MOJALOOP CRYPTOGRAPHIC PROCESSING MODULE

Low Level Technical Specification

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

Table of Contents

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 technical specification of the Cryptographic Processing Module (CPM). This will cover 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
DB	Data Base
SSM	Software Security Module

References

This document references the following:

Nr.	Title and Version	Author	Comments
1	Use Cases V1.0		
2	API Definition V1.0		
3	Generic Transaction Patterns V1.0		
4	Encryption		

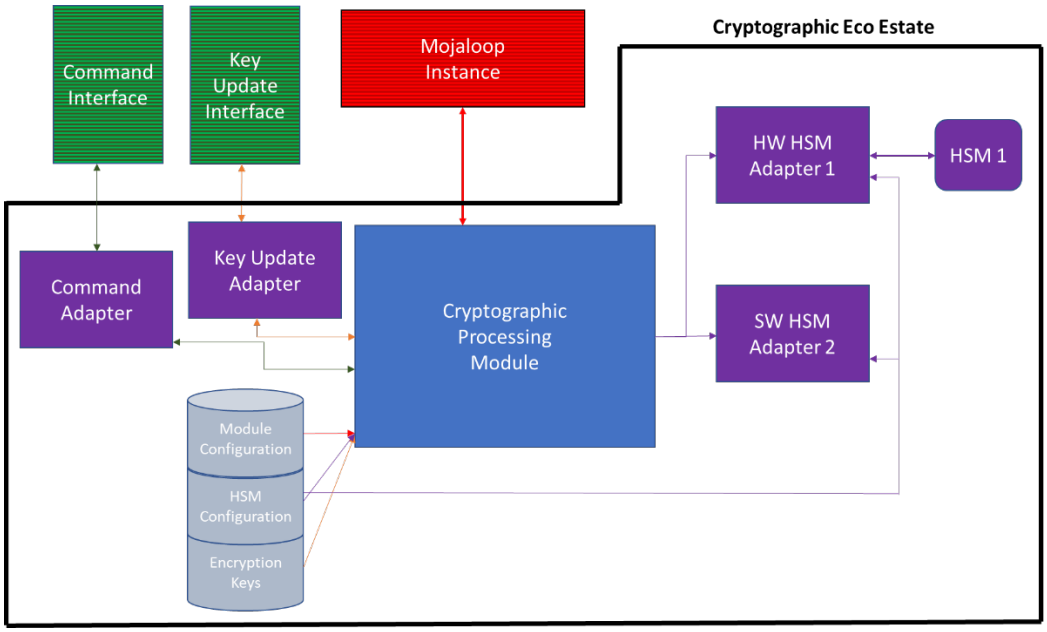
Version

Version	Draft/Release	Author	Comments
0.1	Draft	Max Gysi	InitialVersion

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.



Cryptographic Processing Module

Overview

The CPM will control all aspects of security processing that needs to happen during the processing of a transaction or in the management of keys of the security processor.

Start up

When the CPM starts it will read the DB for the configuration necessary for it to understand how to process any transaction it may receive.

Configuration

At start up the following configuration shall be read into memory

1. Defined Security Module adaptors – The CPM will build a list of Security Module adaptors that will be available to it for the processing of transactions. The following are the necessary configuration the CPM will use
    a. Adaptor Name
    b. Enabled/Disabled
    c. Adaptor IP and port
2. Transaction List – This is the list of transactions that will be permissible for the CPM to perform. The following are the necessary configuration the CPM will use
    a. Transaction Type
    b. Security Adaptor
3. Mojaloop Port to listen on – This is the port on which the CPM will listen on to accept connections and transactions from the Mojaloop instance that it will provide security for.
4. Command Port to listen on – This is the port on which the CPM will listen on to accept connections and commands from the Command adaptors that may be configured to the system.
5. Key Update Port to listen on – This is the port on which the CPM will listen on to accept connections and commands from the Key Update adaptors that may be configured to the system.

Once the CPM has read all its configuration it will implement the configuration and perform self-checks to ensure it can process the transactions as requested. Once all self-checks have been performed the appropriate messages stating the outcome of the self-checks must be logged using the standard Mojaloop logging processing.

