mojaloop

HSM Integration

HSMs and Security Zones

Max Gysi

max@gysisolutions.com

22nd April 2020

mojaloop

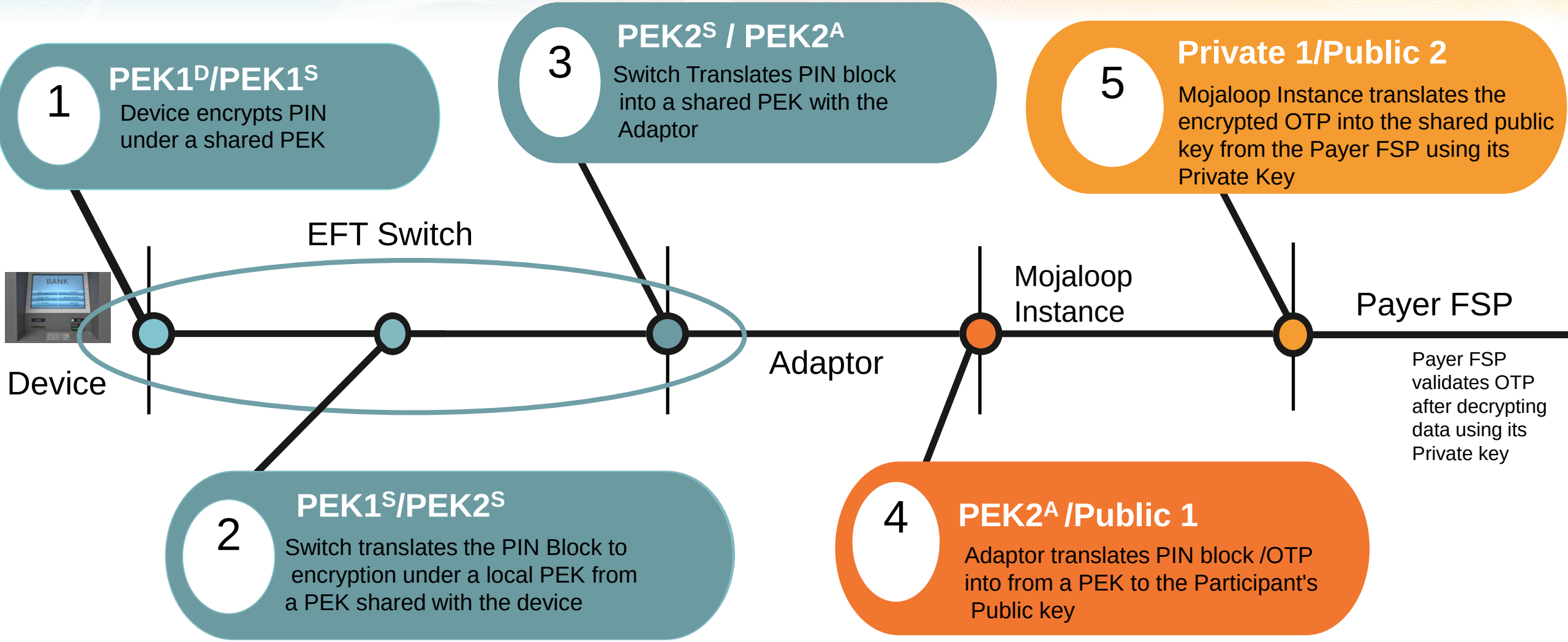
HSMs and Security Zones

- What is an HSM
  - An HSM (Hardware Security Module) is a device that is designed for high speed encryption/decryption of sensitive data in a strictly control environment. These devices are governed by the PCI HSM standards.
- What is a Security Zone
  - A Security Zone is where the data between two points in the flow of a transaction is protected by shared encryption keys. In the case of symmetric keys it a known key encrypted under the Master Key of the HSM at each point. In the case of asymmetric keys data is encrypted by a participant under a public key of the other participant’s private key, or vice versa

