mojaloop

Code Quality & Security (CQS) Work Stream Updates

PI-11 PI Feedback Session – 21 October 2020

Presenters

Godfrey Kutumela
Program Manager & Lead Architect, Crosslake Technologies

Victor Akidiva
Security Architect, ModusBox

Max Gysi
Director, Gysi Solutions

Code Quality & Security Work Stream Overview

Objective:

- *Continuously improve the Trust (reliability, transparency, privacy, quality and security)* of the Mojaloop System.

Delivery Model:

- Supports both *functional and non-functional* requirements of the project, working alongside with other *workstreams & various governance committees o*n a *shared responsibility Model.*

Approach:

- Standards and Control Centric – Define and maintain Mojaloop software quality and security standards and guidelines – In certain areas we provide reference implementation.

- Risk and Threat Centric – Perform risk and threat modelling to identify, validate, classify & prioritize security requirements.

Key Milestones:

- PI 1 – 8 : Foundation Phase - Built-in confidentiality and Integrity as part of the Core Mojaloop Architecture.
  - ✓ Developed and Implemented (To some degree) Signatures, MTLS, PKI, encryption standards
  - ✓ Established a code quality and security framework - DevOps & CI/CD Tools automation, workflows & policies

- PI 9 – Current: Improvement Phase – Consolidate, optimize & improve.
  - ✓ Introduced a risk and threat driven approach
  - ✓ Baselining Mojaloop against best practice standards – PCI DSS and GDPR
  - ✓ Focus on the data – Data Protection Standards and Introduction of a Cryptographic Processing Module (CPM)

Code Quality & Security (CQS) PI 11 Objectives

PI 11 objectives breakdown per epic

CQS Epic	Epic Objective (Multi-PI view)	PI 11 Objective
1. Functionality Support	Enhance security in new functionality additions	Review PISP and Portals security designs
2. Implementation Support	Support major implementations	Assist Mowali GDPR Compliance Initiative
3. Cryptographic Processing	Design a secure cryptographic processing module	Deployment Planning – Low Level Designs
4. Data Protection	Improve data protection measures and controls	Establish Data Protection and logging Standards
5. Standards Baselining	Baselining of Mojaloop against industry standards	Finalize PCI DSS and GDPR baseline reports
6. DevSecOps Integration	Maintain and enhance secure DevOps/CI CD practices	On going maintenance and enhancements
7. Community Engagement	Improve communication and community engagement	Restructure CQS documentation

Epics and PI objectives are sourced from:

- Input from product development teams
- Gap analysis by the CSQ core team
- Requests from implementors
- Requests from community contributors

DevSecOps Integration

PI objective – On going maintenance and enhancement of the DevSecOps processes, policies and tools and policies.

Completed:

1) Regular Security Patches + Updates – Regular Security Patches + Updates - August #1695
   - Addressing regular Dependabot alerts,
   - Running `npm audit` on flagged repos

Planned Enhancements for PI 11:

1) DevSecOps - Create a simple Security Alerts Dashboard #1398 - Simplify and summarize our security alerts into a single page.
   Investigating the possible use of Prometheus Github plug-in for data ingestion and Grafana for a monitoring dashboard
   The available of a Lab Testing Environment will fast track story in PI 12

PI 12 Backlog :

1. DevSecOps - Investigate EFK SIEM capabilities for central logging and security reporting #1680
2. DevSecOps - Investigate Kubernetes security improvements (Alignment to security best practice) #1682
3. DevSecOps - Review current kurbenates audit logging setup and report on findings #1681

Standards Baselining

PI objective – Baselining of Mojaloop against best practice standards starting with PCI DSS and GDPR.

Payment Card Industry Data Security Standard - PCI DSS

- Baseline assessment completed – with focus on the Cardholder Environmental (CDE) requirements (229)
- Developed a responsibility matrix to clearly segregate Mojaloop OSS and Hub Operator in-scope items
- PCI DSS cryptographic requirements were considered in the Cryptographic Processing Module Design

General Data Protection Regulations - GDPR

- Defined Mojaloop GDPR addressable scope
- Identified Personally Identifiable Information (PII) traversing the Mojaloop switch
- Evaluated the current PII protection measures and identified gaps

Next Phase will focus on:

- SOC Type I
- ISO27001
- NIST Cybersecurity Framework

DEFINITIONS:

