MOJALOOP CRYPTOGRAPHIC PROCESSING MODULE

Low Level Design - Use Cases

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

1. 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 the use cases that will catered for in the initial version of the CPM

2. References

This document references the following:

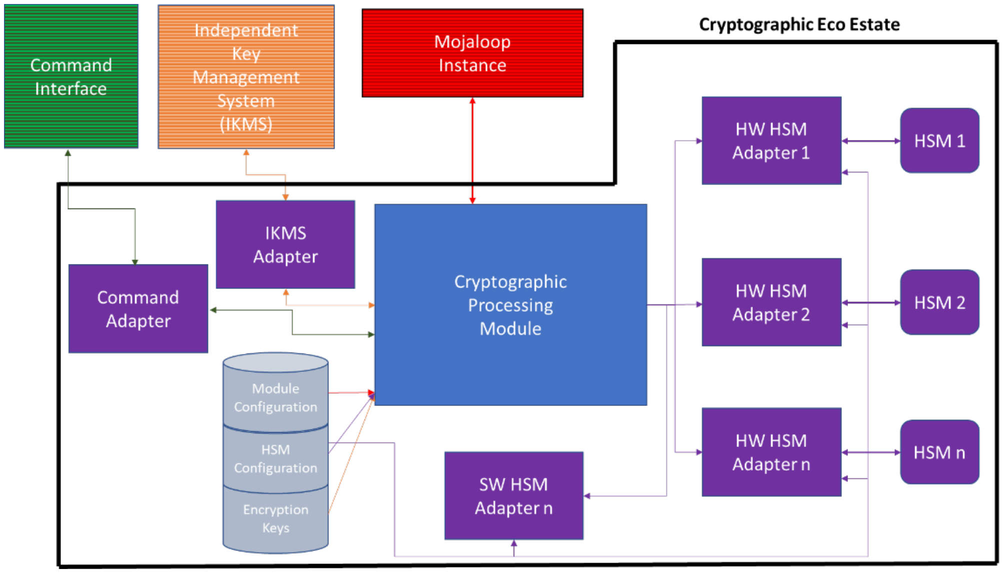
Nr.	Title and Version	Author	Comments
1	Use Cases V1.0	Mojaloop	
2	Encryption V1.0	Mojaloop	Initial Version
3	Mojaloop CPM LLD Highlights	Max Gysi	Version 0.1

3. Glossary

Term	Definition
FSP	Financial Services Provider
CPM	Cryptographic Processing Module
LPS	Legacy Payment System

4. System

For informational purposes only a high-level system diagram of how the Cryptographic Eco Estate will be constituted is shown below.



5. Use Cases

In the Mojaloop CPM LLD Highlights document a sub-set of the uses cases described in the Mojaloop Cryptographic Processing Module document are extracted for inclusion in the initial version of the CPM

These use cases are as follows:

5.1 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.

Currently there are two instances where this will be required.

1. If Mojaloop encrypts a field, then the payload needs to be signed
2. If a message comes in from a system outside the Mojaloop ecosystem, e.g. from an LPS, the payload needs to be signed before forwarding it on to a FSP

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

5.2 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.

Before any processing is performed on the message, especially if fields need to be decrypted, the signature needs to be verified.

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

5.2 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.

Once the field itself has been encrypted, the message will be signed in accordance with the Encryption Document, Section 3.2

5.2 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 signature of the payload will be verified prior to the decryption of the necessary fields in accordance with the Encryption Document, Section 3.3

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