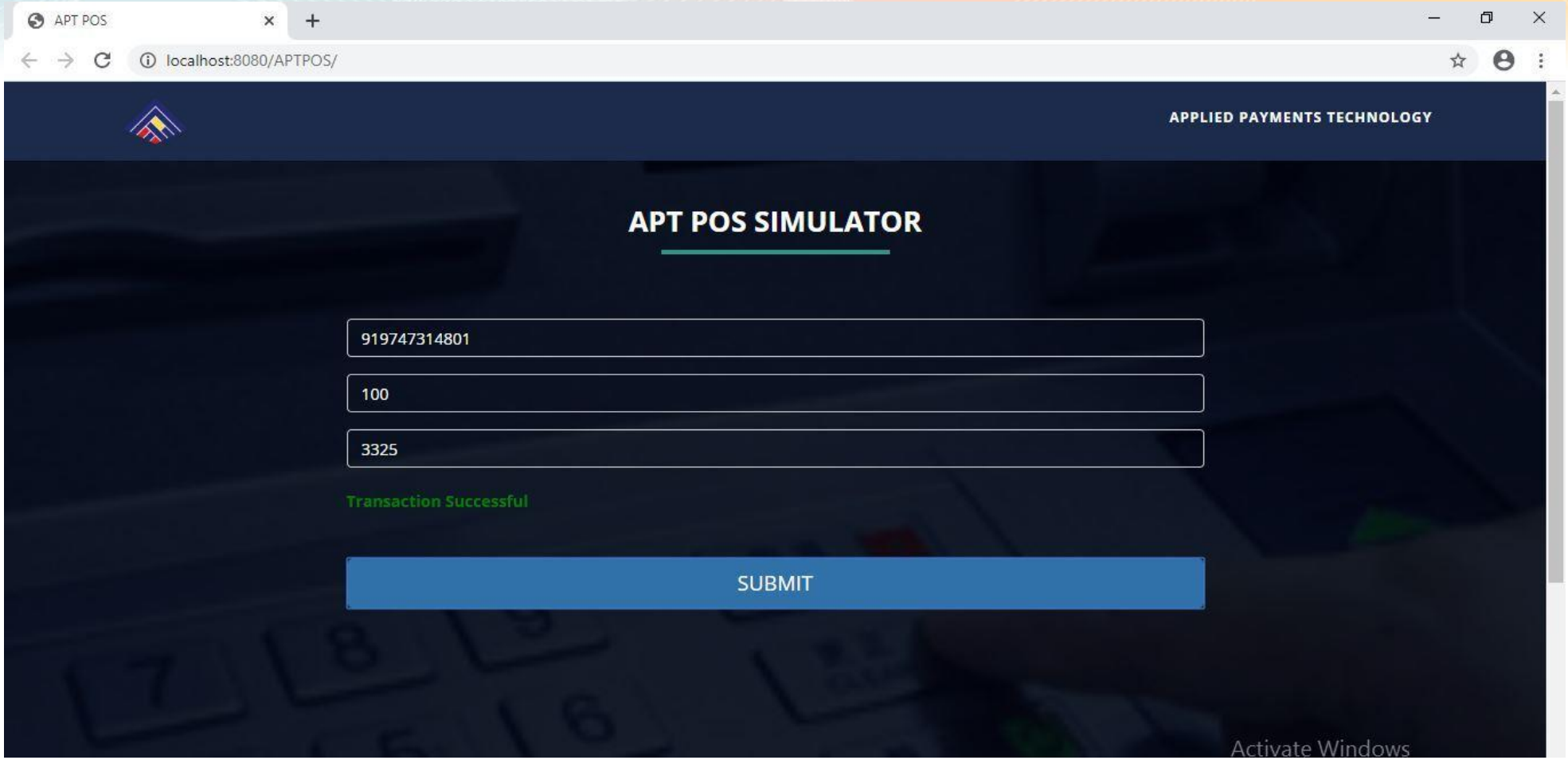
Why do we need them

- Sensitive data that travels through any payment system needs to be secured, through encryption
- If it is done in software, it can be hacked and stolen
- The structure of HSMs is mandated by the PCI council to ensure the integrity of the device, the standards constantly being updated
- HSMs use keys encrypted under a Master Key to encrypt and decrypt data. These keys are shared amongst participants in order to decrypt the data the other has encrypted, or translate from one encryption key to another
- Security zones are used so data can be exchanged between multiple participants in a chain, without the one knowing the keys of the previous. This allows a transaction to take many routes and always stay secure.
- Without Security Zones, in the case of banks and ATMs, every bank would have to know the encryption keys of every ATM in the world.

Switch Payment Security Zones



Simulation of Zones



Phone number is 91 974 731 4801
OTP is 3325

Simulation of Zones – cont.

- Pin is encrypted and Pin Block created
  - First the clear pin is encrypted under the Master Key
    - SENT - 1234BA3325919747314801
    - RECV - 1234BB0049821
  - Then the Pin block is created from the encrypted pin and the PIN Encryption Key
    - SENT - 1234JGU77FBFBC8BC3C864C960124EB984795BA01919747314801 49821
    - RECV - 1234JH00CE5121791BFA597D
- Pin block is moved to 8 character binary field and sent to the switch
- Pin block is translated from Device/Switch Zone (1) to an Internal Zone (2)