- ❖ *The Payment Card Industry Data Security Standard (PCI DSS) is the global data security standard that any business of any size must adhere to in order to accept payment cards.*
- ❖ *The General Data Protection Regulation (GDPR) is a regulation in EU law on data protection and privacy in the European Union and the European Economic Area.*
- ❖ *Service Organization Control (SOC) defines criteria for managing customer data based on five “trust service principles”—security, availability, processing integrity, confidentiality and privacy.*
- ❖ *National Institute of Standards and Technology(NIST) Cybersecurity framework to measure organization’s preparedness in identifying, detecting, and responding to cyber-attacks*

Implementation Support – Mowali GDPR Initiative

Summary of the Data Protection Impact Assessment (DPIA) Findings

Identified PII	Purpose of processing PII	Access to PII	PII data protection measures and controls	The right to be forgotten rules
P2P Transfer same currency: • **Payee MSISDN** • **Payee Name**	• Payee MSISDN for Identifying the Payee DSFP • Payee Name for confirmation of account holder	• Switch • Payer DSFP	• IP whitelisting • Firewalling • Encryption in transit • Message Signing • Role based access controls • Authentication & • Authorization	As per data retention policy
P2P Transfer with Forex • **Payee KYC Data**	Regulatory compliance requirements for forex and cross-border transactions	• Switch • Settlement Bank	* Same as above	As per data retention policy
Settlement • **Payer MSISDN (Indirect PII)** • **Payee MSISDN**	Both Payer and Payee MSISDN are used as source and destination identifiers in the clearing and settlement reports.	• Switch • Payer and Payee DFSP's • Settlement Bank	• Access to settlement data is on a need to know basis	As per data retention policy

Comments:

- A data retention policy should strike the balance between the right to be forgotten requirement of GDPR with those of central bank's monitoring and oversight functions.
- Retained data should be used safely without compromising the right to be forgotten clause of GDPR incase where is has been invoked.