Security Adaptors

The CPM will run through the list of enabled Security Adaptors it has configured and perform the necessary steps:

1. Start the Adaptor service
2. Once successfully started, connect to the Adaptor.
3. Once successfully connected mark it as Active

The CPM needs a minimum of one enabled Security adaptor to function correctly.

Command Port

The CPM will start listening on the configured port where the Command Adaptors will connect to. This is not a necessary configuration for the CPM to function

Key Update Port

The CPM will start listening on the configured port where the Key Update Adaptors will connect to. This is not a necessary configuration for the CPM to function

Mojaloop Port

The CPM will start listening on the configured port where the Mojaloop instance will connect to will connect to. This is a necessary configuration for the CPM to function. If it is not configured or the CPM cannot set up the listening port the CPM will log an error message and shut down

Once all the configuration has been successfully processed and successful passed all self-checks the CPM will set itself into “ACTIVE” state and processing to the main processing module. A message must be logged using the standard Mojaloop logging processing stating the CPM is ready to accept transactions

Processing

The CPM has three main areas of processing

1. Commands
2. Key Updates
3. Encryption/Decryption

Although all three will be done by the CPM they will be as three sections within the CPM processing.

Commands

Through the use of commands sent to the CPM the CPM will be able to control different aspects of the process while ensuring the best possible uptime. The permissible commands are

1. Shutdown
   A shutdown message may be sent to the CPM to shutdown either a particular adapter or the entire system. If the shutdown command contains the name of an

adapter the CPM will shut down that one particular adapter, else will shut down the entire system.

a. Shut down a single adapter
   Should the Shutdown message contain the main of an adapter the message shall be processed as follows:
   i. Validate the Adapter name is a valid adapter.
   ii. If the Adapter name is not a valid adapter in this system an appropriate response is built and a response sent back to the Command adapter.
   iii. Once the Adapter name has been validated a shutdown message will be built and sent to the adapter on the already established link
   iv. A timer set to wait for a response from the adapter
   v. When either a response is received from the adapter or the timer expires the connection will be closed if still active and a message logged using the standard Mojaloop logging processing stating the was closed by the CPM

b. Shutting down the Entire system.
   Should a Shutdown message be received without an Adapter name the entire system will be shutdown in an orderly fashion as described in the Shutdown section.

2. Startup
   A Startup command may be sent to the CPM to instruct it to start any adapters that may be stopped for any reason as follows:
   i. Check its status for any stop adapters
   ii. If the Startup commands contains the name of an adapter that is stopped only that adapter must be started
      a) If the named adapter is not stopped or does not exist an appropriate response message shall be constructed and a response sent
      b) If the named adapter is found to be in a stopped state it must be started and once the start-up routine has completed a successful response message shall be constructed and a response sent.
   iii. If the name of a specific adapter is not supplied all stopped adapters shall be restarted. Once this has been done an appropriate response message shall be constructed and a response sent
   iv. Once processing on the message has been completed a message logged using the standard Mojaloop logging processing stating the adapters were started by the CPM

3. RefreshConfig
   A command may be sent to the CPM instructing it to refresh its config for a variety of reasons, e.g. a new adapter has been added. When this command has been received it shall be processed as follows:
   a. Read the DB for any changes to the configuration
   b. Apply the new configuration as necessary
   c. Stop/Start and adapters as necessary
   d. Construct an appropriate response and send it

e. Log a message using the standard Mojaloop logging processing stating the configuration has been updated

4. RefreshKeys

   A command may be sent to the CPM instructing it to refresh its keys for a variety of reasons. When this command has been received it shall be processed as follows:

   a. Clear all keys from memory
   b. Read the DB for all encryption keys as necessary and load into memory
   c. Construct an appropriate response and send it
   d. Log a message using the standard Mojaloop logging processing stating the keys have been refreshed

