676)

[Process Message 8](#_Toc49771677)

[Command Adapter Flow 9](#_Toc49771678)

[Start-up 9](#_Toc49771679)

[Shut-down 9](#_Toc49771680)

[Process 9](#_Toc49771681)

[Cryptographic Processing Module 9](#_Toc49771682)

[Start-up 9](#_Toc49771683)

[Shut-down 9](#_Toc49771684)

[Process 10](#_Toc49771685)

[Database Configurations 11](#_Toc49771686)

[Adapter Configuration 11](#_Toc49771687)

[Hardware HSM Configurations 11](#_Toc49771688)

[Software HSM Configurations 11](#_Toc49771689)

[Message configuration 12](#_Toc49771690)

[Command configuration 12](#_Toc49771691)

[CPM Configuration 12](#_Toc49771692)

[Key Configuration 12](#_Toc49771693)

# Overview

The current Mojaloop system has been developed with limited built in security. The next phase requires that Mojaloop will conform to international norms as regards security. To achieve this a separate module will be developed that will interact with Mojaloop but will extract the necessary security operations from the current Mojaloop processing.

By having a separate module to handle all the security processing minimal changes will be required on the current Mojaloop system

This module will be able to interact with a key management system as necessary for the necessary encryption keys, as well as various HSMs to perform secure cryptographic operations. Should an external key management system or physical HSMs not be available the module will provide a key storage system as well as limited cryptographic operations performed in software.

This document will provide an overview of what will be included in the first version of the CPM. It should be noted that this list is to be discussed and agreed upon before moving onto the next phase where this will be expanded into a specification which will detail the full agreed functionality of the first phase of the CPM.

When designing and building the CPM the following will be taken into consideration:

1. There will be minimal or no cost in the running of a separate module to handle the security aspects of Mojaloop
2. The system will be designed is a way that hardware security will not be enforced provided the entity running the CPM understands and accepts any risks associated with this
3. Certain aspects of security will only be available under hardware security if by implementing it in software the integrity of any systems connection to the Mojaloop Instance

While the low-level document will give a detail specification of the CPM as known at that stage it must be considered a living document which could change during the development phase.

Although not documented here changes will be required to the main Mojaloop code in order to instruct it that all security functions need to be performed by the CPM. In phase one this can be done via a configuration setting in order not to force current users of the Mojaloop code to use the CPM immediately but rather switch over when they wish to do so. It should be encouraged that all new installations of Mojaloop use the CPM module once it becomes available.