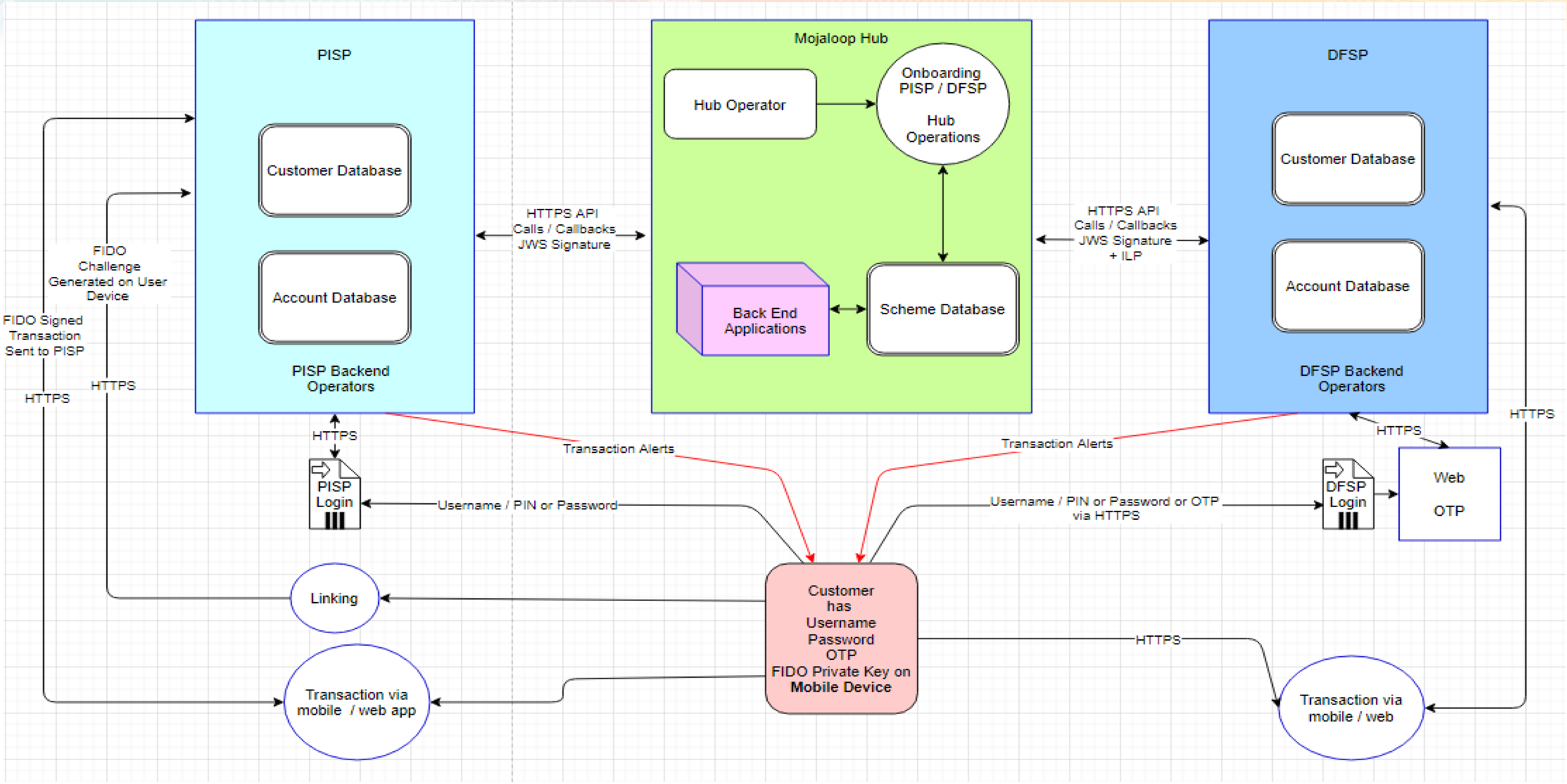
Proposed CQS Documentation Structure

Program Management - Business, Risks and Governance view	**Standards and Guidelines** - Design and Architectural view	**Reference Implementation** - Secure software engineering view
1) Mojaloop Data Security and Privacy Program: a) Program Overview b) Current PI Objectives c) PI Reports: 8 – 11 d) Vulnerability disclosure procedure 2) Scheme Rules Risk Management Guidelines: 3) a) Risk Management, Security, Privacy and Data Confidentiality 4) Standard Baselining a) GDPR Scoping Analysis Report b) PCI DSS Baseline report and recommendations – Responsibility matrix (Hub/Switch)	1) Design Principles a) Coding Standards 2) Scheme Trust Architecture a) Encryption Standard b) Signature Standard c) PKI Best Practice Standard d) Secure Interledger design 3) Data Protection Standards a) Secure Kafka and Zookeeper Standard b) Secure Logging and Auditing Standard c) Personal Identifiable Information (PII) Threat Models and Data Classification Reports 4) Security Architectural Reviews a) Mojaloop Portals b) PISP Linking and Transfer Flows	1) Architectural Implementations a) Message signing b) Message Encryption c) cryptographic receipt d) Secure PISP account linking e) Certificate Management (MCM) 2) Code level security measures a) Open Source Vulnerability Management i. NPM b) Open Source License Management - NPM Audit c) Static Code Analysis – SonarQube d) Container Security i. Anchore-cli ii. AppArmor 3) CI/CD Automation Process – Security Gates and Policies

Functionality Support and Data Protection Epics Update

By Victor Akidiva

PISP Data Flow Diagram


PISP
Customer Database
Account Database
PISP Backend Operators
Mojaloop Hub
Hub Operator
Onboarding PISP / DFSP
Hub Operations
Back End Applications
Scheme Database
DFSP
Customer Database
Account Database
DFSP Backend Operators
HTTPS API Calls / Callbacks JWS Signature
HTTPS API Calls / Callbacks JWS Signature + ILP
FIDO Challenge Generated on User Device
FIDO Signed Transaction Sent to PISP
HTTPS
HTTPS
HTTPS
PISP Login
Transaction Alerts
Transaction Alerts
Username / PIN or Password
Username / PIN or Password or OTP via HTTPS
DFSP Login
HTTPS
Web
OTP
HTTPS
Linking
Customer has Username Password OTP FIDO Private Key on Mobile Device
HTTPS
Transaction via mobile / web app
Transaction via mobile / web

PISP linking process STRIDE summary

COMPONENT	S	T	R	I	D	E
Pre-linking	X	X				
Discovery	X	X		X		
Request consent	X	X	X	X	X	
Authentication - Web	X	X	X	X	X	X
Authentication - OTP/SMS				X		
Grant consent	X	X	X	X	X	X
Credential registration	X	X	X	X	X	X

