mojaloop

Mowali Update

January 2019

Outline

- Mutual TLS Connectivity – Certificate Handling
- OAuth & JWS
- Backend Configuration
- Golden DFSP Simulator

Mutual TLS Connectivity

- Current Setup
  - DFSP to Switch (External WSO2 Gateway)
    - Switch public server certificate exchanged with DFSPs
    - DFSP Client Certificate exchanged with Switch and configured in Switch Gateway
  - Switch to DFSP – Callbacks (Internal WSO2 Gateway)
    - DFSP public server certificate exchanged with Switch and configured in Switch Gateway
    - Switch Client certificate exchanged with DFSP
- Challenges
  - Certificate Handling in WS02, using keystores and trust-stores – No Better UI
  - A better CA Handling
  - Certificte Expiry issues

OAuth & JWS

- OAuth
  - FSP Specific profile is created in Gateway
  - This creates a FSP specific Consumer Key and Secret that is private to DFSP
  - Using Consumer Key and Secret, FSP obtains an Oauth Token that is provided in any requests that are submitted to Switch
- JWS
  - For API Confidentiality and Non-Repudiability
  - FSPIOP-Signature Header used

- Challenges
  - Each DFSP needs to maintain public certs for all the peer DFSPs – A Central Repository
  - Custom mediation flows per DFPS in WSO2 Gateway for OAuth- Not Scalable

Configuration in Backend Services

- FSP Account based on currency is created
- Net Debit Cap limits, initial position values, Threshold Percentage for NDC Approach are configured for FSP
- FSP Callback endpoints are configured
  - Success notifications
  - Error responses/notifications

- Recommendation
  - A Self-Service Portal

Golden DFSP Simulator

- Implementation of Security
  - mTLS, OAuth, JWS
- Functional implementation
  - Parties, quotes, transfers endpoints
  - Including error endpoints
- Locally Downloadable
  - A DFSP able to test it locally against their implementation