5. Status

   A command may be sent to the CPM requesting it to send the status of the system, including statistics on what has been processed. When this command has been received it shall be processed as follows:

   a. Send a command to all adaptors requesting their status
   b. Set a timer for each message sent
   c. Wait for responses from each adapter
   d. When a response is received delete the timer set.
   e. When a timer expires set the status for that adapter as “Unknown”
   f. When all responses have been received the status response will be constructed
      i. All Adapters and CPM
         - Name
         - Status – Active, Stopped, Unknown
      ii. Command Adapter
         - Number of each valid command
            - ❖ Success
            - ❖ Failed
         - Number of each invalid command
      iii. Key Update Adapter
         - Number of valid Updates
            - ❖ Success
            - ❖ Failed
         - Number of invalid Updates
      iv. Software Security Adapter
         - Number of each valid encryption type
            - ❖ Success
            - ❖ Failed
         - Number of each invalid encryption
      v. Hardware Security Adapter
         - Name of HSM
         - HSM Type
            - Number of each valid encryption type per HSM
               - ❖ Success
               - ❖ Failed

- Number of each invalid encryption

vi. CPM

- Commands
  - Number of each command
    - ❖ Success
    - ❖ Failed
- Key Updates
  - Number of each update per FSP
    - ❖ Success
    - ❖ Failed
- Encryptions
  - Number of each type of encryption per FSP per adapter
    - ❖ Success
    - ❖ Failed

6. The appropriate counters will be updated whenever a message is processed

Key Updates

In order to ensure the integrity of the system and to protect the data travelling through the system certificates and key for different FSPs may need to be updated at the CPM as required. This will be done via a key update message which will enable the CPM to update its data base. An update and a Add will be treated the same when processing. When a key update arrives at the CPM it will be processed as follows

1. If the key update is an Add or Update
   a. Check the key does exist in the DB
      i. Make a backup copy of the key, suffix the key name with the date_time
      ii. Update the key with the new key, date time updated, source of command added to the changed by
      iii. If the key had previously been deleted it must be marked as active
   b. If the key does not exist in the DB the new key must be inserted ensuring the date added is the current date time and added by is the source of the command.
2. If the key update is a delete then the key must be marked as deleted, date_updated updated with the current date and time and updated_by set to the source of the command
3. Once processing has been completed the copy of the key in memory must either be update in the case of an Add or Update, or removed from memory in the case of a Delete
4. Once processing on the Key Update has been completed a message logged using the standard Mojaloop logging processing stating the key was updated/added or deleted as applicable.
5. The appropriate counters will be updated whenever a message is processed

Message Encryption/Decryption

While many ancillary services will be performed by the CPM it main function will be to perform Encryption/Decryption or Signing/Verification of data and messages. These

messages will come directly from the Mojaloop system it is providing services to. Once a message has been received by the CPM the processing will be driven as far as possible by configuration. This will enable new security devices and FSPs to be implemented with little or no downtime. During the process steps the general term encryption will cover all types of security processing which may be, but not limited to Encryption, Decryption, Signature Verification and Signature Creation.

When a message has been received it shall be processed as follows:

1. When a message arrives the FSP and encryption type will be extracted.
    a. If these cannot be exracted an appropriate decline response message will be constructed and sent back to the Mojaloop system.
    b. A message will be logged using the standard Mojaloop logging processing stating there the FSP and encryption type could not be extracted.
2. The adapter processing table will be searched for a match on these fields and the adapter name which will process this security operation.
    a. If a match is not found an appropriate decline response message will be constructed and sent back to the Mojaloop system.
    b. A message will be logged using the standard Mojaloop logging processing stating there was no match for the desired processing.
3. When a match is found the name of the adapter is extracted
4. The status of the adapter will be checked
    a. If the adapter is not found to be in a state where it can process the transaction an appropriate decline response message will be constructed and sent back to the Mojaloop system.
5. A security operation message will be constructed from the input message
6. The security message is then sent to the security adapter for processing
7. A timer is started while waiting for a response
8. When a response is received the timer is cancelled and the appropriate response message is constructed and sent back to the Mojaloop system
9. Should a timer expire an appropriate declined response message is constructed and sent back to the Mojaloop system
10. If a response is received after a timer has expired and a decline message sent the response will be ignored.
11. The appropriate counters will be updated whenever a message is processed