<u>STRIDE Analysis summary:</u>

1. The linking process could be spoofed by rogue PISP to enumerate DFSP users.
2. In addition it may be possible for a rogue PISP to simulate a user and complete end to end credential registration and credential registration (they will need to have somehow obtained user DFSP credentials i.e. through Social Engineering).
   a. OTP based credential generation process is complete and mitigates the above risk.
   b. Residual risk with web based DFSP authentication means its possible for rogue PISP to simulate user and attempt to log in (including brute force attacks) and credential theft attacks with fake login page(s).

PISP Linking process Review Summary

PI objective – Security review of the PISP (**linking** process) designs and ensure alignment with other CQS initiatives.

1. PISP - Core Functionality Support - PISP Initiation and Transfer Flows Security Review #1589

Completed:

- Detailed review and analysis of the PISP Linkage Flows (Tri-party Trust Model)
- Detailed review and analysis of the PISP transaction flow process
- Identified areas of possible adjustments and further research – Authentication and Consent Management process

Key recommendations:

- Ensure PISP (and DFSP) sends alert to users upon completion of consent process
- Review FIDO credential security exchange between user and PISP during linkage process that could possibly result in man in the middle attack (Ref section 1.6 in PISP Linking Process).
- There needs to be a way for the end user app to verify that the URL presented by PISP is the actual URL generated by DFSP. If possible, sending of this URL should bypass PISP. (Ref section 1.3.1 in PISP Linking Process).
- Ensure OTP for consent are not transferrable nor reusable within the consent / transaction process.
- PISP and DFSP need to invest in device fingerprinting libraries to authenticate both **device+user** during registration process for nonrepudiation.

PISP transfer process STRIDE summary

COMPONENT	S	T	R	I	D	E
Discovery	X			X		
Agreement	X			X		
Transfer	X			X		

STRIDE Analysis summary:

The transfer process could be spoofed by rogue PISP to enumerate DFSP users. However due to FIDO Challenge that uses private key on user mobile device the rogue user will be unable to sign the challenge thus cannot transact as the user. Residual risk is Spoofing and information disclosure.

Next Steps - Further Research on private key storage and security on user mobile app

The FIDO credential is a critical component of the PISP transaction process. This key is created by the mobile application designed by the PISP but will be stored on the user mobile device. We need to ascertain that there is no possibility that the PISP can programmatically access the private key via the PISP mobile app on the user device. If this key is compromised, then the holder can sign transactions as the user fraudulently.

PISP Transaction process Review Summary

PI objective – Security review of the PISP (**transaction** process) designs and ensure alignment with other CQS initiatives.

1. PISP - Core Functionality Support - PISP Initiation and Transfer Flows Security Review #1589

   Completed:

   - Detailed review and analysis of the PISP transaction flow process
   - Transaction data flows security proposed controls were **satisfactory** for PISP end to end process

   Key recommendations:

   - Ensure security of keystore embedded within the user mobile device that will store the private key used to sign FIDO challenge for transactions.
   - Possible security testing to be done on SDK that is to be embedded in Mobile APPs that will provide functionality for **Mobile App -> PISP -> Hub** communication via APIs. This will be developed by PISPs / DFSPs.
   - PISP and DFSP need to invest in device fingerprinting libraries to authenticate both **device+user** during registration process for nonrepudiation.

Onboarding Portals STRIDE summary

COMPONENT	S	T	R	I	D	E
External entity (users)	X		X			
Process	X	X	X	X	X	X
Data Flow		X		X	X	
Data Store		X	X	X	X	X