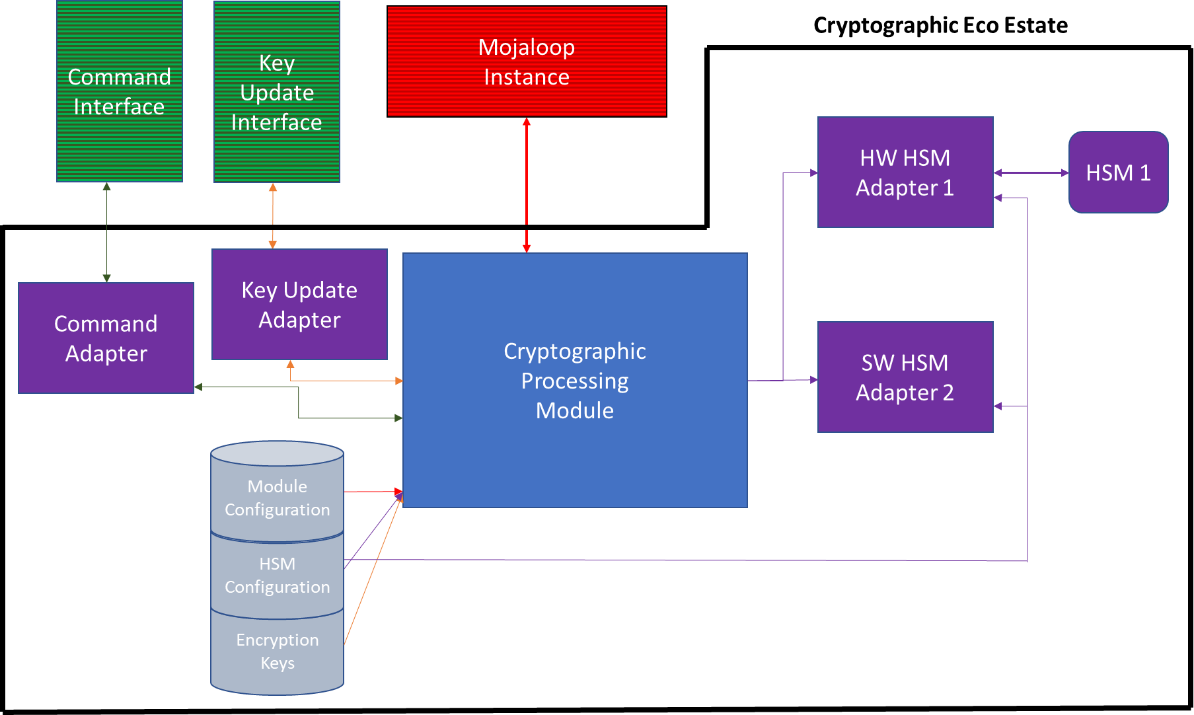
# Glossary

|  |  |
| --- | --- |
| **Term** | **Definition** |
| FSP | Financial Services Provider |
| CPM | Cryptographic Processing Module |
| HSM | Hardware Security Module |
| KMS | Key Management System |

# System

## Overview

Below is a high-level system diagram of how the Cryptographic Eco Estate will be constituted for this first version of the CPM. Only modules within the Eco Estate border will be covered in this document.



The following sections give a high level list of what will be included in the low level design for the CPM

## Message formats

1. From (and response) Mojaloop
2. To (and response) to HSM adapter
3. Message format (and response) to update keys – to be discussed
4. Commands to CPM messages

## Commands Adapter

1. Start-up
2. Shutdown
3. Commands
   1. Shut down
   2. Refresh keys
   3. Refresh config
   4. Status

## Security Adapters

1. Start-up
2. Shutdown
3. Software – Move security code from Mojaloop core into the adapter controlled by the CPM
4. Define basic processing of HSM adapter
   1. Read DB config to obtain necessary information
   2. Connecting to HSM(s)
   3. Regular health messages to each configured HSM
   4. Accept message from CPM
   5. Build message to HSM
   6. Send message to HSM
   7. Accept response
   8. Send response to CPM

## Key update Adapters

1. Start-up
2. Shutdown
3. Define basic processing of Key Update adapter
   1. Read DB config to obtain necessary information
   2. Accept message from external party
   3. Build message to CPM
   4. Send message to CPM
   5. Accept response
   6. Send response to external party

# High level Flows

The following is a high-level flow for each part of the system. Once this has been agreed to a full flow will be documented.

## Key Add/Update/Delete Flow

### Add/Update Key

1. Adapter Accepts message
2. Adapter sends messages to CPM
3. If translation needed
   1. Send to HSM Adapter
   2. Receive message back from adapter
4. If translation successful
   1. If key exists
      1. Update Key
      2. Else Add key
5. Respond to Adapter with result
6. Adapter responds with result

### Delete Key

1. Adapter Accepts message
2. Adapter sends messages to CPM
3. If key exists
   1. Delete Key
4. Respond to Adapter with result
5. Adapter responds with result

## Hardware HSM adapter Flow

### Start-up

1. Read DB for configuration parameters for Adapter
2. For each defined HSM
   1. Connect to HSM
   2. Send status message to HSM
   3. Log status message
   4. Mark each HSM as available
3. Go to wait for message stage

### Shut-down

1. Mark adapter for shut-down
2. Stop accepting new messages, and respond with “Closing” if any received
3. For each defined HSM
   1. Check for outstanding messages
   2. Once all outstanding messages have been received from HSM disconnect from HSM
   3. Log message
4. Respond with “closed message”
5. Close all DB connections
6. Shut down adapter