Shutdown

When a shutdown command has been received the CPM shall do the following

1. Set its state to “Shutting Down”
2. Stop accepting
    a. New transactions
    b. New Commands
    c. New Key updates
3. Send a “Shutdown” command to all adaptors
4. A timer set to wait for a response from the adapter
5. Complete all transactions it is current processing

6. Once all transactions have completed and/or the timers have expired the CPM will disconnect all its connections
7. A message will be logged using the standard Mojaloop logging processing stating the CPM is shutting down
8. Connections to the Data Base will be cleared
9. The CPM will shutdown

NOTES:
Should any new transactions or messages be received while the CPM is in a “Shutting Down” state these must be declined with the appropriate error message.

Software Security Module Adapter

Overview

The software security adaptor will accept transactions from the CPM and process them internally in the same way that the current Mojaloop system process security transactions. The SSM will only process messages that are currently defined in the Mojaloop Encryption document as defined in the References section. Transactions that may affect the PCI status of any organisation will not be processed by software encryption and must be processed in hardware to meet all accepted standards.

Start-up

When the process starts up it read the DB for its parameters as follows:

1. Port on which it must listen for connections.

Once the configuration has been read the adapter shall listen on the configured port and set its status to “Active” and pass processing to the main section

Processing

The following is the processing of a transaction until a use case has been identified for hardware processing.

1. Accept a message from the CPM
2. If the Adapter is not on an Active state an appropriate decline response message constructed and a response sent to the CPM
3. Validate the input message
4. Validate the adapter is mandated to process the type of encryption needed to complete the transaction.
5. Depending on the type of encryption to be performed the message will be processed in accordance with the Encryption document as specified in the References section
6. Build the appropriate message to the CPM and respond
7. The appropriate counters will be updated whenever a message is processed

Shutdown

When a shutdown command has been received the Adaptor shall do the following

1. Set its state to “Shutting Down”
2. Stop accepting
    a. New transactions
    b. New Commands
3. Complete all transactions it is current processing

Should any new transactions or messages be received while the Adaptor is in a “Shutting Down” state these must be declined with the appropriate error message.

Once all transactions have been completed the state will be set to “Inactive”, a message must be logged using the standard Mojaloop logging processing stating the Adaptor has shut down all connections to databases will be closed and the service shutdown.

Hardware Security Module Adapter

Overview

The Hardware Security adaptor will be used where a stronger level of security is needed when software encryption cannot the required level of encryption required or by not using hardware or where the use of software encryption would compromise the PCI status of an organisation. Where encryption is needed that is not supported by a hardware vendor the hardware vendor will be approached with a view to implementing the required commands into their offering.

An adaptor can have several HSMs defined to it, as long as devices operate under the same master keys and command set. Should more than one device be defined the devices will eb used in a round-robin format

Start-up

When the service starts up it will read in its configuration from the DB as follows

1. Port on which it must listen for connections
2. HSM common name
3. IP and Port for each device
4. HSM Specific details

Once the configuration has been read in the Adaptor will do the following

1. For each device
    a. Connect to device
    b. Once connected send a status/health message to confirm device is ready to process transactions

c. Log a message using the standard Mojaloop logging processing stating the HSM is ready for transactions
d. Add HSM details to a table stating it is active and ready for transactions

2. Set up a listen on the desired port

Once all the configuration has been successfully processed and successful passed all self-checks the Adaptor will set itself into “ACTIVE” state and hand control processing to the main processing module. A message must be logged using the standard Mojaloop logging processing stating the adapter is ready to accept transactions

Processing

Internal Processing

At all times will either processing massages or waiting for new messages the Adaptor will process a series of health checks as follows:

Based on the interval set in the configuration a health message will be constructed and sent to each HSM the Adaptor has a connection to. If a successful response is received a memory entry will be updated stating the HSM is Active and the time of the message. Should this be the first HSM to become Active and after the Adaptor has been marked Inactive, the adapter will now be marked as Active and start accepting transactions from the CPM.