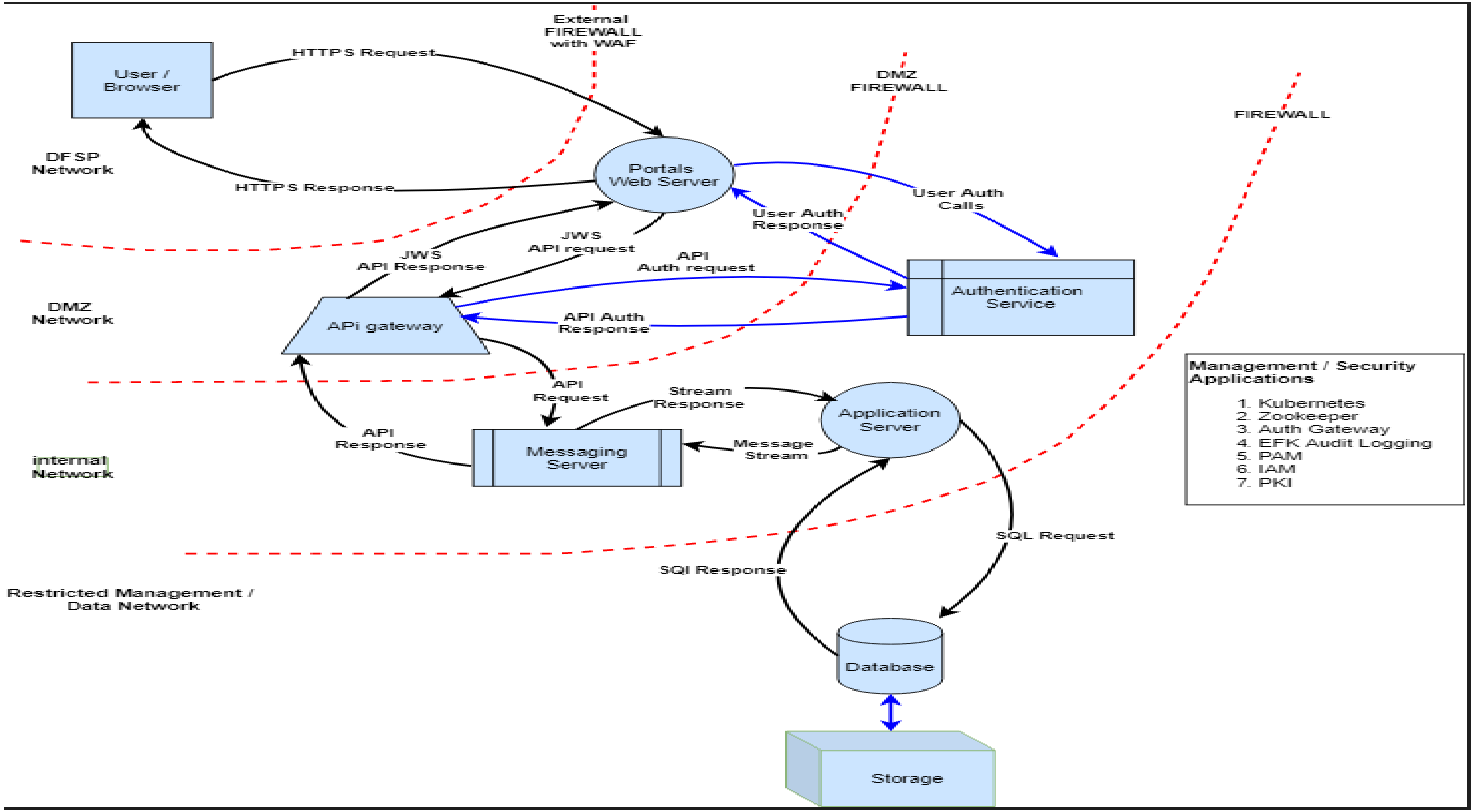
STRIDE Analysis summary:

1. The transfer process could be spoofed by rogue PISP to enumerate DFSP users. However due to FIDO Challenge that uses private key on user mobile device the rogue user will be unable to sign the challenge thus cannot transact as the user. Residual risk is Spoofing and information disclosure.

Next Steps

1. Explore federation policies that will support Portals deployment in test area with WSO2.

Portals Data Flow Diagram



Management / Security Applications

1. Kubernetes
2. Zookeeper
3. Auth Gateway
4. EFK Audit Logging
5. PAM
6. IAM
7. PKI

Onboarding Portals Review Summary

PI objective – Security review of the Portals designs and ensure alignment with other CQS initiatives - Core Functionality Support - Mojaloop Portals for Hub Operations Design Review #1576.

