Gysi Solutions Pty Ltd

Cryptographic Processing Module

High Level Overview

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 a high-level design and description of the system which will enable a detailed design to be documented and developed based on the principles described in this document.

The principles already accepted by the Mojaloop community will be applied to the cryptographic module. These are

1. We shall not prescribe to the Mojaloop community of any external hardware or software to be used, but rather provide a set to tools to interact with several possible solutions, and make recommendations where necessary
2. The use of internationally accepted standards will be used wherever possible
    a. KMIP
    b. PKCS11

The main processing module will determine what type of transaction is to be processed and via configuration be able to invoke the correct processing adapter. As necessary adapters will be added to the system as necessary to cater for new standards or new commands sets. Once the initial changes have been made to the current Mojaloop system to enable the CPM module the adding of any adapters or standards will not result in any changes to the core Mojaloop system.

References

This document references the following:

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

Glossary

Term	Definition
MAC	Message Authentication Cryptogram
FSP	Financial Services Provider
CPM	Cryptographic Processing Module
LPS	Legacy Payment System
PIN	Personnel Identification Number
OTP	One Time Pin
MAC	Message Authentication Cryptogram
HSM	Hardware Security Module
KMS	Key Management System
IKMS	Independent Key management System
KMIP	Key Management Interoperability Protocol

Assumptions

The following is a list of assumptions for this document

1. The high-level design will adhere to the principles where Mojaloop will not dictate external hardware or software to be used.
2. Any OTP that is encrypted by an LPS as a PIN Block will result in an encrypted OTP
3. Translation from a PIN block under a symmetric key to an OTP under an asymmetric key will be supported by the necessary hardware HSM vendors
4. The system will make use of any libraries or APIs provided by HSM providers to assist in the use of any approved standards, however this will only be documented in the next phase of design.

Exclusions

The following is a list of exclusions for this document

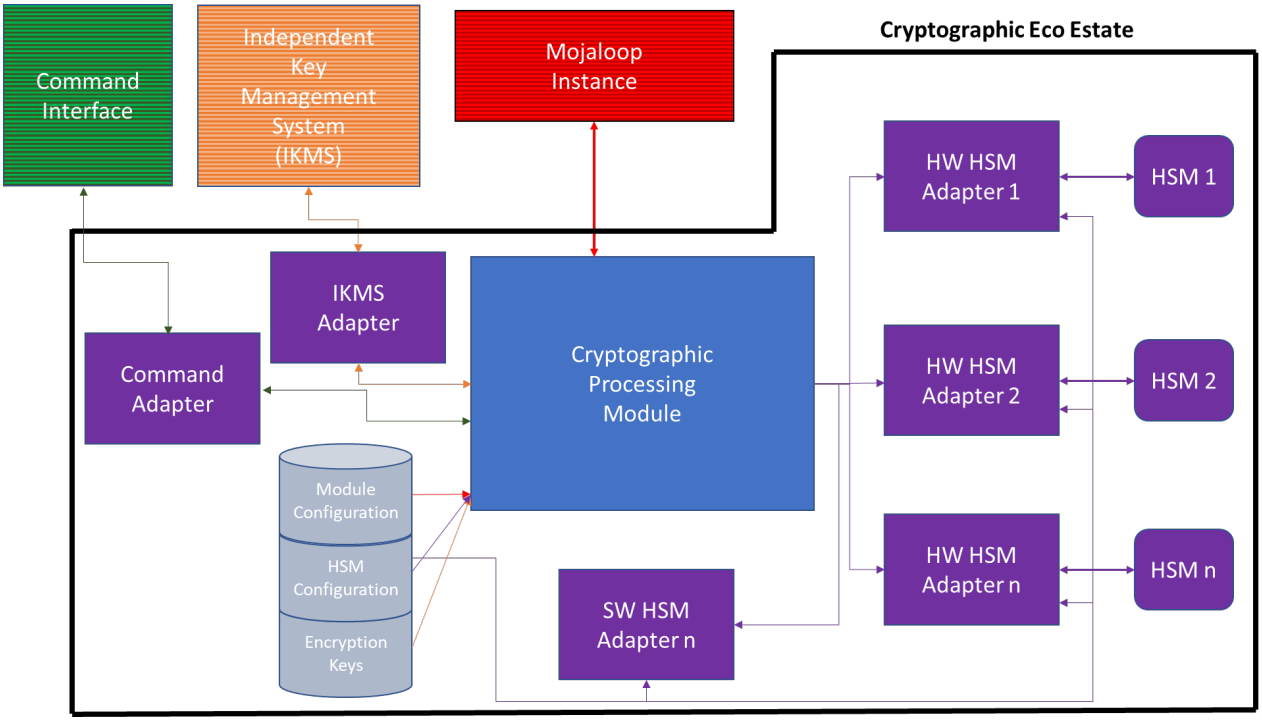
1. Documentation of creation and signing of any necessary certificates
2. Documentation of creation of any symmetric static keys
3. Any design of load balancing or failure of any component.