Should the message be unsuccessful the HSM will be marked as Inactive and will not be used for processing transactions until it has been marked as successful. After 3 consecutive un-successful messages the connection will be closed and re-established. Should all HSMs become Inactive at the same time the status of the Adaptor will be set to Inactive and will not accept transactions from the CPM until it has an Active HSM.

Transaction Processing

The following is the base processing of a transaction until a use case has been identified for hardware processing.

8. Accept a message from the CPM
9. If the Adapter is not on an Active state an appropriate decline response message constructed and a response sent to the CPM
10. Validate the input message
11. Validate the adapter is mandated to process the type of encryption needed to complete the transaction.
12. Construct a HSM message based on the input message
13. Choose the appropriate HSM to process the message
14. Send the message to the selected HSM
15. Accept the response from the HSM
16. Build the appropriate message to the CPM and respond
17. The appropriate counters will be updated whenever a message is processed

Shutdown

When a shutdown command has been received the Adaptor shall do the following

1. Set its state to “Shutting Down”
2. Stop accepting
    a. New transactions
    b. New Commands
3. Complete all transactions it is current processing

Should any new transactions or messages be received while the Adaptor is in a “Shutting Down” state these must be declined with the appropriate error message.

Once all transactions have been completed and responded to,

1. All HSMs will be disconnected
2. The state will be set to “Inactive”,
3. All connections to DBs will be closed
4. The service shutdown.

Key Update Adapter

Overview

Should a Key Management System not be available to either an FSP or the Mojaloop instance an organisation will be able to update their keys or certificates by sending a message to the CPM in order that the latest keys/certificates may be used. The Key Update Adaptor will accept these messages and pass them onto the CPM for processing, while managing the connections and flow of messages to the organisations connecting to it

Start-up

When the service starts up it will read in its configuration from the DB as follows

1. Port on which it must listen for connections
2. IP and port on which it must connect to the CPM

Once the configuration has been read in the Adaptor will do the following

1. Connect to the CPM
2. Set up a listen on the desired port for inward connections

Once all the configuration has been successfully processed and successful passed all self-checks the Adaptor will set itself into “ACTIVE” state and hand control processing to the main processing module. A message must be logged using the standard Mojaloop logging processing stating the adapter is ready to accept transactions

Processing

Once the Adaptor has successful started the Key Update Adaptor will wait for a command to arrive. After the Adaptor has received a transaction the following

1. Check the status of the Adaptor and if is in “Shutting Down” state the command will be declined and the appropriate response returned.
2. If the status is “Active” the Adaptor will check it is a valid key update message from an external source or an internal command from the CPM.
3. If the transaction is a shutdown command from the CPM the adapter will perform the shutdown as per the process in the Shutdown section command.
4. If the transaction is a command from the CPM, but not a shutdown command an appropriate response will be returned CPM and a message must be logged using the standard Mojaloop logging processing stating an invalid command was received. No further action taken on the transaction.
5. If the transaction is from an external source it must be validated to be key update command by ensuring the action to be taken is “Add”, “Update” or “Delete” Should it be determined that it is not a valid key update command an appropriate response will be returned source and a message must be logged using the standard Mojaloop logging processing stating an invalid transaction was received. No further action taken on the transaction.

6. Once it has been determined that id it a valid key update transaction the message will be reformatted into the correct internal format and sent on to the CPM for processing.
7. Once a response is received from the CPM it will be formatted into a response message with the appropriate response code and responded back to the sent to the source.
8. The appropriate counters will be updated whenever a message is processed

Shutdown

When a shutdown command has been received the Adaptor shall do the following

1. Set its state to “Shutting Down”
2. Stop accepting
    a. New transactions
3. Complete all transactions it is current processing

Should any new transactions or messages be received while the Adaptor is in a “Shutting Down” state these must be declined with the appropriate error message.

Once all transactions have been completed and responded to

1. The Adaptor will disconnect from the CPM
2. The state will be set to “Inactive”,
3. All connections to DBs will be closed
4. A message must be logged using the standard Mojaloop logging processing stating the adapter is shutting down
5. The service shutdown.

Command Adapter

Overview

To effectively control the system there must be the ability to accept commands to control various aspects of the system. Through these commands the system will be able to control the refresh key and start or stop different aspects of the system.