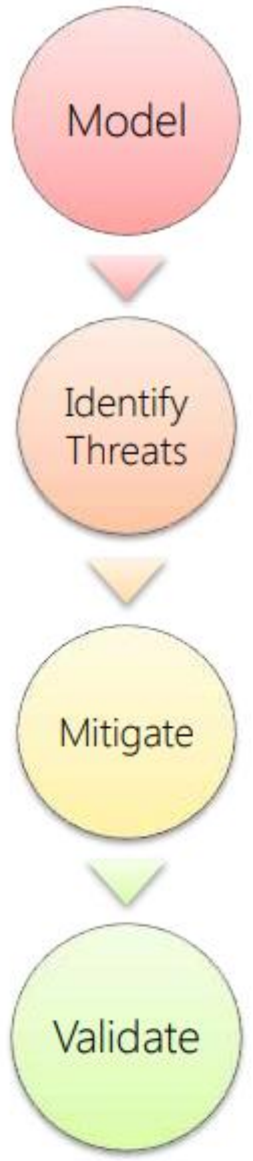
1. Portals - The portals application acts as single pane gateway to critical services in Mojaloop backend, on this note it is classified as a high-risk application.

   Completed:

   - Developed STRIDE based threat modelling process.
   - Detailed review and analysis of the Portals proposed design using STRIDE model
   - Identified areas of possible adjustments

   Key Recommendations:

   - Incorporate web application firewall / reverse proxy in design to protect Portals frontend from layer 7 attacks
   - Support DMZ design with web services published from DMZ and back end applications protected behind DMZ firewall
   - Document role profiles to be incorporated in federated identity management process (further research depending on IDM solution to be used)
   - Implement a reporting services architecture for Mojaloop (data warehouse) control and regulate database load from report queries over and above normal transactional data



Audit logging standard

Objective – Document a security logging standard for Mojaloop to ride on the event framework

Value to Mojaloop – Standardized security logging format for all Mojaloop components. Support implementation of audit log in event framework.

Findings from Log Analysis of Mojaloop logs:

- Audit logs create records that help you track access to the Mojaloop environment. Therefore, a complete audit log needs to include, at a minimum all or a combination of:
  - Audit log trace ID
  - Audit log data signature (tamper proofing)
  - Audit log category (for classification to separate say performance from security audit logs)
  - Service/command/application name
  - User or system account associated with the event
  - Device used (e.g. source and destination IPs)
  - Action or command executed e.g. select, create, delete
  - User ID associated with action performed
  - Date and time stamp in standard format (use central time server)
  - Access status for applications, and data – whether successful or not
  - Protection system notifications (i.e. intrusion detection or anti-malware notifications)
- Audit trace logs need to be enabled and formatted to capture forensic information.

Log Design Approach

Objective – Review existing Mojaloop audit logging design

Value to Mojaloop – Investigate possible audit logging design for Mojaloop.

- Security and compliance are distinct from operational diagnostics
- Logging design critical for:
  - Capacity (data retention).
  - Maintaining context
- How would a good logging design look like
  - "Easy/Fast" diagnostics, incident detection and response, compliance
  - Support frameworks and APIs for integration and automation
  - Legacy support (esp. the open source universe)

Security Triage and Compliance	EFK SIEM Tool		
Integration Interface	Mojaloop Event Framework | Syslog		
Log platform	Log4J / Log4J 2	**Winston**	Logback
Log Sources	Operating System | Infrastructure | Databases | Applications | APIs | Identity Manager		
Log Types	Application Diagnostics Security Audit		