    - SENT - 1234CCU77FBFBC8BC3C864C960124EB984795BAU0F0C4B64621AC36DCACC576B3FEC408C12CE5121791BFA597D0101919747314801
    - RECV - 1234CD0004A7177354BD7ED40E01

Simulation of Zones

Example of data received and response in HSM Endpoint

```
DATA + 127.0.0.1
<Buffer 35 61 65 31 38 38 65 65 64 33 61 32 36 38 34 36 39 31 39 37 34 37 33 31 34 38 30
31>
String data :
Sending to HSM: 172.10.10.135:9005
Sending JC command to HSM :  00JCUDB736E98DF7589C14A7EBD533D62D46E5ae188eed3a268460191974
7314801
Received JD command from HSM  <Buffer 00 0b 30 30 4a 44 30 30 33 36 36 39 32>
Client connected to: 172.10.10.135:9005
encrypted 36692
Sending NG command to HSM :  00NG919747314801366 92
Received NH command from HSM  <Buffer 00 16 30 30 4e 48 30 30 37 37 36 31 35 32 32 36 30
32 35 39 31 37 30 34>
***Clear OTP : 7761***
```

Simulation of Zones – cont.

- PIN block is translated from Internal Zone (2) to Switch/Adaptor Zone (3)
  - SENT - 1234CCU0F0C4B64621AC36DCACC576B3FEC408CU77FBFBC8BC3C864C960124EB984795BA12A7177354BD7ED40E0101919747314801
  - RECV - 1234CD0004CE5121791BFA597D01
- PIN block is then inserted into authorisation message and sent to the Adaptor
- Adaptor translates the PIN block under PEK(Zone3) to JWS encryption (Zone4) under Public key 1
  - SENT - 1234JCU77FBFBC8BC3C864C960124EB984795BACE5121791BFA597D01919747314801
  - RECV - 1234JD0049821
  - SENT - 1234NG919747314801 49821
  - RECV - 1234NH0033325923555964304
- Mojaloop instance translates the data from it’s Private key to Payer FSP Public key