### Process Message

1. Accept message from CPM
2. Check for Available HSM, if no HSM active recline message
3. Validate input message
4. Translate message from input format into HSM specific format
5. Choose HSM to process message
6. Send to HSM
7. Accept response from HSM
8. Translate message to input format from HSM specific format
9. Respond to CPM

### Health Checks

1. Based on the interval set in the configuration send a message to the HSM to confirm it is still connected and functional
2. If Health Check unsuccessful remove HSM from active list
3. If Health Check successful and HSM was in the in-active list move to active list

## Software HSM adapter Flow

### Start-up

1. Read DB for configuration parameters for Adapter
2. Go to wait for message stage

### Shut-down

1. Mark adapter for shut-down
2. Stop accepting new messages, and respond with “Closing” if any received
3. Once all outstanding messages have been processed and responded to log message
4. Respond with “closed message”
5. Close all DB connections
6. Shut down adapter

### Process Message

1. Accept message from CPM
2. Validate input message
3. Process message
4. Translate message to input format
5. Respond to CPM

## Command Adapter Flow

### Start-up

1. Read DB for configuration parameters for Adapter
2. Set up listen on appropriate port
3. Go to wait for connection stage

### Shut-down

1. Mark adapter for shut-down
2. Stop accepting new messages, and respond with “Closing” if any received
3. Once all outstanding commands have processed respond with “closed message”
4. Close all DB connections
5. Shut down adapter

### Process

1. Accept connection
2. Check source IP is acceptable IP (from config)
3. Accept and validate input message
4. Format from external message format to internal format
5. Send message to CPM
6. Wait for response
7. Respond to sender of message

## Cryptographic Processing Module

### Start-up

1. Read DB for configuration parameters
2. Set up Adapters
3. Go to wait for connection stage

### Shut-down

1. Mark CPM for shut-down
2. Send Shut down to all adapters
3. Stop accepting new messages, and respond with “Closing” if any received
4. Once all outstanding messages have processed respond with “closed message”
5. Close all DB connections
6. Shut down adapter

### Process

#### Commands

1. Accept command from adapter
2. Process command as required
3. Respond to adapter with result

#### Key Update

1. Accept command from adapter
2. Verify message fields
3. Update/Add/Delete key as necessary in DB
4. Refresh keys in memory
5. Respond to adapter with result

#### Message

1. Accept message
2. Verify fields
3. Check adapter definitions for match on FSP and security command to determine the correct HSM adaptor
4. Format from message format to internal HSM format
5. Send to appropriate adapter
6. Wait for response
7. Respond to sender of message

# Database Configurations

The following is a suggested layout for the basic database configuration for each part of the system. Once this has been agreed it will be documented in more detail.

## Adapter Configuration

1. Adapter Name
2. Adapter Specific Information

## Hardware HSM Configurations

1. Adapter Name – Key
2. Adapter type
3. HSM type – Informational
   1. HSM1
      1. Name
      2. IP
      3. Port
      4. Header type
      5. Priority
      6. Health Message interval (seconds) – 0 = no health message
      7. Message timeout
      8. HSM Specific information
   2. HSM..n
      1. Name
      2. IP
      3. Port
      4. Header type
      5. Priority
      6. Health Message interval (seconds) – 0 = no health message
      7. Message timeout
      8. HSM Specific information

## Software HSM Configurations

1. Adapter Name – Key
2. Adapter type

## Message configuration

1. FSP name - Key
2. Message type – Key
3. Enabled – True/False
4. Adapter

## Command configuration

1. Whitelist IPs
2. User
   1. User ID
   2. User Group
3. User Groups
4. Commands per group

## CPM Configuration

1. Common Name
2. Adapters

## Key Configuration

1. FSP
2. Key Name
3. Date created
4. Date updated
5. Created by
6. Updated by
7. Key type
8. Key Expiry type
9. Key Use
10. Key Specific details