Next Steps

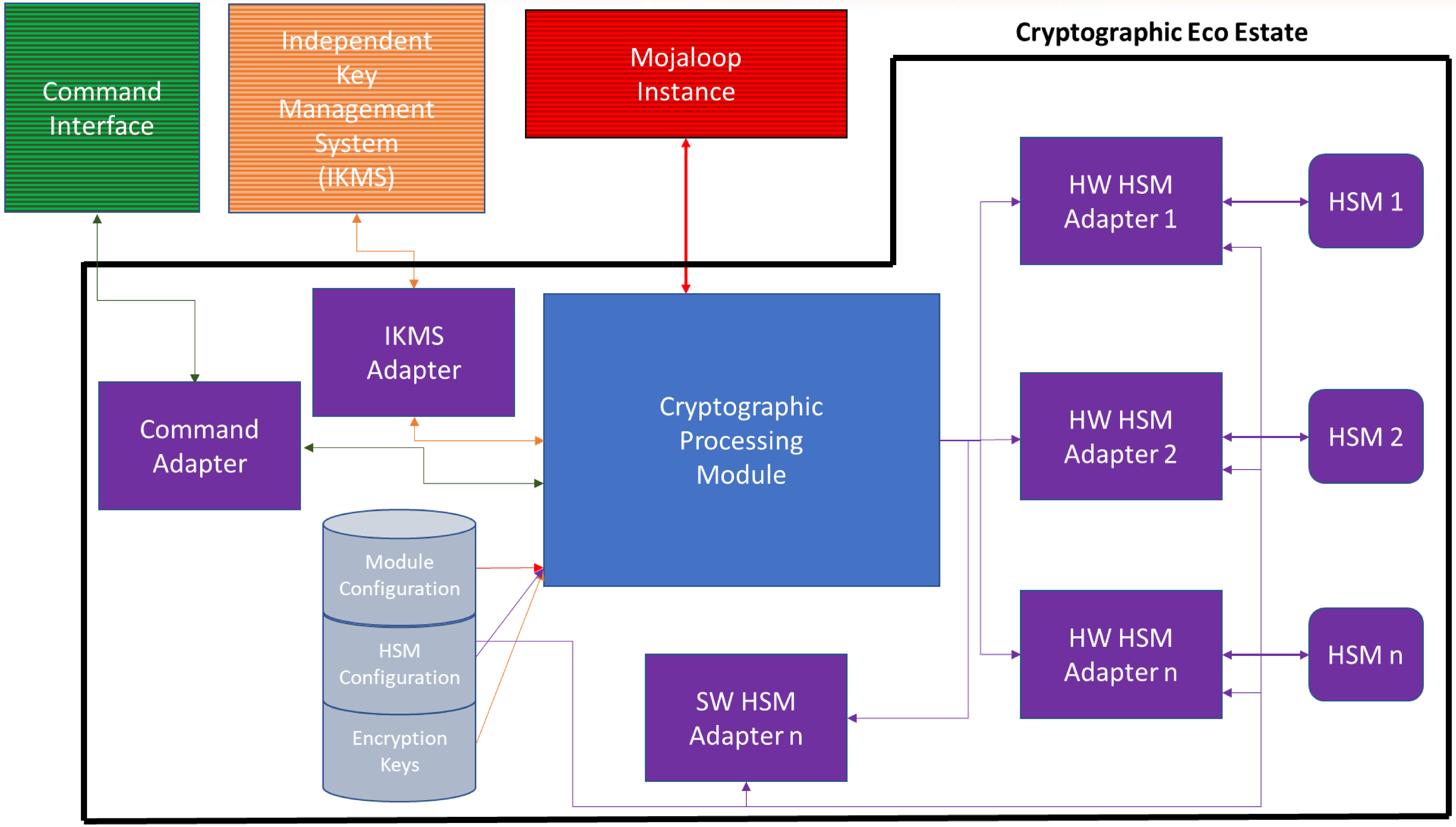
1. Explore Winston audit log format in Mojaloop and enable audit logging for Kafka, Kubernetes, WSO2, Databases etc Mojaloop Infrastructure in test environment
2. Develop EFK security dashboards in Mojaloop for logs above as MVP