Simulation of Zones - cont

- Payer FSP decrypts and validates the OTP using it’s private key


```
JWT :  {"JWT":"eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJwaG9uZU5vIjoiOTE5NzQ3MzE0ODAxIiwib3RwIjoiMzMyNSJ9.OYHTfHkb7uQzlc06l0arnYFgxy7SXNAqr9EXdMSUUStyxksADc9R2
qmqufHQMBEbKJ68Pbl--xMyL7tqqbD4rhZIinXUAEnniDXB-qVdEkR2FHASJ1NW73qDUZmwRh_9sqYrwCg_PjRsURFTHklJoNxggRHllzlCRIWQ1j9MM7zafZRCQFL3oL3Mgfn1dz_G3MT5noHixKDt_cw4XbB
zT4TAyw2SmTh3IEMgPYOXSdFdro_9k0nH29RqYcCViLsYuVlxwI841Dywfz1_zARk3MMKB3-0MUUT7I6KOw4gAfvR97x2wlqqSf_9dbOm6yor9MakMAuziZYAjswwuN4-pw"}
PUB_KEY :  -----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAnzyis1ZjfNB0bBgKFMSv
vkTtwlvBsaJq7S5wA+kzeVOVpVWwkWdVha4s38XM/pa/yr47av7+z3VTmvDRyAHc
aT92whREFpLv9cj5lTeJSibyr/Mrm/YtjCZVWgaOYIhwrXwKLqPr/11inWsAkfIy
tvHWTxZYEcXLgAXFuUuaS3uF9gEiNQwzGTU1v0FqkqTBr4B8nW3HCN47XUu0t8Y0
e+lf4s4OxQawWD79J9/5d3Ry0vbV3Am1FtGJiJvOwRsIfVChDpYStTcHTCMqtvWb
V6L11BWkpzGXSW4Hv43qa+GSYOD2QU68Mb59oSk2OB+BtOLpJofmbGEGgvmwyCI9
MwIDAQAB
-----END PUBLIC KEY-----

jwtHeader : {"JWT":"eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9
jwtPayload : eyJwaG9uZU5vIjoiOTE5NzQ3MzE0ODAxIiwib3RwIjoiMzMyNSJ9
jwtSignature: OYHTfHkb7uQzlc06l0arnYFgxy7SXNAqr9EXdMSUUStyxksADc9R2qmqufHQMBEbKJ68Pbl--xMyL7tqqbD4rhZIinXUAEnniDXB-qVdEkR2FHASJ1NW73qDUZmwRh_9sqYrwCg_PjRsURFT
HklJoNxggRHllzlCRIWQ1j9MM7zafZRCQFL3oL3Mgfn1dz_G3MT5noHixKDt_cw4XbBzT4TAyw2SmTh3IEMgPYOXSdFdro_9k0nH29RqYcCViLsYuVlxwI841Dywfz1_zARk3MMKB3-0MUUT7I6KOw4gAfvR97
x2wlqqSf_9dbOm6yor9MakMAuziZYAjswwuN4-pw"}
jwtSignatureBase64 :  OYHTfHkb7uQzlc06l0arnYFgxy7SXNAqr9EXdMSUUStyxksADc9R2qmqufHQMBEbKJ68Pbl++xMyL7tqqbD4rhZIinXUAEnniDXB+qVdEkR2FHASJ1NW73qDUZmwRh/9sqYrwCg/
PjRsURFTHklJoNxggRHllzlCRIWQ1j9MM7zafZRCQFL3oL3Mgfn1dz/G3MT5noHixKDt/cw4XbBzT4TAyw2SmTh3IEMgPYOXSdFdro/9k0nH29RqYcCViLsYuVlxwI841Dywfz1/zARk3MMKB3+0MUUT7I6KO
4gAfvR97x2wlqqSf/9dbOm6yor9MakMAuziZYAjswwuN4+pw"}
payloadInBase64UrlFormat : eyJwaG9uZU5vIjoiOTE5NzQ3MzE0ODAxIiwib3RwIjoiMzMyNSJ9
signatureIsValid : true
decodedPayload : {"phoneNo":"919747314801","otp":"3325"}
```


- Providing all other checks are successful, the transaction can now be authorised and responded to the Payer FSP

Online Demonstration of OTP Encryption and Decryption

Renjith Palamattom

Jordy George