4. Translation from a PIN block under a symmetric key to an OTP under an asymmetric key will be not be supported under software

System

Overview

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



Components

The CPM will be designed and built in a modular way that should a new HSM or IKMS need to be incorporated into the system it will be done seamlessly and mainly through configuration. Whether the adapters are part of the CPM module or separate executables will be decided in either the full design phase or as part of the technical design.

Cryptographic Processing Module

The CPM will control all aspects of processing and will execute the adapters as necessary based on configuration. It will form the bridge between Mojaloop and the processes that will perform any security operations. The CPM will also, via a IKMS adapter ensure that all keys are kept up to date, or if necessary, control a refresh of keys.

HSM Adapters

Software

An adapter will be developed that will allow most security operations to be performed via software where these operations will not affect any certifications that the system connected to Mojaloop may need to adhere to. If an organization running Mojaloop wishes to use this option in a production environment it must understand the risks associated with it.

Hardware

Several hardware adapters depending on the decisions taken during the next round of designs. These adapters will either use PCKS11 libraries provider by HSM providers or will use the propriety message formats supported by the physical HSMs. Although not shown in the system overview the adapters will be capable of holding connections to several physical HSMs and will either round robin between them or work in an active/passive role depending on configuration. If during the low-level design, a necessary security operation is needed but not available by a HSM provider discussions will be held with that provider to ascertain if they can provide it.

IKMS Adapters

An adapter will be developed to interface with external KMS systems in order to either ask for the latest instance of cryptographic keys or to accept a new key that has been updated. A decision has been accepted that in the initial phase that only KMES systems that adhere to the KMIP standard will be catered for. Should an organization which to use an IKMS that does not adhere to the KMIP standard this will be catered for on a case by case basis.

Commands Adapter

There will be instances when a command will need to be sent to the CPM to instruct it to perform certain functions, for example refresh keys, change logging levels or refresh configuration. An adapter will be developed to accept these commands. This will give the CPM

Use Cases

The Use Cases that have been identified fall into 2 categories, Online Processing and Key Management Processing. These use cases are as follows:

Online Processing

Based on the current message flow, Mojaloop Use Cases and business rules the following use cases have been identified

Message Signature Creation

All messages from Mojaloop should be signed before they are sent on to an entity in order that all parties can be assured that any message sent by Mojaloop is authentic and unaltered.

To ensure this the CPM will provide the ability to sign messages as per the Encryption document.

Message Signature Verification

Any messages sent to Mojaloop may be signed by an entity before sending to assure that any message sent to Mojaloop is authentic and unaltered.

To ensure this the CPM will provide the ability to verify any messages received based on the signature as per the Encryption document.

Data Field Encryption

With the adherence to international privacy standards some FSPs will want to protect sensitive data by encrypting it while in flight between Mojaloop and the FSB. This will be a case by case basis and will be by agreement between the two parties.

The CPM will provide the ability for Mojaloop to encrypt these individual fields as per the Encryption document.

Data Field Decryption

With the adherence to international privacy standards some FSPs will want to protect sensitive data by encrypting it while in flight between Mojaloop and the FSB. This will be a case by case basis and will be by agreement between the two parties.

The CPM will provide the ability for Mojaloop to decrypt these individual fields as per the Encryption document after the receiving the message form the other party

Encrypted Data Field Translation

With the adherence to international privacy standards some FSPs will want to protect sensitive data by encrypting it while in flight between Mojaloop and the FSB. This will be a case by case basis and will be by agreement between the two parties.

Under certain circumstances by mutual agreement this data will need to be encrypted on both legs of the transaction (in and out) and should not be held in the clear at any point in the transaction and therefore will need to be translated from one key to another, rather than decrypted and then encrypted.