Cryptographic Processing Module Update

By Max Gysi

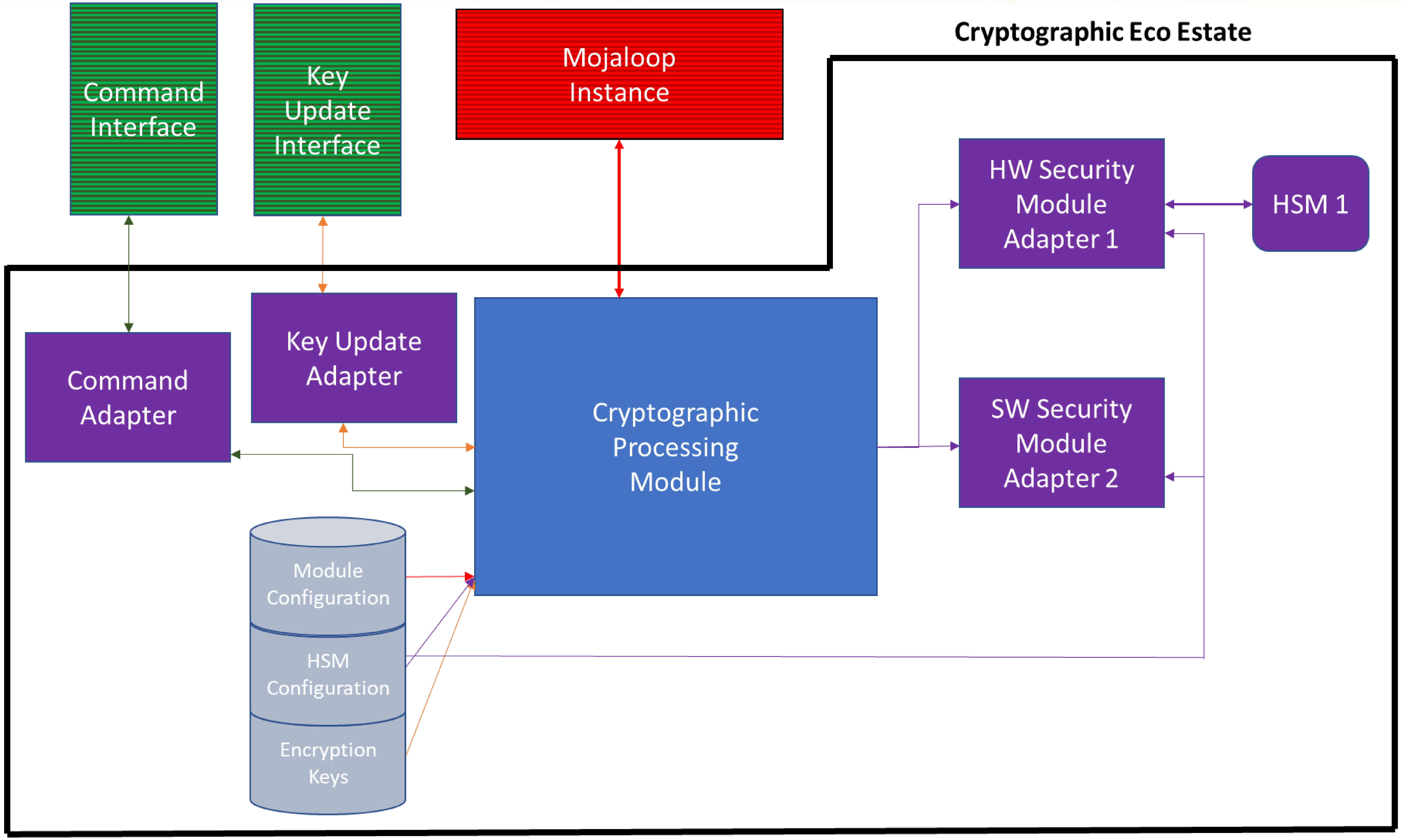
Cryptographic Processing Module HLD

High Level Design(HLD) System Overview - Approved



Cryptographic Processing Module LLD

Low Level Design(LLD) System Overview Phase 1 - Approved



Cryptographic Processing Module - LLD

Phase 1 In-Scope - System Components Included

1. Cryptographic Processing Module
   a. Heart and brains of the system
   b. Controls who does what and how via configuration
2. Command Adapter
   a. Will expose the use of commands to run the system to approved operators
3. Key Update Adapter
   a. Will allow organizations to Add/Update or Delete Keys/Certificates as necessary
4. Software Security Module
   a. Will Implement the security for already accepted Use Cases in Software
   b. Adhere to the currently agreed security principles
5. Hardware Security Module
   a. A base skeleton to build-on when a hardware security module is needed, and one vendor has been selected

Cryptographic Processing Module - LLD

Phase 1 Out of Scope - System Components Excluded

Low Level System Overview Phase 1 – Components Excluded

1. Key Management System Adapter
   a. An adapter that will accept updates from a full Key Management system that can handle the full life cycle of a key
   b. Will adhere to the KMIP standard initially
   c. Not all FSPs will have access to one initially
2. Full Hardware Security Adapter
   a) Only the skeleton will be developed, not full hardware security functionality
   b) A full adapter can be developed once a use case and vendor agreed upon

Cryptographic Processing Module Roadmap

Next Steps

1. Plan the development of phase 1
2. Start discussion with other players on new use cases
3. Plan the integration of the CPM with other adapters like the ISO8583 and ISO20022

muchas gracias

mojaloop

Thank you

Questions and Comments