The acceptable commands are:

1. Shutdown – This will enable the CPM to shut down either the entire system or single instance of the system
2. Startup – This will enable the CPM to start up parts of the system that has previously been shut down. The exception to this is if the CPM is not running that the command adapter will be able to start the CPM
3. RefreshKeys – This will result in all keys held in memory to be refreshed from the database.
4. RefreshConfig (”Adaptor Name”) – This will cause either the CPM or an adapter to refresh its config and if necessary make any necessary running changes. This could be for instance adding or deleting an adapter or adding/deleting an HSM in the case of an adapter.
5. Status – This will return statistics and status of the system

Start-up

When the service starts up it will read in its configuration from the DB as follows

1. Port on which it must listen for connections
2. IP and port on which it must connect to the CPM

Once the configuration has been read in the Adaptor will do the following

1. Connect to the CPM
2. Set up a listen on the desired port for inward connections

Once all the configuration has been successfully processed and successful passed all self-checks the Adaptor will set itself into “ACTIVE” state and hand control processing to the main processing module. A message must be logged using the standard Mojaloop logging processing stating the adapter is ready to accept transactions

Processing

Once the Adaptor has successful started the Command Adaptor will wait for a command to arrive. After the command has arrived the following procession will be done

1. Check the status of the Adaptor and if is in “Shutting Down” state the command will be declined and the appropriate response returned.
2. If the status is “Active” the Adaptor will check it is a valid command. If the command is invalid the command will be declined and the appropriate response returned. A

message must be logged using the standard Mojaloop logging processing stating a command was sent to the adapter
3. If the source of the command is not the CPM the message the message will be reformatted as necessary and sent onto the CPM.
4. When a response is received from the CPM for this command it shall be formatted into the external format as necessary and a response sent back to the sender of the command.
5. If the source of command is CPM and “Shutdown” the shut down routine as per the Shutdown section performed.
6. If the source of command is CPM and “RefreshConfig” the Adaptor will refresh it configuration and perform any changes, as necessary.
7. If the source of the command is CPM and not one of the above commands the command will be declined, and the appropriate response returned.
8. The appropriate counters will be updated whenever a message is processed

Shutdown

When a shutdown command has been received the Adaptor shall do the following

1. Set its state to “Shutting Down”
2. Respond to the CPM that message was received
3. Stop accepting
    a. New transactions
4. Complete all transactions it is current processing

Should any new transactions or messages be received while the Adaptor is in a “Shutting Down” state these must be declined with the appropriate error message.

Once all transactions have been completed and responded to

1. The Adaptor will disconnect from the CPM
2. The state will be set to “Inactive”,
3. All connections to DBs will be closed
4. A message must be logged using the standard Mojaloop logging processing stating the adapter is shutting down
5. The service shutdown.

Message formats to be completed

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

Database Configurations

The following is the configuration needed to be held in the Data Base

Adapter Configuration

1. Adapter Name
2. Adapter Type (Command, Key Update, Security)
3. Adapter IP
4. Adapter Port
5. Adapter Specific Information
6. Data base connection details

Hardware Security Module Configurations

1. Adapter Name – Key
2. HSM type – Informational
    a. HSM1
        i. Name
        ii. IP
        iii. Port
        iv. Header type
        v. Priority
        vi. Health Message interval (seconds) – 0 = no health message
        vii. Message timeout
        viii. HSM Specific information
    b. HSM..n
        i. Name
        ii. IP
        iii. Port
        iv. Header type
        v. Priority
        vi. Health Message interval (seconds) – 0 = no health message
        vii. Message timeout
        viii. HSM Specific information

Software Security Module Configurations

1. Adapter Name – Key
2. Security Module Specific information

Security Message Routing Configuration

1. FSP name - Key
2. Encryption type – Key
3. Enabled – True/False

4. Adapter Name

Command configuration

1. Adapter Name
2. Whitelist IPs
3. User
    a. User ID
    b. User Group
4. User Groups
5. Commands per group

CPM Configuration

1. Common Name
2. Port to Listen on for connections
3. Data base connection details

Key Configuration

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