The CPM will provide the ability for Mojaloop to perform a data translation on these individual fields as per the Encryption document before sending the message on to the other party

Symmetric Key Importing

When transactions are being accepted by an LPS to be processed by Mojaloop for interaction with a FSP some transaction may carry a PIN, have encrypted fields or have a MAC on the message. In order to be able to process these transactions the adapter will perform a key exchange with the LPS as necessary for each type of key depending on the configuration.

Pin Translation from Symmetric to Asymmetric Key

For LPS systems that have encrypted the OTP as a PIN block, the incoming PIN block will need to be translated from a PIN block under a symmetric key to a encrypted OTP under an asymmetric key

MAC Verification

Similar to the verification of a Mojaloop message under an asymmetric key, messages from an LPS may be configured to carry a MAC which must be verified by the adapter when it receives the message to ensure its integrity. Once the MAC has been verified the message will be processed as normal

MAC Creation

Similar to the signing of a Mojaloop message under an asymmetric key, messages being sent to an LPS may be configured to carry a MAC which must be created by the adapter before it the message to ensure its integrity.

Key Management Processing

Accepting a new key from an IKMS

When an external KMS has changed a key the properties of a key the key will need to be updated in the systems which need to use that key. These properties could cover many

circumstances for example, a new value for the key, new valid dates or the key has been revoked for any reason. Some KMS will be able to notify the required systems of these changes and the CMP will accept this new key, update itself in memory as well as updating it database.

Refresh keys as needed

Under certain circumstances keys may become out of sync with the other party involved in a security operation. Under these circumstances or start-up, the CPM will either communicate with an IKMS to obtain the most recent keys or refresh the keys in memory from its database.

Processing

The processing will be controlled by the Cryptographic Processing Module (CPM) but will be broken done into three main areas. While each area will have specific processing all communication with Mojaloop system by the central processing are of the CPM.

Startup

When the CPM starts up it shall go through an initialization phase where the CPM's configuration shall be read, and the system set up as per the configuration. Once all start up process have been successfully completed the necessary connections will be made to the Mojaloop system

Key Management

If an external Independent Key Management System (IKMS) is configured to the system a connection shall be made to the system and all necessary keys as per the CPMs database retrieved form the KMS. If no external KMS is configured the database shall be checked to ensure all defined keys are valid

If no connection can be made to the IKMS the system shall be started on the current defined keys, and regular attempts made to connect to the IKMS to update the system with the most recent keys. Once the system has been updated with the latest keys processing shall continue as normal

HSMs

A single CPM may make use of several different HSM adapters to process different security messages. During the Start Up phase the details of each HSM type shall be read into the system and setup as required. A connection will be made to each physical HSM and if the protocol permits it a health message sent to each HSM

Online Security processing

When the CPM receives a request from the Mojaloop it will check the processing request is a valid request for the installation as well as the FSP or LPS. If the request is not validated a decline message will be formatted and the response sent back to the Mojaloop system. Once the CPM has validated the request the correct adapter to process the transaction will be identified and invoked with the necessary inputs.

Once an adapter has received a request it will either process it internally if it is software adapter or build the correct message to be sent to a physical HSM. Once the message has been processed the appropriate response will be returned to the CPM.

Once the CPM has received a response the response shall be interrogated, and the appropriate action taken as follows:

1. If successful, all necessary error counters reset and a response returned to Mojaloop
2. If the transaction is declined due to a key issue the appropriate error counter increased. If the configurable threshold met or exceeded the CPM will attempt to refresh the keys from the KMS. An error message logged that the keys are being refreshed and a response returned to Mojaloop.
3. If the transaction is declined for any reason other than keys a response will be returned to Mojaloop.

Separate to any transaction processing the HSM adapters will be able to send the necessary health check message to the HSM and should any errors be recorded the appropriate action taken.

Key Management

Once the system has started up and performed it startup processes key management will only be processed under certain conditions as per the use cases.

The key management adapter will wait to receive messages from an external source which will either be an IKMS sending new keys to replace the current keys, or a command to refresh the keys.

Should an IKMS send new keys the adapter will accept these keys and update both the database with the new values as well as update memory with the new values. Should an error be encountered while performing these actions an error message must be logged. Once either the keys have been updated, or an error encountered the appropriate response returned to the IKMS.

Should a command be received to refresh the keys the CPM will either, based on the configuration, refresh it memory from the database, or pass control to an adapter which will communicate with an IKMS to obtain the latest keys. The command could come from an external source or from the internal online processing when the CPM detects a key may be out of sync.

Once the latest version of the keys has been obtained the data base will be updated and memory refreshed.

After the necessary processing has been completed a response message to the received will be returned.